



EUROPEAN UNION AGENCY
FOR CYBERSECURITY



ENISA THREAT LANDSCAPE 2024

July 2023 to June 2024

SEPTEMBER 2024

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency collaborates with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at: www.enisa.europa.eu.

CONTACT

To contact the authors, please use etl@enisa.europa.eu

For media enquiries about this paper, please use press@enisa.europa.eu

EDITORS

Ifigeneia Lella, Marianthi Theocharidou, Erika Magonara, Apostolos Malatras, Rossen Svetozarov Naydenov, Cosmin Ciobanu, Georgios Chatzichristos – European Union Agency for Cybersecurity

CONTRIBUTORS

Claudio Ardagna, Stephen Corbiaux, Koen Van Impe

ACKNOWLEDGEMENTS

We would like to thank the ENISA Advisory Group and the National Liaison Officers network for their valuable feedback, as well as ENISA colleagues Jamila Boutemeur and Johannes Clos for their invaluable review.

We would also like to thank the Information Integrity and Countering Foreign Information Manipulation and Interference Division (SG. STRAT.4) for sharing the data on information manipulation and revising and contributing to Chapter 9.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.



COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2024

This publication is licenced under CC-BY 4.0 "Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated".

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN: 978-92-9204-675-0, DOI: 10.2824/0710888



TABLE OF CONTENTS

1. THREAT LANDSCAPE OVERVIEW	6
2. THREAT ACTOR TRENDS	20
3. VULNERABILITIES LANDSCAPE	34
4. RANSOMWARE	45
5. MALWARE	56
6. SOCIAL ENGINEERING	62
7. THREATS AGAINST DATA	69
8. THREATS AGAINST AVAILABILITY: DENIAL OF SERVICE	78
9. INFORMATION MANIPULATION AND INTERFERENCE	91
A ANNEX: MAPPING TO MITRE ATT&CK FRAMEWORK	101
B ANNEX: RECOMMENDATIONS	110



EXECUTIVE SUMMARY

2024 marks the 20th anniversary of the European Union Agency for Cybersecurity, ENISA. ENISA has been constantly monitoring the cybersecurity threat landscape and monitoring on its state with its annual ENISA Threat Landscape (ETL) report and additionally with a series of situational awareness and cyber threat intelligence products.

Over time, the ETL has served as a crucial tool for comprehending the present state of cybersecurity within the European Union (EU), furnishing insights into trends and patterns. This, in turn, has guided pertinent decisions and prioritisation of actions and recommendations in the domain of cybersecurity.

Reporting over the course of 2023 and 2024, ETL highlights findings on the cybersecurity threat landscape during a yearlong geopolitical escalation. Throughout the latter part of 2023 and the initial half of 2024, there was a notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents, as well as their consequences. The ongoing regional conflicts still remain a significant factor shaping the cybersecurity landscape. The phenomenon of hacktivism has seen steady expansion, with major events taking place (e.g. European Elections) providing the motivation for increased hacktivist activity.

7 prime cybersecurity threats were identified, with threats against availability topping the chart and followed by ransomware and threats against data, and the report provides a relevant deep-dive on each one of them by analysing several thousand publicly reported cybersecurity incidents and events:

- **Ransomware**
- **Malware**
- **Social Engineering**
- **Threats against data**
- **Threats against availability: Denial of Service**
- **Information manipulation and interference**
- **Supply chain attacks**

The report is complemented by a detailed analysis of the vulnerability landscape during 2023 and 2024, as well as a detailed analysis of four distinct threat actors' categories, namely:

- **State-nexus actors;**
- **Cybercrime actors and hacker-for-hire actors;**
- **Private Sector Offensive actors (PSOA);**
- **Hacktivists.**

With 2024 being the year that NIS2 Directive comes into force, an analysis of the cybersecurity threat landscape across different sectors is provided. Notably, we have again observed a large number of events targeting organisations in the public administration (19%), transport (11%) and finance (9%) sectors.

The key findings and judgments in this assessment are based on multiple and publicly available resources. The report is mainly targeted at strategic decision-makers and policy-makers, while also being of interest to the technical cybersecurity community.





1. THREAT LANDSCAPE OVERVIEW

In its twelfth edition, the ENISA Threat Landscape (ETL) report offers a broad overview of the cybersecurity threat landscape. Over time, the ETL has served as a crucial tool for comprehending the present state of cybersecurity within the European Union (EU), furnishing insights into trends and patterns. This, in turn, has guided pertinent decisions and prioritisation of actions and recommendations. The ETL report combines strategic and technical elements, catering to both technical and non-technical audiences. The ETL 2024 report has been validated and supported by the ENISA Advisory Group and the ENISA National Liaison Officers (NLO) Network.

Throughout the latter part of 2023 and the initial half of 2024, there was a notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents, as well as their consequences. The ongoing regional conflicts still remain a significant factor shaping the cybersecurity landscape. The phenomenon of hacktivism has seen steady expansion, marked by the emergence of numerous new groups. Major events taking place at a national or European level provided the motivation for increased hacktivist activity during the reporting period (e.g. European Elections).

The ETL 2024 report follows the same customary approach, drawing on diverse open-source data and cyber threat intelligence sources. It pinpoints significant threats, discerns emerging trends and offers practical high-level strategies for mitigating risk. This year's ETL continues to use the officially endorsed ENISA Cyber Security Threat Landscape Methodology¹, which was released in 2022. The ENISA CTL Methodology serves as a foundational framework for the transparent and systematic creation of comprehensive cybersecurity threat landscapes, spanning horizontal, thematic and sector-specific perspectives. This process is characterised by rigorous data collection and analysis procedures.

1.1 METHODOLOGY

The ENISA Cybersecurity Threat Landscape (CTL) methodology² was used to produce the ETL 2024 report. The methodology was published in July 2022.

The ENISA Threat Landscape (ETL) 2024 report is based on information from open sources, mainly of a strategic nature and ENISA's own Cyber Threat Intelligence (CTI) capabilities. It covers more than one sector, technology and context. The report aims to be industry and vendor agnostic. It references or cites the work of various security researchers, security blogs and news media articles throughout the text in multiple footnotes to validate findings and statements. The time span of the ETL 2024 report is July 2023 to June 2024 and is referred to as the 'reporting period' throughout the report.

During the reporting period, ENISA gathered a list of major incidents as they appeared in open sources through situational awareness. This list serves as the foundation for identifying the list of prime threats and the source material for several trends and statistics in the report.

¹ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology>.

² ENISA Cybersecurity Threat Landscape (CTL) methodology, July 2022. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology>.



Subsequently, an in-depth desk research of available literature from open sources such as news media articles, expert opinion, intelligence reports, incident analysis and security research reports were conducted by ENISA and external experts. Note that many intelligence and research reports are written on the basis of a January to December year, contrary to the ETL's reporting period which is from July to June. Through continuous analysis, ENISA derived trends and points of interest. The key findings and assessments are based on multiple and publicly available resources which are provided in the references used for the development of this document.

Within the report, we differentiate between what has been reported by our sources and what is our assessment. When conducting an assessment, we convey probability by using words that express an **estimate of likelihood**³.

When we refer to threat actors in this report, we use the naming convention used by the company revealing the campaign, as well as a number of aliases⁴ commonly used in the industry.

1.2 PRIME THREATS

According to the findings detailed in this report, the ENISA Threat Landscape 2024 report highlights and directs attention toward eight prime threat types (see Figure 1). These particular threat types have been singled out due to their prominence over the years, their widespread occurrence and the significant impact resulting from the realisation of these threats.

- **Ransomware**

According to ENISA's Threat Landscape for Ransomware Attacks⁵ report, ransomware is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability or in exchange for publicly exposing the target's data. This definition is needed to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques and the various goals, other than solely financial gains, of the perpetrators. Ransomware has been, once again, one of the prime threats during the reporting period, with several high profile and highly publicised incidents.

- **Malware**

Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system.

- **Social Engineering**

Social engineering encompasses a broad range of activities that attempt to exploit human error or human behaviour with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information. Users may be lured to open documents, files or e-mails, to visit websites or to grant access to systems or services. Although the lures and tricks used may abuse technology, they rely on a human element to be successful. This threat canvas consists mainly of the following attack vectors: phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps and scareware. While social engineering techniques are often used to gain initial access, they may also be

³ MISP estimative language https://www.misp-project.org/taxonomies.html#_estimative_language.

⁴ MISP Galaxies and Clusters <https://github.com/MISP/misp-galaxy>.

⁵ ENISA Threat Landscape for Ransomware Attacks <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks>.



used at later stages in an incident or breach. Notable examples are business e-mail compromise (BEC)⁶, fraud, impersonation, counterfeit and, more recently, extortion.

- **Threats against data**

A data breach is defined in the GDPR as *any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed* (article 4.12 GDPR). Technically speaking, threats against data can be broadly classified as data breach or data leak. Though often used as interchangeable, they entail fundamentally different concepts that mostly lie in how they happen^{7 8}.

Data breach is an intentional cyber-attack brought by a cybercriminal with the goal of gaining to unauthorised access and release sensitive, confidential or protected data. In other words, a data breach is a deliberate attack against a system or organisation with the intention of stealing data. *Data leak* is an event (such as misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data (intentional attacks are sometimes referred to as data exposure).

- **Threats against availability: Denial of Service**

DDoS targets system and data availability and, though it is not a new threat, it plays a significant role in the cybersecurity threat landscape^{9 10}. Attacks occur when users of a system or service are not able to access relevant data, services or other resources. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure¹¹. The impact of DDoS attacks is often limited and symbolic¹²

- **Information Manipulation**

Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. FIMI can be carried out by state or non-state actors, including their proxies inside and outside their own territory; in this report we study the threat regardless of its origin.

It should be noted that the aforementioned threats involve categories and refer to collections of diverse types of threats that have been consolidated into the seven areas mentioned above. Each of the threat categories is further analysed in a dedicated chapter in this report with the exception of the supply chain, which elaborates on its particularities and provides more specific information on findings, trends, attack techniques and mitigation vectors.

⁶ [Internet Organised Crime Threat Assessment IOCTA 2024.pdf \(europa.eu\)](#)

⁷ <https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference>.

⁸ <https://www.upguard.com/blog/data-breach-vs-data-leak#:~:text=Simply%20put%2C%20a%20data%20leak,Apps%20data%20leak%20in%202021>.

⁹ Federal Office for Information Security (BSI), The State of IT Sec in Germany, September 2020.

¹⁰ Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>.

¹¹ CISA, Understanding Denial-of-Service Attacks, November 2019, <https://www.uscert.gov/ncas/tips/ST04-015>.

¹² [Nederlandse organisaties doelwit van DDoS-aanvallen | Nieuwsbericht | Nationaal Cyber Security Centrum \(ncsc.nl\)](#)

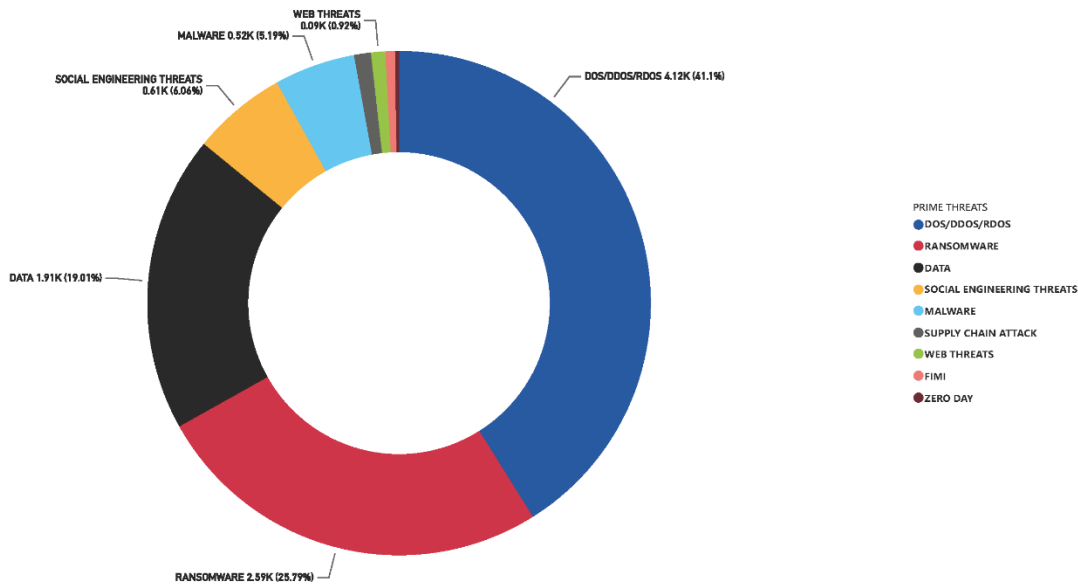


Figure 1: ENISA Threat Landscape 2024 - Prime threats



In the following figure it can be seen that for another year ransomware and DDoS attacks were the most reported forms of attacks during the reporting period and accounted for more than half of the observed events followed by threats related to data. In several cases incidents involved more than one threat category and were thus analysed in the context of all respective categories. Given that the ETL is based on publicly available information and the fact that such information might not always provide the full picture, in certain cases incidents could not be classified into any threat category.

Figure 2: Breakdown of analysed incidents by threat type (July 2023 till June 2024)



1.3 KEY TRENDS

The list below summarises the main trends observed in the cyber threat landscape during the reporting period. Further details and analysis of the trends may be found throughout the various chapters that comprise the ENISA threat landscape of 2024.

- **Threats against availability (DDoS) and Ransomware ranked at the top during the reporting period for another year.**
- **Living Off Trusted Sites (LOTS):** Threat actors extended their stealth techniques into the cloud, using trusted sites and legitimate services to avoid detection and disguising Command and Control communications (C2) as ordinary traffic or innocuous messages on platforms like Slack and Telegram.
- **Geopolitics continued to be a strong driver for cyber malicious operations.**
- **Advancements in defensive evasion techniques:** Cybercrime groups, especially ransomware operators, evaded detection by using Living Off The Land (LOTL) techniques. to blend into environments and mask their malicious activities.
- There has seen a **sharp increase^{13 14} in Business Email Compromise (BEC) incidents¹⁵**
- **Extortion by weaponizing disclosure requirements,** pushing companies to fulfil extortion demands ahead of the required reporting deadline.
- **Ransomware attacks appear to have stabilized in quite high numbers in regards to the previous reporting period**
- **Ever more impactful law enforcement operations,** such as Operation Chronos and Operation Endgame.
- **AI tools for cyber criminals:** Threat actors used tools such as FraudGPT and large language models to co-author scam emails and generate malicious PowerShell scripts.
- **19,754 vulnerabilities** were identified with 9.3% fell into the 'critical' category and 21.8% were categorised as 'high'.
- **Information stealers continue to be heavily used by threat actors: Due to the popularity of IABs and downloaders.** Information stealers are now essential components in attack chains.
- **Hacktivists overlapping their activities with State-nexus actors:** A notable trend is the increasing similarity between State-nexus actors and alleged hacktivist activities.
- **Data leak site have started being considered to be unreliable.** Many of the data leaks posted are duplicates of previous attacks or wrongly attributed to the Lockbit ransomware group. This follows the disruption of their operations by Operation Chronos.
- **Recent surge in mobile banking trojans has been observed,** with a concomitant increase in the complexity of their attack vectors.
- **Malware-as-a-Service (MaaS)** offerings continued to be a significant and rapidly evolving threat, particularly since mid-2023.
- **Supply chain compromises through social engineering are emerging:** for example, in March 2024, backdoor code was introduced in an open-source project XZ Utils, a set of tools and libraries used for data compression¹⁶.
- **Data compromise increased in 2023-2024.** There was a rise in data compromises leading up to 2021 and although this trend remained relatively stable in 2022, it began to increase once more in 2023 and showed signs of maintaining this momentum in 2024.
- **DDoS-for-Hire allows large-scale attacks** to be launched by unskilled users having access to DDoS services.
- **Information manipulation continues to be a key element of Russia's war of aggression against Ukraine,** although an effort to further localise content and, at the

¹³ FBI - IC3 Report - https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf

¹⁴ Group IB - Hi-Tech crime trends - <https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-eu/>

^{15 15} [Internet Organised Crime Threat Assessment IOCTA 2024.pdf \(europa.eu\)](https://www.europa.eu/press-room/media/infographic/item/12345)

¹⁶ [The XZ-factor: social vulnerabilities in open source projects | By our experts | National Cyber Security Centre \(ncsc.nl\)](https://www.ncsc.nl/en/news/2024/03/xz-factor-social-vulnerabilities-in-open-source-projects)



same time, to globalise its presence is observed. Manipulating information in response of specific news seems to have increased, probably because 2024 has been marked by many major events, elections in particular.

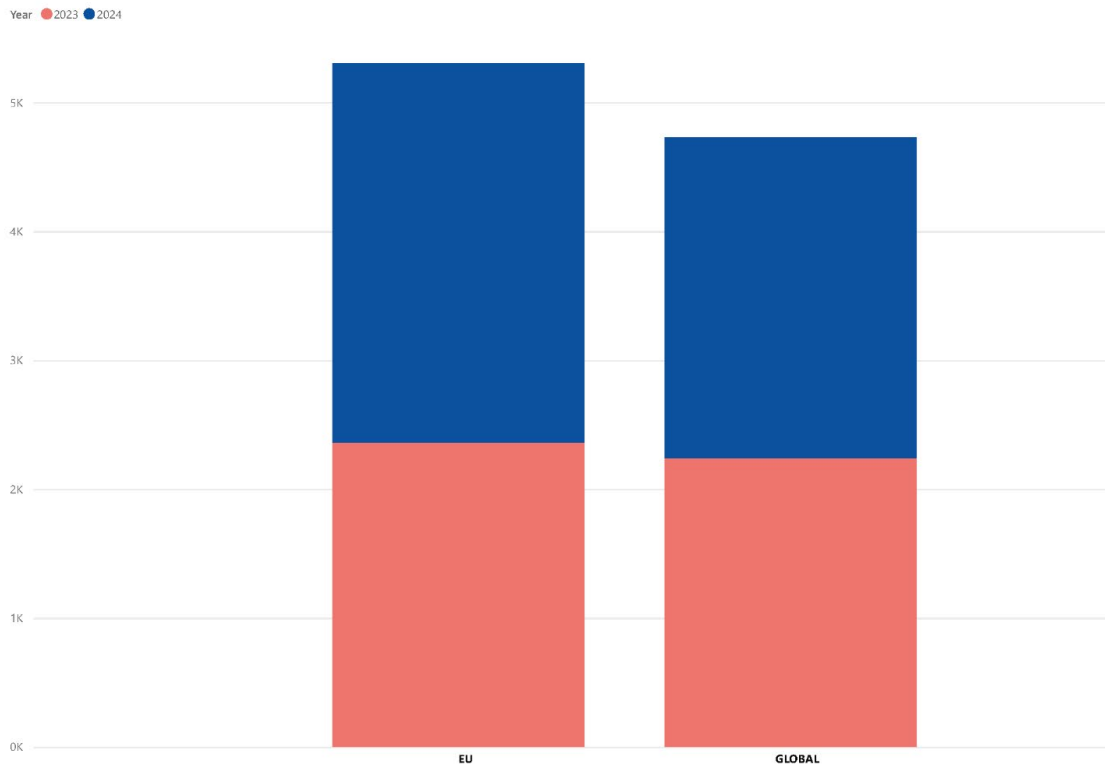
- **The threat of AI-enabled information manipulation has been observed**, but still on a limited -albeit evolving - scale. For example, some threat actors are experimenting with AI for information manipulation seemingly to assess how AI can be exploited in this context.

1.4 EU PRIME THREATS

Cyber-attacks continue to increase on the global scale; however, ENISA’s scope is primarily focused on EU member states and thus more emphasis is placed on the landscape within the EU.

Figure 3 shows a significant increase in events in the EU in the first half of 2024 compared to the second half of 2023, though on a global scale (non-EU) the spread seems to be more even. It’s important to recognise that the observed number of events can be influenced by various factors. An increase in reported cyber-attacks doesn’t necessarily indicate an actual rise in the number or severity of attacks. This surge could be due to heightened media or public attention to specific events, leading to more incidents being documented in open-source intelligence (OSINT) channels, or threat actors claiming victims with no real impact on those victims.

Figure 3: Break down of Global and EU events (July 2023 – June 2024)



Throughout the reporting period, EU Member States continued to be affected by ongoing geopolitical crises, with a growing number of threat actors directing their efforts against both public and private organisations. These kinds of events more often fall under the DDoS threat (chapter 2, section 4, and chapter 7) with little to no impact in most of the cases reported through OSINT. Ransomware attacks have shown a decrease (chapter 4) in the EU.



ENISA observed 11,079 incidents, including 322 incidents specifically targeting two or more EU Member States (labelled 'EU') as it can be seen in Figure 4 which shows a timeline of when the events were first reported through open-source channels. In addition, throughout this iteration of the ETL it can be seen that ransomware and DDoS still remained the two prime threats for the EU as shown in Figure 5.

Figure 4: Timeline of EU events (count of number of observed incidents a month)

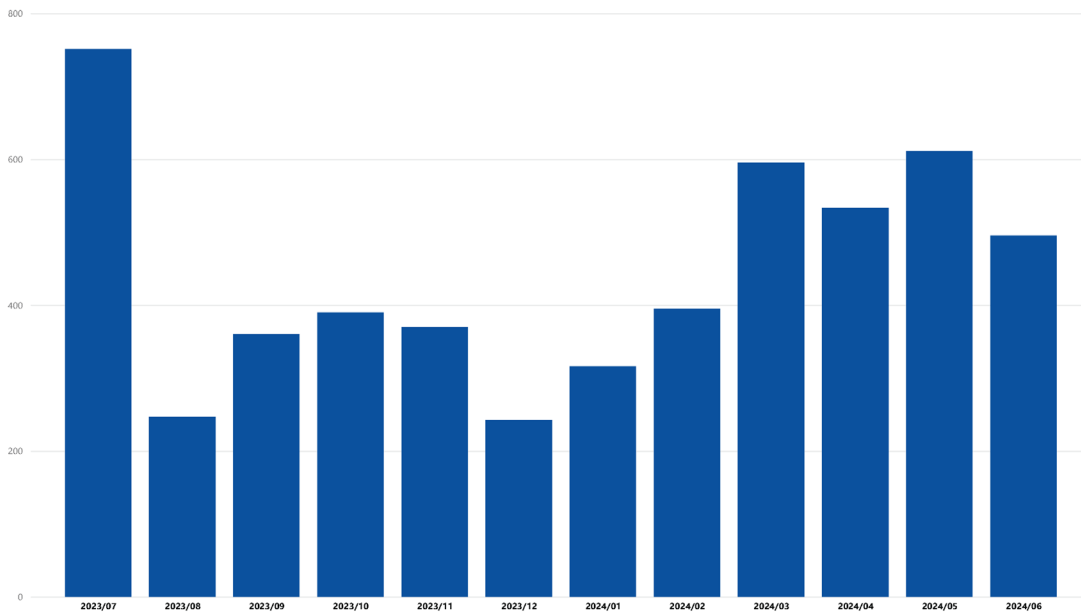
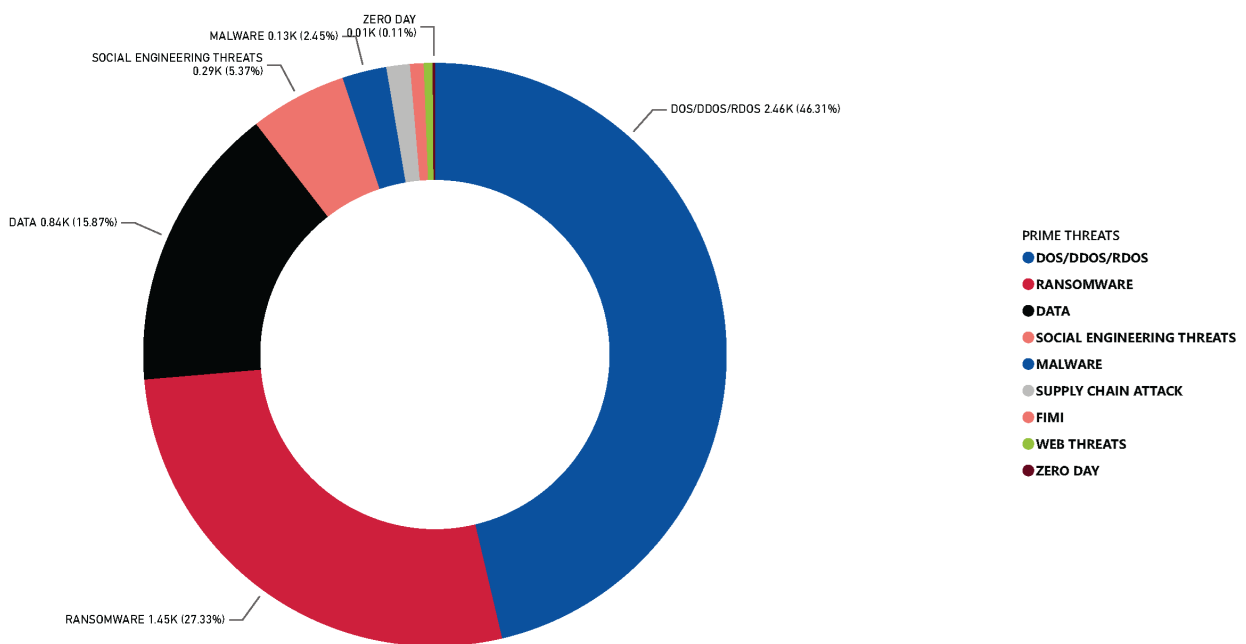


Figure 5: EU breakdown of number of threats by threat group



1.5 SUPPLY CHAIN

Supply chain attacks has become a threat on a horizontal level touching upon multiple of the other threats. The reason why for this year it was decided not to have a separate chapter even



though was that few incidents were reported to be of a supply chain attack. This does not mean that we did not have incidents just that maybe they were not reported publicly as being or affecting supply chains.

One of the most controversial incidents during the reporting period was of the incident with 3CX which offered a glimpse into the potentials threats we face. In March 2024, backdoor code was introduced in an open-source project XZ Utils¹⁷, a set of tools and libraries used for data compression.¹⁸ Luckily, the vulnerability was discovered by a software engineer who investigated CPU spikes resulting from the backdoor. The vulnerability was considered critical, as it allowed for easy remote code execution through SSH. This was possible as the malicious actor was made maintainer of the project after a long-lasting social engineering campaign.

The account creation dates to 2021, and the user's first code commit in the project was pushed in 2022. In that period, different (but as it would later seem, connected) accounts started pressuring the original maintainer, accusing him of standing in the way of the project's advancement, suggesting that he would start giving over the reigns over the project. In January, the threat actor took over as primary contact over the project. Over 2023 and 2024, different steps were then performed to prepare the environment and eventually push the backdoor.¹⁹

In a similar case the OpenJS Foundation received a suspicious series of emails with similar messages, bearing different names and overlapping GitHub-associated emails, asking OpenJS to take action to update one of its popular JavaScript projects to "address any critical vulnerabilities,". They also requested OpenJS to designate them as a new maintainer of the project despite having almost no prior involvement. The Open Source Security (OpenSSF) and OpenJS Foundations called out all open source maintainers to be alert for social engineering takeover attempts, to recognize the early threat patterns emerging, and to take steps to protect their open source projects.²⁰

Recent public reports also have highlighted a general high interest²¹, primarily from North Korean-nexus groups²², characterised by more aggressive and expansive intrusions across multiple networks. There has also been a focus^{23 24} on attacks that target update mechanisms or compromise the **open-source software supply chain**. Such attacks^{25 26 27} involve name or repository confusion, tricking developers into using compromised software, or embedding malware in test files. A notable instance involved the introduction of a backdoor in XZ Utils. The sophistication, meticulous planning, and duration of this campaign suggest the involvement of a well-resourced actor, although specific attribution remains unclear at this time. Build systems became^{28 29} a popular target as well for groups associated with Russia and North Korea, but primarily due to vulnerabilities in publicly accessible systems.

¹⁷ [The XZ-factor: social vulnerabilities in open source projects | By our experts | National Cyber Security Centre \(ncsc.nl\)](#)

¹⁸ <https://lists.debian.org/debian-security-announce/2024/msg00057.html>

¹⁹ <https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27>

²⁰ <https://openssf.org/blog/2024/04/15/open-source-security-openssf-and-openjs-foundations-issue-alert-for-social-engineering-takeovers-of-open-source-projects/>

²¹ Mandiant - Assessed Cyber Structure and Alignments of North Korea in 2023 -

<https://www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023>

²² [Notice | Media Center | NIS NATIONAL INTELLIGENCE SERVICE](#)

²³ NSPX30: A sophisticated AitM-enabled implant evolving since 2005 -

<https://www.welivesecurity.com/en/eset-research/nsp30-sophisticated-aitm-enabled-implant-evolving-since-2005/>

²⁴ AVAST - GuptiMiner: Hijacking Antivirus Updates - <https://decoded.avast.io/janrubin/guptiminer-hijacking-antivirus-updates-for-distributing-backdoors-and-casual-mining/>

²⁵ JPCERT - New Malicious PyPI Packages used by Lazarus - https://blogs.jpCERT.or.jp/en/2024/02/lazarus_pypi.html

²⁶ APIIRO - Over 100,000 Infected Repos Found on GitHub - <https://apiiro.com/blog/malicious-code-campaign-github-repo-confusion-attack/>

²⁷ Cyware - North Korean Hackers Targeting Developers with Malicious npm Packages - <https://cyware.com/news/north-korean-hackers-targeting-developers-with-malicious-npm-packages-2a033144>

²⁸ CERT.pl - Russian Foreign Intelligence Service (SVR) Cyber Actors Use JetBrains TeamCity CVE in Global Targeting -

<https://cert.pl/en/posts/2023/12/apt29-teamcity/>

²⁹ Microsoft - Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability -

<https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/>



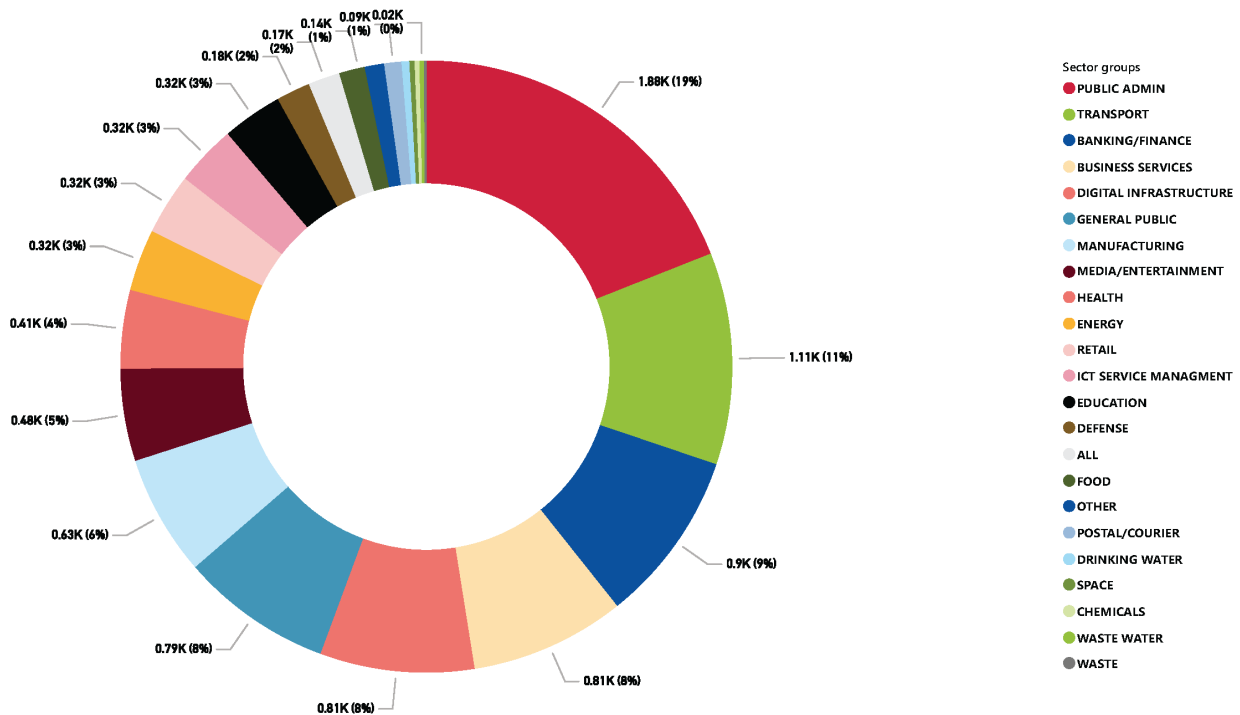
Finally, out of the observed events that ENISA collected, the following ones affected sectors that offer services and products to other sectors: Digital infrastructure (8%), manufacturing (6%) business services (8%), energy (3%) and ICT service management (3%).

1.6 SECTORIAL ANALYSIS

Cyber threats are indiscriminate, impacting a wide range of industries and sectors. This is a direct consequence of our hyper-connected digital world. As the following figures illustrate, threat actors target every sector, highlighting the universal nature of cyber risk.

The sectors analysed in this report follow, in general, the classification of the sector categories in the Network and Information Security Directive (NIS2)³⁰. There are however some deviations, derived by the samples used, as the report may include events affecting sectors beyond the scope of the NIS2 directive. Examples include defence, education³¹, media and entertainment, retail and more. We have also grouped under the term ‘Digital service provider’, the sectors listed in NIS2 as ICT service management (MSPs and MSSPs) and digital providers. There is also a separate category, labelled as ‘all sectors’ which is used when events have an effect across sectors. During the analysis, other sectors were identified that are not currently within the scope of the NIS2 directive, such as consulting, legal, and hospitality services etc, which are grouped under the category ‘Services’.

Figure 6 Targeted sectors per number of incidents (July 2023 - June 2024)



During this reporting period in the overall global landscape, we have again observed a large number of events (Figure 6) targeting organisations in the public administration (19%), transport (11%) and finance (9%) sectors. Events targeting digital infrastructure (8%) and business services form a substantial portion of the events observed. We also observed a considerable number of events targeting civil society and not necessarily a particular sector (these are

³⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555>.

³¹ The education sector was coupled in our sample with the research sector, as they are often intertwined. While the research sector is considered to be within the scope of the NIS2 directive, educational organisations are not included.



labelled as 'General Public' and amount to 8% of the events observed). They consist of social engineering or information manipulation campaigns.

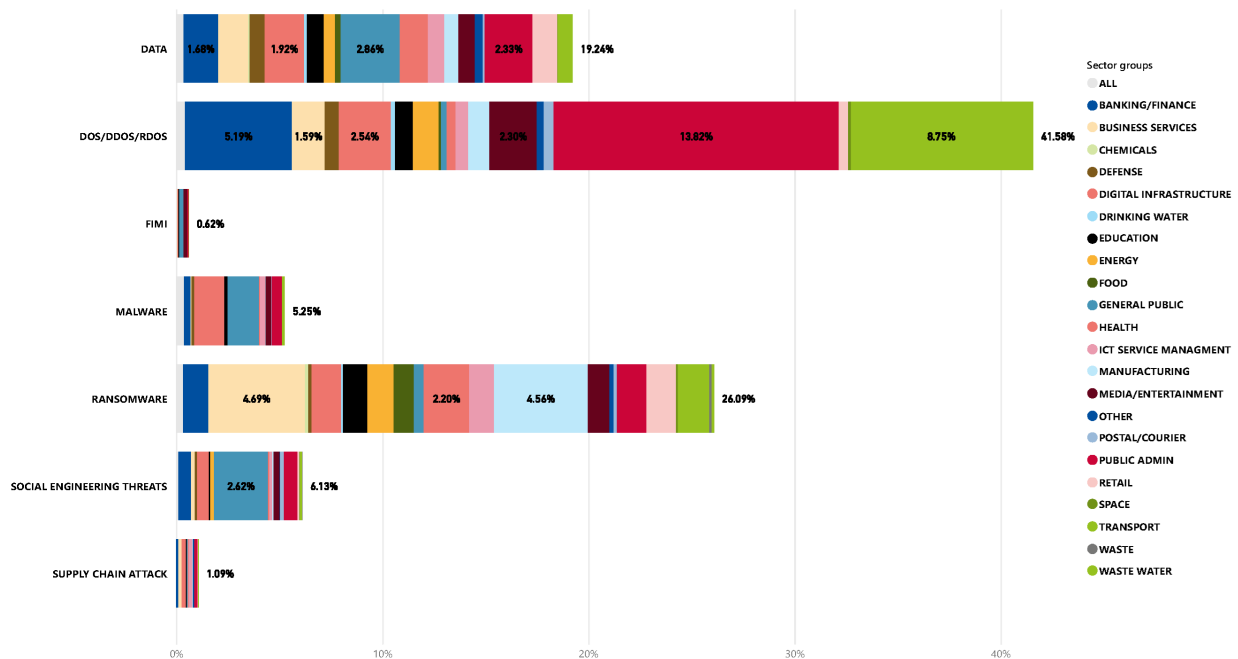
The prime threat was DDoS and it appears to target the entire range of the sectors (Figure 7). The most targeted sectors were public administration (33% out of DDoS events), transport (21% out of DDoS events), banking (12% out of DDoS events) and digital infrastructure (6% out of DDoS events).

These are followed by ransomware attacks and data-related threats. Ransomware appears to target different sectors indiscriminately during this reporting period, with Business services (18% out of ransomware events), Manufacturing (17% out of ransomware events) and Health (8% out of ransomware events) being more affected. Data related threats targeted all sectors, with the ones that hold personal information being more affected. Out of data related events, these affected general public (15%), public administration (12%), digital infrastructure (10%), finance (9%) and business services (8%).

29% of the events involving malware affected the general public, followed by malware infections in digital infrastructure (25%) and in public administration (11%). 9% of observed malware events affects all sectors.

Out of the observed events related to social engineering, 28% focused on the general public, followed by digital infrastructure (15%), public administration (10%) and finance (10%) sectors. Likewise, information manipulation campaigns targeted general public in most of the collected events.

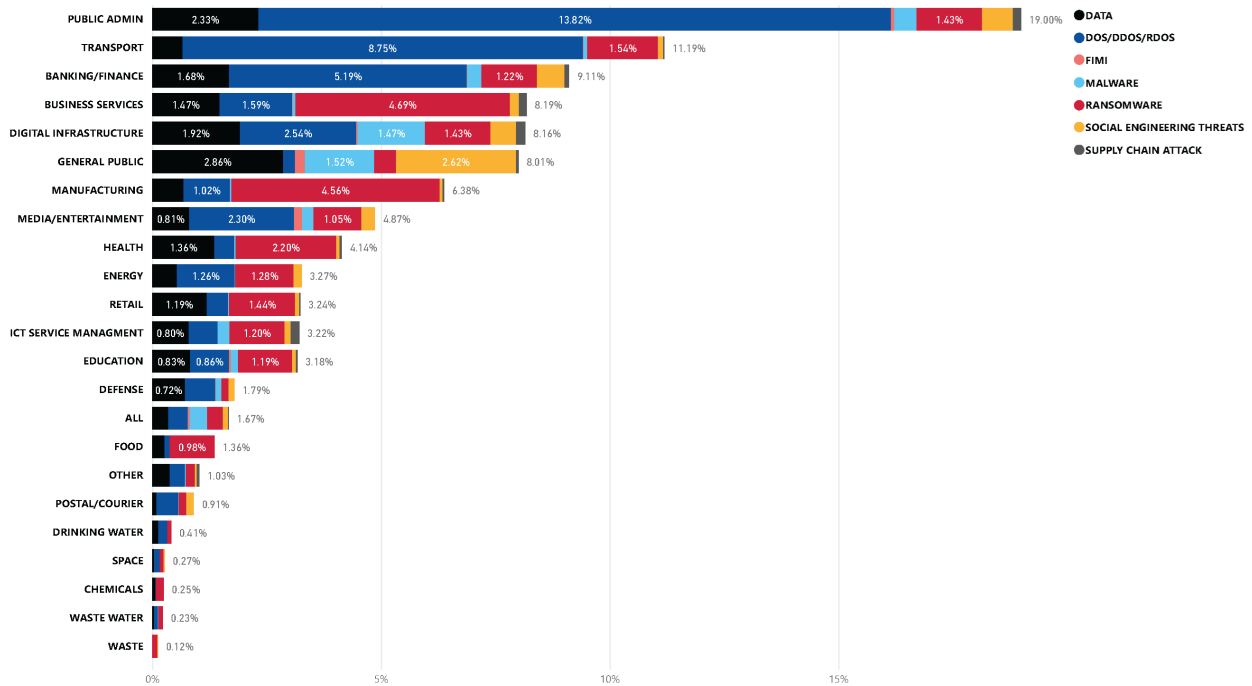
Figure 7: Observed events related to prime ETL threats in terms of the affected sectors



More information on how each sector is affected during the reporting can be found in the following figure.

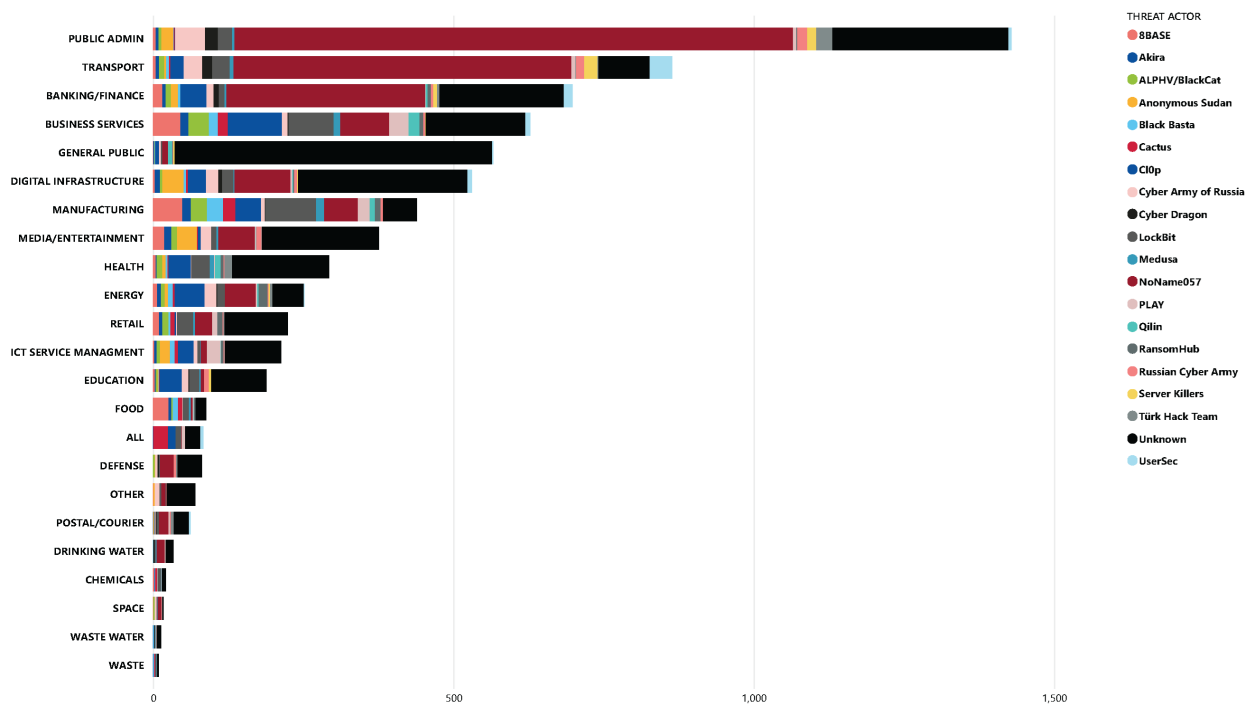


Figure 8: ETL threats per sector



In the breakdown of the top 20 'active' threat actors during the reporting period, the trend that actors are often sector-agnostic becomes evident once more, as nearly all of them are dispersed across various sectors. Similarly to 2023, public administration and transport remains a preference by the active Hacktivists groups.

Figure 9 Threat actor per sector



1.7 MOTIVATION

Understanding the enemy and the motivation behind a cybersecurity incident or targeted attack is important because it can determine what an adversary is after. Assessing the motives provides an idea of the intentions of attackers and helps entities focus their efforts in defence on the most likely attack scenario for any particular asset.

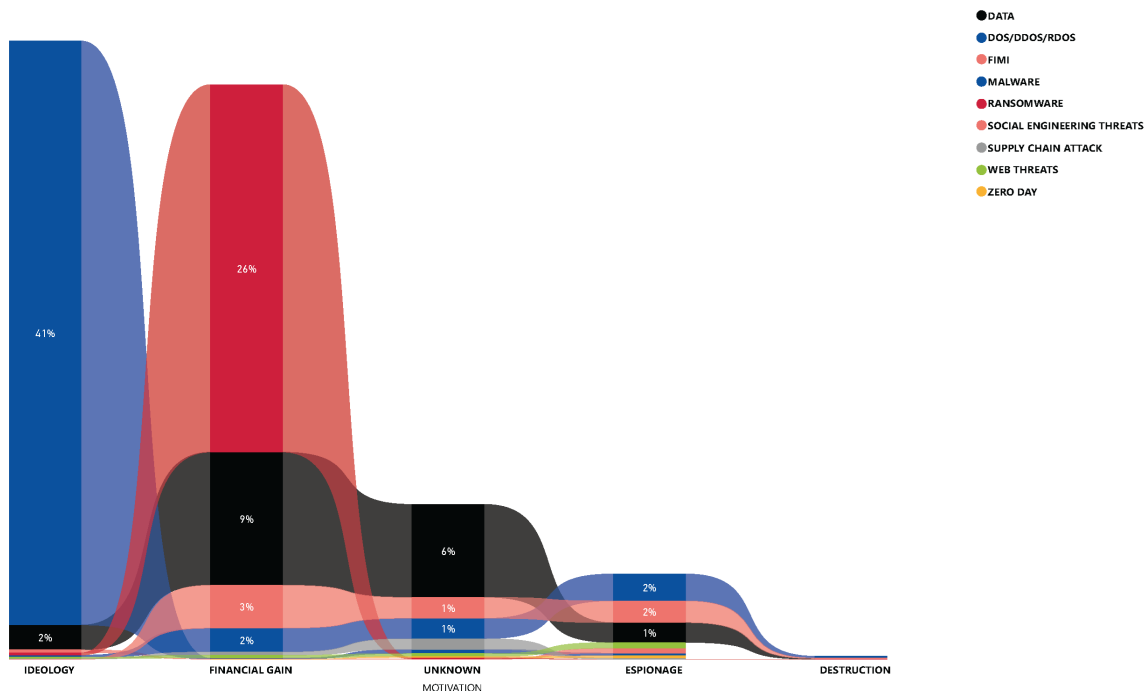
For the third year ETL 2024 includes an assessment of the motivation behind the incidents observed during the reporting period. For this purpose, five distinct kinds of motivation that can be linked to threat actors have been defined:

- **Financial gain:** any financially related action (carried out mostly by cybercrime groups);
- **Espionage:** gaining information on IP (intellectual property), sensitive data, classified data (mostly executed by state-sponsored groups);
- **Destruction:** any destructive action that could have irreversible consequences;
- **Ideological:** any action backed up with an ideology behind it (such as hacktivism).

It is apparent that in the majority of cases the primary threats can be attributed to one or more motivations, with certain motivations emerging as more dominant than others. As with the previous iteration within the realm of Ransomware attacks, while the primary motivation typically revolves around financial gain, there is a small percentage where a disruptive motive also plays a role.

Following financial gain as the top motivation, disruption was the second most common motive, primarily due to the prevalence of DDoS attacks during the reporting period. These disruptive attacks were aimed at causing operational downtime.

Figure 10: Motivation of threat actors per threat category



Additionally, most data-related threats were linked to multiple motivations, with financial gain being the primary driver. Ideology and espionage also played significant roles, as attackers sought to advance specific agendas or exfiltrate strategic information. This highlights the



diverse motivations behind cyber threats, ranging from financial incentives to ideological and intelligence-gathering objectives.

For a considerable number of the events we have gathered, the motivation remains unclear. This lack of clarity could be due to either limited or undisclosed information or the victims themselves being unaware of the underlying motive.

1.8 STRUCTURE OF THE REPORT

The ENISA Threat Landscape (ETL) 2024 has maintained the core structure of previous ETL reports for highlighting the prime cybersecurity threats in 2023. Those familiar with previous versions will observe that the current editions now incorporate the CVE landscape within chapters that offer an overview of the most significant CVEs identified during the reporting period. ENISA considers this inclusion to be crucial because it sheds light on yet another facet of what threat actors can exploit, as highlighted in Chapter 3. This addition also underscores the significance of vulnerability disclosure and timely patching.

This report is structured as follows:

- Chapter 2** explores the trends related to threat actors (i.e., state-nexus groups, cybercrime actors, Private Sector Offensive Actors (PSOA) and hacktivists);
- Chapter 3** includes a CVE landscape, as observed during the reporting period;
- Chapter 4** discusses major findings, incidents and trends regarding ransomware;
- Chapter 5** presents major findings, incidents and trends regarding malware;
- Chapter 6** describes major findings, incidents and trends regarding social engineering;
- Chapter 7** highlights major findings, incidents and trends regarding threats against data (data breach, data leak);
- Chapter 8** discusses major findings, incidents and trends regarding threats against availability (denial of service);
- Chapter 9** underlines the importance of hybrid threats and describes major findings, incidents and trends regarding information manipulation;
- Annex A** presents the techniques commonly used for each threat, based on the MITRE ATT&CK® framework;
- Annex B** presents recommendations and security controls that might add to the mitigation of the threats.





2. THREAT ACTOR TRENDS

Cyber threat actors are an integral component of the threat landscape. They are entities carrying out malicious activities. Understanding how threat actors's assessed objectives and Tactis, Techniques and Procedures (TTPs) is essential for a more robust cyber threat management and incident response.

In this section, we explore the trends related to threat actors. This assessment does not provide an exhaustive list of all trends during the reporting period but rather a overview of the significant trends observed at a strategic level. We focus on the motives of threat actors, their impact, and targeting. Their evolution is also assessed. For the ETL 2024, we consider once more the following four categories of cybersecurity threat actors:

- **State-nexus** actors;
- **Cybercrime** actors and **hacker-for-hire** actors ;
- **Private Sector Offensive** actors (PSOA);
- **Hacktivists**.

State-nexus actors, are in general well-funded, resourced and advanced. Their objective is primarily espionage and disruption, sometimes directed by the military, intelligence or state control apparatus of their country. And although the techniques they employ might not always be that novel, their motivation and planning allow them to execute advanced, large-scale or targeted and long-term operations. State-nexus actors often spend considerable time investigating their targets to identify weaknesses and entry points and they focus on avoiding operational mistakes. State-nexus actors do not only target other states. They can as well target other organisations for sensitive data or conduct operations to obtain funding for their country.

The objective of **cybercrime** actors is financial gain or profits in general. Their attacks are opportunistic and indiscriminate and they target the data or infrastructure that has the highest impact on the operations of victims. They can either steal directly from victims, can extort the victim or can monetise the information stolen from victims. Cybercrime actors often use social engineering and employ multiple different methods for monetising their access into organisations. In addition, cybercrime actors have shown an increased level of collaboration and professionalisation, making them a force with which to be reckoned.

Under cybercrime actors we can also observe the **hacker-for-hire** actors which contribute to the professionalisation of the cybercrime market, but also provide services to State-nexus actors. The hacker-for-hire actors can lower the barrier to get access to the criminal market, such as for example with ransomware-as-a-service or RaaS. They also play a key role in the market that thrives on selling access to environments (so called Initial Access Brokers or IAB), either because the threat actor is tasked or because of opportunistic reasons. The hacker-for-hire threat actor is also available for vulnerability research and exploitation.

In regards to **Private Sector Offensive Actors (PSOAs)**, are commercial entities that engage in the cyber-surveillance industry. They specialize in developing and selling cyberweapons, including "zero-day" exploits and malicious software, to a variety of clients, often governments and private individuals. They are a growing concern in the cybersecurity landscape due to their ability to provide advanced cyber capabilities to a wide range of clients, potentially leading to serious consequences for individuals, organizations, and societies.

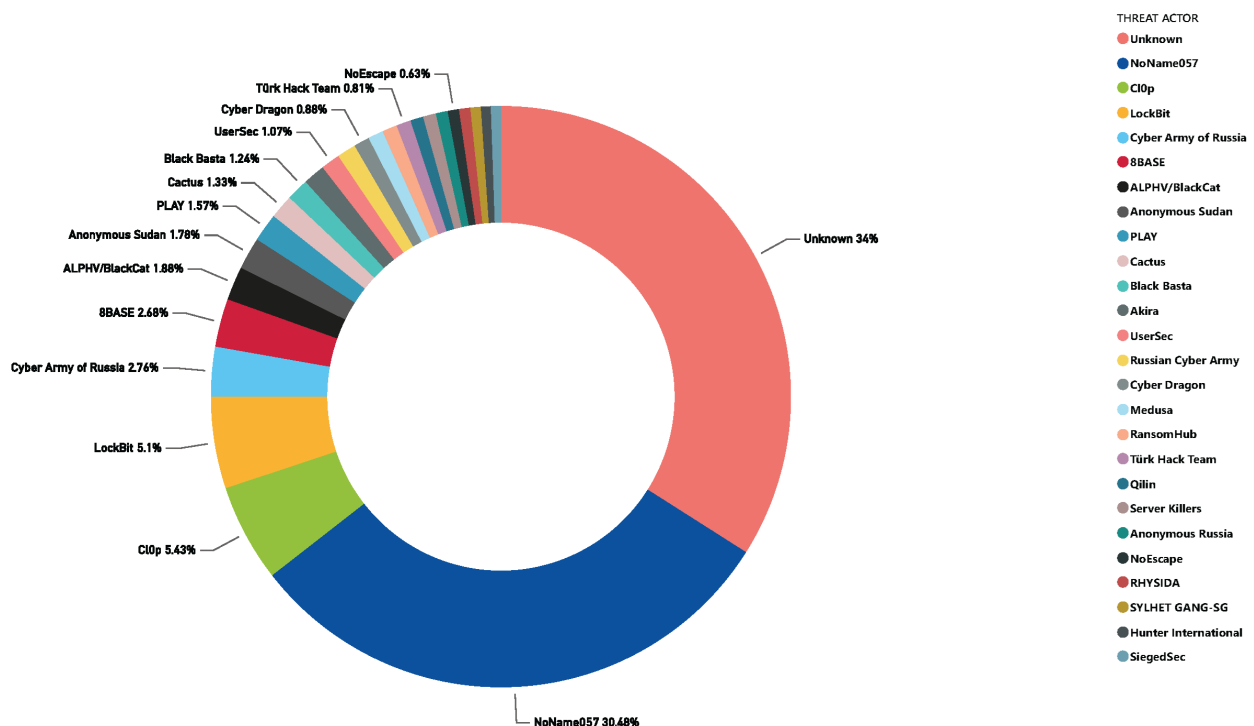


Lastly, we cover the **hacktivists**. Hacktivists are not as well-resourced as the other threat actors but are often fuelled by strong motivations. Their objectives often involve disruption and they use hacking to affect some form of political or social change. The hacktivists groups are very diverse and vary heavily in skillsets and capabilities. The hacktivists threat actors are sometimes also leveraged by State-nexus actors for influence operations or other forms of intrusion campaigns.

As an attentive reader you probably noticed we did not include the **insider threat actor** as one of the prime threat actors in this ETL. We excluded this threat actor because of the very low number of public reporting of incidents³². Despite the fact that there are programs that highlight the need to focus on insider threat mitigation^{33,34}, **organisations remain reluctant in sharing details** of these incidents. This does not imply that the risk of a malicious insider is deemed of lesser significance. On the contrary, insiders remain an efficient way for gaining access to the internals of an organisation, and as such they are sometimes used -knowingly or unknowingly- by State-nexus or cybercrime actors for initial access into a victim’s environment. It is relevant to highlight that human errors or carelessness constitute a portion of incidents considered as ‘insider threats’.

Over the course of the reporting period, we have pinpointed the 25 most active threat actors overall from the data we collected. It is worth highlighting that a significant majority of the events we gathered have not been attributed to any specific threat actor, which underscores the challenges associated with accurate political attribution. Hacktivist group NoName057 has also been very active during the reporting period followed by the ransomware group CI0p.

Figure 11: 25 Most active Threat actors during the reporting period



2.1 STATE-NEXUS GROUP TRENDS

Avoiding detection at all costs

³² According to CIRAS, the Cybersecurity Incident Reporting and Analysis System, 13% of the reported incidents in 2023 and 2024 are ‘human errors’ <https://ciras.enisa.europa.eu/>

³³ ; [Managing Insider Threats | Publication | National Cyber Security Centre \(ncsc.nl\)](#)

³⁴ CISA Insider Threat Mitigation <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation>



One of the most significant trends observed in campaigns of State-nexus threat actors are their methods³⁵ to **avoid detection** and sidestepping organisational defences. They increasingly employ³⁶ ³⁷ Living Off the Land (LOTL) techniques to minimise their footprint and rely³⁸ on remote monitoring and management (RMM) software. Although these techniques have been noted in previous reports, they have now surged to the forefront of prominent trends. Moreover, State-nexus actors are ³⁹ cleverly utilising tools that are ubiquitous across nearly all environments: **security tools** and their control panels. This not only facilitates stealthy malware deployment and lateral movements but also enables them to harvest detailed insights into an organisation's infrastructural vulnerabilities, all without raising much suspicion.

In general, State-nexus threat actors have always been increasingly adept⁴⁰ at **understanding the environments** they infiltrate. They strategically deploy tools and take their time to conduct thorough **reconnaissance** and skilfully prevent the detection and analysis of their implants by employing⁴¹ ⁴² ⁴³ robust anti-forensic measures. Predominantly, actors from Russia and Iran ⁴⁴ ⁴⁵ continue to deploy disruptive malware such as wipers not only to wreak havoc but also as an extremely effective method to **cover their tracks**. Given the effectiveness of these techniques and the significant advancements in the detection and response capabilities of organisations, it is very likely that State-nexus actors will further intensify their use of these strategies.

The effort to remain undetected, while simultaneously complicating attribution, is also evident in the operational infrastructure of threat actors, where they employ⁴⁶ a mix of **self-registered** and **compromised** infrastructure. This infrastructure is not only shared among various groups but is also used⁴⁷ by both State-nexus and cybercrime actors. To further obfuscate their activities, they are increasingly adopting⁴⁸ network anonymising techniques such as commercial VPNs, TOR, and proxy software. Moreover, there's a marked increase in the use of compromised devices within **residential networks**, often orchestrating them into **botnets**⁴⁹. China-nexus actors especially relied⁵⁰ on a mix of self-registered and compromised networks, referred to as Operational Relay Box (**ORB**) networks.

The broad adoption introduces new complexities for defenders, including the increased ephemerality and temporality of indicators. We expect this trend in operational infrastructure, predominately undertaken by China and Russia-nexus groups, is likely to continue in the coming years.

Leveraging cloud services for stealth and strategy

The theme of stealth extends into the cloud, where State-nexus actors use trusted sites and legitimate cloud services to evade detection, so called **Living Off Trusted Sites** (LOTS). They

³⁵ Mandiant - M-Trends 2024 - <https://www.mandiant.com/m-trends>.

³⁶ CISA - PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

³⁷ Mandiant - The GRU's Disruptive Playbook - <https://www.mandiant.com/resources/blog/gru-disruptive-playbook>.

³⁸ Recorded Future - Adversary Infrastructure - <https://www.recordedfuture.com/2023-adversary-infrastructure-report>.

³⁹ Picus Security - Picus Red Report 2024 - <https://www.picussecurity.com/resource/report/picus-red-report-2024>.

⁴⁰ CrowdStrike - Global threat report - <https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf>.

⁴¹ Mandiant - Active North Korean campaign targeting security researchers. <https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/>.

⁴² Trend Micro - Earth Freybug Uses UNAPIMON for Unhooking Critical APIs -

https://www.trendmicro.com/en_us/research/24/d/earth-freybug.html.

⁴³ Cisco - ArcaneDoor - New espionage-focused campaign - <https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/>.

⁴⁴ Palo Alto - Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors -

<https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/>.

⁴⁵ Mandiant - The GRU's Disruptive Playbook - <https://www.mandiant.com/resources/blog/gru-disruptive-playbook>.

⁴⁶ Recorded Future - Adversary Infrastructure - <https://www.recordedfuture.com/2023-adversary-infrastructure-report>.

⁴⁷ Trend Micro - Router Roulette - https://www.trendmicro.com/en_us/research/24/e/router-roulette.html.

⁴⁸ ANSSI - <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf>.

⁴⁹ CISA - PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

⁵⁰ Mandiant - IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders - <https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks/>.



disguise^{51 52 53} command and control communications (**C2**) as ordinary Microsoft traffic or as innocuous messages to platforms like Slack and Telegram. Services⁵⁴ such as Google Drive and OneDrive are exploited for **data exfiltration** and **malware storage**. GitHub has become⁵⁵ a particular favourite, serving as a hub for payload delivery, acting as a dead drop, command and control communication, and for facilitating data exfiltration. These actors are increasingly harnessing API services to achieve their objectives, including reconnaissance and data exfiltration, making use⁵⁶ of free APIs like mockbin.org and mocky.io. Groups linked to Russia and Iran have shown an interest in APIs associated with Microsoft services⁵⁷, such as the Microsoft Graph API.

State-nexus actors have not confined themselves to merely using cloud services for evasive manoeuvres; they⁵⁸ also **directly target these services** on two levels: by compromising hosts within a cloud tenant and by targeting **identities** associated with cloud infrastructure.

Targeting identities

It is hardly surprising that State-nexus actors maintain a keen interest in attacks targeting identities and **credentials**. They harness^{59 60 61 62} credentials from previous breaches, employ password spraying and brute force attacks, or reactivate dormant accounts. When direct access to credentials is not at hand, these actors resort^{63 64} to **social engineering** tactics. **Phishing** remains their preferred method, while refining their strategies by leveraging social media, Microsoft Teams, compromised tenants and popular email marketing platforms. To circumvent corporate defences, they increasingly turn⁶⁵ to social media and **communication platforms** such as WhatsApp or LinkedIn. **Personal accounts**, typically less secure than corporate ones, are especially vulnerable. We also observed **an increase in targeting precision**, sometimes via geofencing or web beacons, and it is likely this approach will further continue.

Exploiting vulnerabilities and edge devices

Exploiting vulnerabilities remains a favoured tactic for State-nexus actors to infiltrate organisations. As end-user platform vendors invest significantly in security, attackers shift their focus to other environments, highlighting the impact⁶⁶ of these investments. However, this does not mean end-user platforms are off the radar. Vulnerabilities in software^{67 68} such as Outlook, continue to be exploited for executing arbitrary code. In general, the number of known

⁵¹ Palo Alto - Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific -

<https://unit42.paloaltonetworks.com/stately-aurus-targets-philippines-government-cyberespionage/>.

⁵² Mandiant - Backchannel Diplomacy: APT29's Rapidly Evolving Diplomatic Phishing Operations -

<https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing>.

⁵³ Cisco - Operation Blacksmith: Lazarus targets organizations worldwide using novel Telegram-based malware written in

DLang - https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/.

⁵⁴ Symantec - Growing number of threats leveraging Microsoft API - [https://symantec-enterprise-](https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/graph-api-threats)

[blogs.security.com/blogs/threat-intelligence/graph-api-threats](https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/graph-api-threats).

⁵⁵ Recorded Future - Flying Under the Radar: Abusing GitHub for Malicious Infrastructure -

<https://www.recordedfuture.com/flying-under-the-radar-abusing-github-malicious-infrastructure>.

⁵⁶ CERT.pl - APT28 campaign targeting Polish government institutions - <https://cert.pl/en/posts/2024/05/apt28-campaign/>.

⁵⁷ ESET - OilRig's persistent attacks using cloud service-powered downloaders - [https://www.welivesecurity.com/en/eset-](https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/)

[research/oilrig-persistent-attacks-cloud-service-powered-downloaders/](https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/).

⁵⁸ CrowdStrike - Global threat report - <https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf>.

⁵⁹ CISA - Compromised Account of Former Employee to Access State Government Organization -

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-046a>.

⁶⁰ Microsoft - Iranian hackers breach defense orgs - [https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-](https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/)

[sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/](https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/).

⁶¹ Trend Micro - Pawn Storm Uses Brute Force and Stealth Against High-Value Targets -

https://www.trendmicro.com/en_in/research/24/a/pawn-storm-uses-brute-force-and-stealth.html.

⁶² CISA - SVR Cyber Actors Adapt Tactics for Initial Cloud Access - [https://www.cisa.gov/news-events/cybersecurity-](https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a)

[advisories/aa24-057a](https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a).

⁶³ NCSC UK - SVR cyber actors adapt tactics for initial cloud access - [https://www.ncsc.gov.uk/files/Advisory-SVR-cyber-](https://www.ncsc.gov.uk/files/Advisory-SVR-cyber-actors-adapt-tactics-for-initial-cloud-access.pdf)

[actors-adapt-tactics-for-initial-cloud-access.pdf](https://www.ncsc.gov.uk/files/Advisory-SVR-cyber-actors-adapt-tactics-for-initial-cloud-access.pdf).

⁶⁴ Microsoft - Midnight Blizzard conducts targeted social engineering over Microsoft Teams - [https://www.microsoft.com/en-](https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/)

[us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/](https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/).

⁶⁵ Genians - Kimsuky APT attack discovered using Facebook & MS management console -

https://www.genians.co.kr/blog/threat_intelligence/facebook.

⁶⁶ Google - A review of zero-day in-the-wild exploits in 2023 - [https://blog.google/technology/safety-security/a-review-of-](https://blog.google/technology/safety-security/a-review-of-zero-day-in-the-wild-exploits-in-2023/)

[zero-day-in-the-wild-exploits-in-2023/](https://blog.google/technology/safety-security/a-review-of-zero-day-in-the-wild-exploits-in-2023/).

⁶⁷ Palo Alto - Fighting Ursa Aka APT28: Illuminating a Covert Campaign - [https://unit42.paloaltonetworks.com/russian-apt-](https://unit42.paloaltonetworks.com/russian-apt-fighting-ursa-exploits-cve-2023-233397/)

[fighting-ursa-exploits-cve-2023-233397/](https://unit42.paloaltonetworks.com/russian-apt-fighting-ursa-exploits-cve-2023-233397/).

⁶⁸ Mandiant - Government-backed actors exploiting WinRAR vulnerability - [https://blog.google/threat-analysis-](https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winar-vulnerability/)

[group/government-backed-actors-exploiting-winar-vulnerability/](https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winar-vulnerability/).



vulnerabilities is increasing, as shown in chapter 3. Although this doesn't precisely track zero-day exploits, it still serves as a valuable indicator of trends. Chinese groups lead the charge in exploiting vulnerabilities, heavily investing in zero-day exploits and occasionally collaborating⁶⁹ with **commercial** surveillance vendors to enhance their capabilities.

Edge devices, used for networking and security, remain a lucrative^{70 71} entry point. Access via these devices is popular because of^{72 73} security on the many number of issues found in these devices, and devices often rely on legacy components. Additionally, the lack of security monitoring makes them easy prey. Products such as Ivanti Connect Secure, Cisco or FortiGate were prime targets for State-nexus activity. Actors also **anticipate**⁷⁴ **remediation** efforts and create tools to remain embedded in high-value targets by installing backdoors⁷⁵ on routers or modifying firmware⁷⁶. **Virtualisation**^{77 78} technology and hypervisors, remain lucrative targets as well. **Public applications** continue to be a prime target for actors operating in the interests of China, North Korea, and Iran. Their main focus^{79 80 81} includes web applications such as e-commerce platforms, collaboration tools and service desk software, alongside lingering vulnerabilities in Log4J, and SQL and Java applications. A notable example^{82 83} is the exploitation of RMM software, such as ScreenConnect, which has become a feast for both State-nexus actors and cybercriminals. Another notable example was the COATHANGER-campaign where State-nexus actors exploited vulnerability affecting FortiGate devices to conduct espionage activities⁸⁴.

Given the sheer volume of vulnerabilities and the challenges vendors face in addressing them, coupled with the complexity for large organisations to organise timely patching, it is highly likely that exploiting vulnerabilities will continue to be one of the main entry points for State-nexus actors.

Misinformation, disinformation and foreign interference

The **sharp rise**^{85 86 87} in reported **misinformation and disinformation campaigns is concerning**. The role of technology in these campaigns remains highly significant^{88 89 90}, as

⁶⁹ Mandiant - M-Trends 2024 - <https://www.mandiant.com/m-trends>.

⁷⁰ NCSC NL - MIVD AIVD Advisory COATHANGER - <https://www.ncsc.nl/documenten/publicaties/2024/februari/6/mivd-aidv-advisory-coathanger-ttp-clear>.

⁷¹ ANSSI - <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf>.

⁷² ENISA - Joint Statement on Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities - <https://www.enisa.europa.eu/news/joint-statement-on-ivanti>.

⁷³ CISA - Supplemental Direction V1: ED 24-01 - <https://www.cisa.gov/news-events/directives/supplemental-direction-v1-ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure>.

⁷⁴ Mandiant - Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868) - <https://www.mandiant.com/resources/blog/unc4841-post-barracuda-zero-day-remediation>.

⁷⁵ Cisco - ArcaneDoor - New espionage-focused campaign - <https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/>.

⁷⁶ CISA - People's Republic of China-Linked Cyber Actors Hide in Router Firmware - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a>.

⁷⁷ Mandiant - Chinese Espionage Group UNC3886 Found Exploiting CVE-2023-34048 Since Late 2021 - <https://www.mandiant.com/resources/blog/chinese-vmware-exploitation-since-2021>.

⁷⁸ MITRE - Technical Deep Dive: Understanding the Anatomy of a Cyber Intrusion - <https://medium.com/mitre-engenuity/technical-deep-dive-understanding-the-anatomy-of-a-cyber-intrusion-080bddc679f3>.

⁷⁹ Palo Alto - Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors - <https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/>.

⁸⁰ Cisco - Lazarus Group exploits ManageEngine vulnerability to deploy QuiterAT - <https://blog.talosintelligence.com/lazarus-quiterat/>.

⁸¹ Microsoft - Flax Typhoon using legitimate software to quietly access Taiwanese organizations - <https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/>.

⁸² ZScaler - Multiple Vulnerabilities Found In ConnectWise ScreenConnect - <https://www.zscaler.com/blogs/security-research/multiple-vulnerabilities-found-connectwise-screenconnect>.

⁸³ Kröll - TODDLERSHARK: ScreenConnect Vulnerability Exploited to Deploy BABYSHARK Variant - <https://www.kroll.com/en/insights/publications/cyber/screenconnect-vulnerability-exploited-to-deploy-babyspark>.

⁸⁴ <https://www.ncsc.nl> Ongoing state-sponsored cyber espionage campaign via vulnerable edge devices | News item | National Cyber Security Centre (ncsc.nl)

⁸⁵ Checkpoint - Elections Spotlight: Generative AI and Deep Fakes - <https://research.checkpoint.com/2023/elections-spotlight-generative-ai-and-deep-fakes/>.

⁸⁶ Cyberark - Election Security - <https://www.cyberark.com/resources/blog/election-security-defending-democracy-in-todays-dynamic-cyber-threat-landscape>.

⁸⁷ BlackBerry - Threat Intelligence Report - <https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report>.

⁸⁸ Sekoia - Master of Puppets: Uncovering the DoppelGänger pro-Russian influence campaign - <https://blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign/>.

⁸⁹ DNI - Threat Assessment - <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>.

⁹⁰ TBIJ - What are influence operations? - <https://www.thebureauinvestigates.com/stories/2023-07-27/what-are-influence-operations-and-why-are-we-investigating-them/>.



many are amplified through **social media platforms** like X, Facebook, and **video hosting services** such as Instagram, TikTok, and YouTube. Additionally, broadcasted real-time bidding (RTB) data provides opportunities⁹¹ for State-nexus actors to target key individuals. While social media platforms have begun addressing these issues, sometimes reluctantly, there is still a **substantial amount of work to be done**. Notable campaigns were Doppelgänger⁹² and Portal Kombat⁹³ (in favour of Russia) and PAPERWALL⁹⁴ (in favour of China).

As campaigns linked to geopolitical events continue to evolve, along with an increase in social engineering, it is almost certain that State-nexus actors will further expand this trend as an effective means to further achieve their objectives.

Threat actors leveraging artificial intelligence as an assistant

Recent observations^{95 96} reveal that large language models (LLMs) such as ChatGPT^{97 98} are employed by Russian, North Korean, Iranian, and Chinese State-nexus groups. They use AI for a variety of malicious activities including scripting and phishing assistance, vulnerability research and target reconnaissance. The principal danger **lies not in entirely new risks**, but rather in AI's capacity to enhance existing techniques, allowing for the **massive** distribution^{99 100} of fake, targeted narratives, including social media posts, articles, memes, and photos. We have already witnessed its capabilities with doctored recordings of a candidate alleging¹⁰¹ election rigging or endorsing¹⁰² another presidential candidate.

2.2 CYBERCRIME ACTOR TRENDS

Advances in defensive evasion techniques

Cybercrime groups refined their **evasion techniques** to blend seamlessly into environments. These criminals, for the most part ransomware operators, use^{103 104} Living Off The Land (LOTL) strategies and rely^{105 106} on remote monitoring and management (RMM) software such as AnyDesk and Atera to mask their activities. In their efforts to blend in, the adoption of **commodity** tools, **dual-use** software, and **open-source** software remains significant. They predominantly use^{107 108} Cobalt Strike, Viper, BloodHound, and Impacket. The emergence¹⁰⁹ of

⁹¹ ICCL - Europe's hidden security crisis - <https://www.iccl.ie/2023/new-iccl-reports-reveal-serious-security-threat-to-the-eu-and-us/>.

⁹² AP - France accuses Russia of a disinformation campaign in a key election year - <https://apnews.com/article/france-russia-disinformation-campaign-websites-96de49e381cfa357fcd6d0e7d8ff1e48>.

⁹³ VIGINUM – Portal Kombat - https://www.sqdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf.

⁹⁴ CitizenLab - Outlets Target Global Audiences with Pro-Beijing Content - <https://citizenlab.ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/>.

⁹⁵ Gartner - Alarm Over GenAI Risk Fuels Security Spending in Middle East & Africa - <https://www.gartner.com/en/newsroom/press-releases/2024-02-13-gartner-forecasts-security-and-risk-management-spending-in-mena-to-grow-12-percent-in-2024>.

⁹⁶ NCSC - The near-term impact of AI on the cyber threat - <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>

⁹⁷ OpenAI - Disrupting malicious uses of AI by state-affiliated threat actors - <https://openai.com/blog/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors>.

⁹⁸ Microsoft - Staying ahead of threat actors in the age of AI - <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/>.

⁹⁹ Checkpoint - Elections Spotlight: Generative AI and Deep Fakes - <https://research.checkpoint.com/2023/elections-spotlight-generative-ai-and-deep-fakes/>.

¹⁰⁰ BlackBerry - Threat Intelligence Report - <https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report>.

¹⁰¹ CNN - A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning - <https://edition.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html>.

¹⁰² Microsoft - China tests US voter fault lines and ramps AI content to boost its geopolitical interests - <https://blogs.microsoft.com/on-the-issues/2024/04/china-ai-influence-elections-mtac-cybersecurity/>.

¹⁰³ Trend Micro - Kasseika Ransomware Deploys BYOVD Attacks, Abuses PsExec and Exploits Martini Driver - https://www.trendmicro.com/en_us/research/24/a/kasseika-ransomware-deploys-byovd-attacks-abuses-psexec-and-expl.html.

¹⁰⁴ Cisco - Medusa Ransomware Turning Your Files into Stone - <https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/>.

¹⁰⁵ Why ransomware gangs love using RMM tools and how to stop them - <https://www.malwarebytes.com/blog/business/2024/02/why-ransomware-gangs-love-using-rmm-tools-and-how-to-stop-them>.

¹⁰⁶ Microsoft - Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction - <https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/>.

¹⁰⁷ Recorded Future - Adversary Infrastructure - <https://www.recordedfuture.com/2023-adversary-infrastructure-report>.

¹⁰⁸ Mandiant - Malware Trends: Yearly 2023 - <https://blog.unpac.me/2024/01/30/malware-trends-yearly/>.

¹⁰⁹ Mandiant - Mandiant M-Trends 2024 - <https://www.mandiant.com/m-trends>.



AzureHound, Pacu, and CloudFox underscores a growing trend towards exploiting cloud services. Popular open-source software was^{110 111 112}

Public reports also reveal that criminals either opt^{113 114} for **speed**, indiscriminately grabbing¹¹⁵ data, or adopt¹¹⁶ a more **targeted** approach with keyword searches for sensitive files such as financial documents, confidential information, and stores of credentials. This is often enhanced¹¹⁷ with hands-on or **interactive intrusion** techniques. These methods mimic typical user behaviour, making it challenging for defenders to distinguish between legitimate user activity and a cyber-attack.

It is very likely that cybercriminals will further continue to expand their use of these techniques to evade defensive measures.

Anonymisation networks to hide traffic

Continuing with the theme of stealth, cybercriminals used **anonymisation networks** and large **botnets composed of compromised residential devices**. These botnets^{118 119} are frequently used for DDoS attacks, cryptocurrency mining, and malware distribution.

Often, **multiple groups** compromise¹²⁰ these devices, leading to situations within the network infrastructure. The use of **proxyware** networks is further expanding^{121 122 123} and incorporating mobile devices and macOS systems. While these networks serve legitimate purposes, there is an increasing trend in their misuse for malicious and illegal activities.

Zero-day and one-day vulnerabilities

As way of easy entry into organisations, financially motivated actors increasingly relied on **exploiting**^{124 125} zero-day and one-day **vulnerabilities** to infiltrate systems and steal valuable data. While zero-day vulnerabilities pose a significant threat, cybercriminals often focus on a smaller subset of one-day vulnerabilities. This preference stems from the established attack paths of one-day vulnerabilities and the relative **shortage of zero-days either for sale on cybercrime forums or in general announced by vendors or found by researchers**. This trend underscores that effective and prioritised¹²⁶ patching could be likely to prevent a large number of incidents or at least make them considerably more challenging to execute. However, numerous challenges still hinder organisations and suppliers from achieving this level of security.

¹¹⁰ Microsoft - Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction -

<https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/>.

¹¹¹ Palo Alto - Diving Into Glupteba's UEFI Bootkit <https://unit42.paloaltonetworks.com/glupteba-malware-uefi-bootkit>

¹¹² <https://github.com/Mattiwatti/EfiGuard>.

¹¹³ CrowdStrike - Threat Hunting Report - <https://www.crowdstrike.com/resources/reports/threat-hunting-report/>.

¹¹⁴ ACS - Cyber criminals are getting faster - <https://ia.acs.org.au/article/2023/cyber-criminals-are-getting-faster.html>

¹¹⁵ ESET - A year in review: 10 of the biggest security incidents of 2023 -

<https://www.welivesecurity.com/en/cybersecurity/year-review-10-biggest-security-incidents-2023/>.

¹¹⁶ Mandiant - Ransomware Rebounds: Extortion Threat Surges in 2023 - <https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools/>.

¹¹⁷ CrowdStrike - Global threat report - <https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf>.

¹¹⁸ Lumen - The Darkside of TheMoon - <https://blog.lumen.com/the-darkside-of-themoon/>.

¹¹⁹ Fortinet - New Goldoon Botnet Targeting D-Link Devices by Exploiting 9-Year-Old Flaw -

<https://www.fortinet.com/blog/threat-research/new-goldoon-botnet-targeting-d-link-devices>.

¹²⁰ Trend Micro - Router Roulette - https://www.trendmicro.com/en_us/research/24/e/router-roulette.html.

¹²¹ Okta - Credential-Stuffing Attacks Spike via Proxy Networks <https://sec.okta.com/blockanonymizers>.

¹²² Human - PROXYLIB and LumiApps - <https://www.humansecurity.com/learn/blog/satori-threat-intelligence-alert-proxylib-and-lumiapps-transform-mobile-devices-into-proxy-nodes>.

¹²³ ATT - Mac systems turned into proxy exit nodes by AdLoad - <https://cybersecurity.att.com/blogs/labs-research/mac-systems-turned-into-proxy-exit-nodes-by-adload>.

¹²⁴ Arctic Wolf Labs- Threat report 2023 - https://arcticwolf.com/resource/_pfcfn/assets/preprocessed/10926/4e9f02a5-641d-41f4-9d14-e264c0d9d4ea/4e9f02a5-641d-41f4-9d14-e264c0d9d4ea.pdf.

¹²⁵ Mandiant - Mandiant M-Trends 2024 - <https://www.mandiant.com/m-trends>.

¹²⁶ Flashpoint - Global Threat Intelligence Report - <https://go.flashpoint.io/2024-global-threat-intelligence-report-download>.



A persistent trend is the exploitation^{127 128} of vulnerabilities in **internet-facing** services such as web management systems, firewalls, VPNs and routers. Noteworthy examples include vulnerabilities in Ivanti Connect Secure, NetScaler, Fortinet devices and older¹²⁹ issues in MOVEit. Additionally, **misconfigured services**, such as unintentionally exposed Redis services or exploitable Remote Desktop Protocol (RDP), continue¹³⁰ to present significant risks.

In the context of internet-connected devices, it's relevant to note that, as of April, suppliers in the UK are prohibited¹³¹ from providing devices with easy guessable default passwords. This change is likely to have a positive impact on markets outside the UK as well.

Changes in social engineering

Identity compromises and the **misuse of valid credentials** are nearly ubiquitous in today's threat landscape. Alongside exploiting vulnerabilities, criminals prefer this **malware-free** access method^{132 133}, exploiting the increase¹³⁴ in **stolen data**, often sourced from information stealers. When direct breaches fail to yield credentials, they turn¹³⁵ to traditional brute-force tactics such as password spraying and credential stuffing or exploit easily guessable passwords. Moreover, the misuse^{136 137} of cloud-specific credentials has escalated, leading to **cloud account takeovers**, particularly within Microsoft Azure environments. The rise in identity-centric attacks parallels increases in social engineering campaigns, primarily through **phishing**. Cybercriminals use link staging and traffic filtering, often via **legitimate cloud services**, to hide their schemes. Social media, especially LinkedIn, serves¹³⁸ as fertile ground for crafting **targeted lures**. These campaigns have also expanded¹³⁹ into **areas with lower visibility** such as communication platforms. Despite the adoption of multi-factor authentication, such efforts are^{140 141} increasingly difficult to counter due to **Adversary-in-the-Middle** (AitM) techniques and tools like Evilginx. Cybercriminals are likely to further integrate these methods into their attack playbooks.

While ransomware often captures the headlines, this reporting period has seen a sharp increase^{142 143} in **Business Email Compromise** (BEC) incidents. BEC poses and will very likely remain a pervasive threat due to its effectiveness and simplicity in execution. These incidents are particularly challenging to detect because they seldom involve malware or other malicious activities that leave detectable traces of compromise.

The use^{144 145} of crypto drainers and QR¹⁴⁶, code phishing, or **Qishing**, has seen a significant surge. Tools like EvilGophish¹⁴⁷ streamline the creation of QR codes for use in social

¹²⁷ Checkpoint - Magnet Goblin Targets Publicly Facing Servers Using 1-Day Vulnerabilities -

<https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/>.

¹²⁸ FS-ISAC - LockBit: Access, Encryption, Exfiltration, & Mitigation - <https://www.fsisac.com/hubfs/Knowledge/LockBit-AccessEncryptionExfiltrationMitigation.pdf>.

¹²⁹ SentinelOne - MOVEit Transfer Vulnerability used to Drop File-Stealing SQL Shell -

<https://www.sentinelone.com/blog/moveit-transfer-exploited-to-drop-file-stealing-sql-shell/>.

¹³⁰ Ahnlab - Metasploit Meterpreter Installed via Redis Server - <https://asec.ahnlab.com/en/64034/>.

¹³¹ NCSC-UK - Smart devices - <https://www.ncsc.gov.uk/blog-post/smart-devices-law>.

¹³² Palo Alto - Incident Response Report -

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf.

¹³³ Proofpoint - The Concerning Rise in Identity-Centric Attacks: Trends and Facts -

<https://www.proofpoint.com/us/blog/identity-threat-defense/rise-in-identity-threats>.

¹³⁴ Flashpoint - Global Threat Intelligence Report - <https://go.flashpoint.io/2024-global-threat-intelligence-report-download>.

¹³⁵ Verizon - 2024 Data Breach Investigations Report - <https://www.verizon.com/business/resources/reports/dbir/>.

¹³⁶ Red Canary - Inside The 2024 Threat Detection Report - <https://redcanary.com/blog/2024-threat-detection-report/>.

¹³⁷ Proofpoint - Campaign Impacting Azure Cloud Environments - [https://www.proofpoint.com/uk/blog/cloud-](https://www.proofpoint.com/uk/blog/cloud-security/community-alert-ongoing-malicious-campaign-impacting-azure-cloud-environments)

[security/community-alert-ongoing-malicious-campaign-impacting-azure-cloud-environments](https://www.proofpoint.com/uk/blog/cloud-security/community-alert-ongoing-malicious-campaign-impacting-azure-cloud-environments).

¹³⁸ Mandiant - M-Trends 2024 - <https://www.mandiant.com/m-trends>.

¹³⁹ Cisco - CoralRaider targets victims' data and social media accounts - <https://blog.talosintelligence.com/coralraider-targets-socialmedia-accounts/>.

¹⁴⁰ Proofpoint - Cloud Account Takeover Campaign - <https://www.proofpoint.com/us/blog/email-and-cloud-threats/cloud-account-takeover-campaign-leveraging-evilproxy-targets-top-level>.

¹⁴¹ Mandiant - Mandiant M-Trends 2024 - <https://www.mandiant.com/m-trends>.

¹⁴² FBI - IC3 Report - https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf.

¹⁴³ Group IB - Hi-Tech crime trends - <https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-eu/>.

¹⁴⁴ Avast - Avast Q1/2024 Threat Report - <https://decoded.avast.io/threatresearch/avast-q1-2024-threat-report/>.

¹⁴⁵ Checkpoint - The Rising Threat of Phishing Attacks with Crypto Drainers - <https://research.checkpoint.com/2023/the-rising-threat-of-phishing-attacks-with-crypto-drainers/>.

¹⁴⁶ FS-ISAC - New Cyber Threats to Challenge Financial Services Sector in 2024 -

<https://www.fsisac.com/hubfs/Knowledge/NavigatingCyber/2024/FSISAC-NavCyber24-Report.pdf>.

¹⁴⁷ EvilGoPhish - <https://github.com/fin3ss3q0d/evilgophish?tab=readme-ov-file#qr-code-generator>.



engineering campaigns, making them a simple addition for security professionals and attackers alike. Meanwhile, SEO poisoning remains¹⁴⁸ lucrative as well, ensnaring users who search for legitimate documents or software.

Relying on cloud services

A prominent trend^{149 150} in cybercrime is the **use of legitimate cloud services** not just for orchestrating social engineering attacks but also for malware and data exfiltration. Although this strategy isn't new, its use has been ramped up significantly. This does not suggest a lack of security in these services but rather underscores the adaptability of threat actors. They show a keen interest^{151 152} in **document publishing platforms**, leveraging the trusted reputations of these sites. Additionally, they create^{153 154} subdomains or paths under popular social media and sharing services, or use well-known websites like Ars Technica, GitHub^{155 156} and Vimeo to host their payloads. Given their effectiveness and relatively low cost, it is highly likely this trend will continue in the foreseeable future.

Financially motivated attackers also demonstrate creativity^{157 158} by using Google Cloud Run for **malware distribution**, deploying Cloudflare Workers as reverse proxies for **phishing** or setting up their own **workloads** in cloud environments. These tactics blend seamlessly with standard IT operations, leaving the victim to bear the cost of the computing resources.

Targeting virtualisation environments

Virtualisation platforms have become pivotal to organisational IT infrastructures, but they can suffer from misconfigurations and vulnerabilities. Moreover, security teams frequently struggle with limited visibility within these platforms, making them prime targets for cybercriminals, especially^{159 160 161} **ransomware** gangs. These groups generally follow a consistent approach, regardless of the ransomware variant used. They gain initial access through social engineering or by exploiting vulnerabilities. Once inside, they delete or encrypt backup systems, exfiltrate data, launch the ransomware and then spread it beyond the virtual environment.

Furthermore, actors have been observed creating¹⁶² **snapshots** of virtual domain controller disks for offline credential extraction and using virtual **serial console** access or their own **virtual machines**^{163 164} within a victim's environment to evade detection. Additionally, they exploited¹⁶⁵ network tunnelling features of QEMU, a virtualisation platform, to maintain stealth.

¹⁴⁸ BlackBerry - Threat Intelligence Report - <https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report>.

¹⁴⁹ Group-IB - Hi-Tech Crime Trends - <https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-eu/>.

¹⁵⁰ Trend Micro - Threat Actors Leverage File-Sharing Service and Reverse Proxies for Credential Harvesting - https://www.trendmicro.com/en_us/research/23/k/threat-actors-leverage-file-sharing-service-and-reverse-proxies.html.

¹⁵¹ Cisco - Threat actors leverage document publishing sites for ongoing credential and session token theft

<https://blog.talosintelligence.com/threat-actors-leveraging-document-publishing-sites/>.

¹⁵² Palo Alto - Ransomware Delivery URLs - <https://unit42.paloaltonetworks.com/url-delivered-ransomware/>.

¹⁵³ Mandiant - Evolution of UNC4990: Uncovering USB Malware's Hidden Depths -

<https://www.mandiant.com/resources/blog/unc4990-evolution-usb-malware>.

¹⁵⁴ SentinelOne - Exploiting Repos | 6 Ways Threat Actors Abuse GitHub & Other DevOps Platforms -

<https://www.sentinelone.com/blog/exploiting-repos-6-ways-threat-actors-abuse-github-other-devops-platforms/>.

¹⁵⁵ Darkreading - Hackers Create Legit Phishing Links With Ghost GitHub, GitLab Comments -

<https://www.darkreading.com/threat-intelligence/hackers-create-legit-phishing-links-with-ghost-github-gitlab-comments>.

¹⁵⁶ McAfee - Redline Stealer: A Novel Approach - <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/>.

¹⁵⁷ Cisco - Astaroth, Mekotio & Ousaban abusing Google Cloud Run in LATAM-focused malware campaigns -

<https://blog.talosintelligence.com/google-cloud-run-abuse/>.

¹⁵⁸ Netskope - Phishing with Cloudflare Workers: Transparent Phishing and HTML Smuggling -

<https://www.netskope.com/blog/phishing-with-cloudflare-workers-transparent-phishing-and-html-smuggling>.

¹⁵⁹ Trend Micro - Agenda Ransomware Propagates to vCenters - https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html.

¹⁶⁰ CISA - StopRansomware: Akira Ransomware - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a>.

¹⁶¹ SentinelOne - From Conti to Akira | Decoding the Latest Linux & ESXi Ransomware Families -

<https://www.sentinelone.com/blog/from-conti-to-akira-decoding-the-latest-linux-esxi-ransomware-families/>.

¹⁶² Microsoft - Octo Tempest crosses boundaries - <https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/>.

¹⁶³ Palo Alto - BlackCat Climbs the Summit With a New Tactic - <https://unit42.paloaltonetworks.com/blackcat-ransomware-releases-new-utility-munchkin/>.

¹⁶⁴ Palo Alto - Incident Response Report -

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf.

¹⁶⁵ Network tunneling with... QEMU? - <https://securelist.com/network-tunneling-with-qemu/111803/>.



This exploitation of virtualisation technology demonstrates that cybercriminals have discovered their potential to maximise the **impact** of their campaigns and remain undetected, making these platforms likely targets of continued interest.

Adding creativity to extortion techniques

In general, double extortion shows no¹⁶⁶ ¹⁶⁷ signs of slowing down. Ransomware groups are also actively engaging¹⁶⁸ ¹⁶⁹ with the media and the public to shape the narrative around their activities. Some groups even shifted¹⁷⁰ from double extortion to **extorting without encryption**. Instead of encrypting data, they proceed directly to data theft. Additionally, affiliates are actively finding new ways to monetise¹⁷¹ ¹⁷² stolen data, sometimes by collaborating with third parties or external data leak services to **re-extort their victims**. Cybercrime gangs also noted¹⁷³ ¹⁷⁴ the implementation of **key legislation** in 2023 and are adjusting their tactics accordingly. They may likely **weaponize disclosure requirements**, pushing companies to fulfil extortion demands ahead of the required reporting deadline.

Actions by law enforcement agencies

High-profile arrests¹⁷⁵ ¹⁷⁶ and successful take-downs demonstrate a concerted effort to dismantle criminal networks by law enforcement agencies. Notably¹⁷⁷ ¹⁷⁸, Operation EndGame against the dropper ecosystem and **Operation Cronos** against LockBit, one of the largest ransomware groups, stood out, not least due to the tongue-in-cheek humour expressed by the participating agencies.

Artificial intelligence for the bad

It is no surprise that cybercriminals have embraced artificial intelligence, and not just as users. They targeted¹⁷⁹ ChatGPT users in social engineering attacks to **steal login credentials**, while also promoting¹⁸⁰ fake AI services through Facebook ads and hijacked pages. Cybercriminals enlisted ChatGPT and similar tools to **co-author** their fraudulent communications. Researchers uncovered tools such as FraudGPT, designed specifically to craft scam emails, and have identified incidents¹⁸¹ where actors used PowerShell scripts likely generated by large language models. Deepfake scams, though less frequent, also made headlines. In one notable incident¹⁸², a multinational corporation lost over \$25 million when attackers used deepfake technology to impersonate senior executives. Furthermore, criminals have exploited¹⁸³ AI-driven face-swapping services to create deepfakes from stolen mobile phone facial recognition data.

¹⁶⁶ FBI - IC3 Report - https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf.

¹⁶⁷ NCC - Threat Monitor Report 2023 - <https://www.nccgroup.com/us/threat-monitor-report-2023/>.

¹⁶⁸ Dragos - Dragos Industrial Ransomware Analysis: Q4 2023 - <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2023/>.

¹⁶⁹ Netenrich - Red CryptoApp: A New Threat Group in the Ransomware World - <https://netenrich.com/blog/red-cryptoapp-ransomware-new-threat-group/>.

¹⁷⁰ Palo Alto - BianLian - <https://unit42.paloaltonetworks.com/bianlian-ransomware-group-threat-assessment/>.

¹⁷¹ SentinelOne - Ransomware Evolution | How Cheated Affiliates Are Recycling Victim Data for Profit -

<https://www.sentinelone.com/blog/ransomware-evolution-how-cheated-affiliates-are-recycling-victim-data-for-profit/>.

¹⁷² Palo Alto - Incident Response Report -

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf.

¹⁷³ FS-ISAC - New Cyber Threats to Challenge Financial Services Sector in 2024 -

<https://www.fsisac.com/hubfs/Knowledge/NavigatingCyber/2024/FSISAC-NavCyber24-Report.pdf>.

¹⁷⁴ Wiley - Ransomware Attacker Files SEC Complaint to Increase Pressure on Victim - <https://www.wiley.law/alert-ransomware-attacker-files-sec-complaint-to-increase-pressure-on-victim/>.

¹⁷⁵ Bitdefender - French Authorities Arrest Russian National - <https://www.bitdefender.com/blog/hotforsecurity/french-authorities-arrest-russian-national-allegedly-connected-to-hive-ransomware/>.

¹⁷⁶ Europol - Ragnar Locker ransomware operation taken - <https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop>.

¹⁷⁷ Europol - Largest ever operation against botnets - <https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem>.

¹⁷⁸ Europol - Law enforcement disrupt world's biggest ransomware operation - <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>.

¹⁷⁹ ESET - ESET Threat Report H2 2023 - <https://www.welivesecurity.com/en/eset-research/eset-threat-report-h2-2023/>.

¹⁸⁰ Bitdefender - AI meets next-gen info stealers in social media malvertising campaigns -

<https://www.bitdefender.com/blog/labs/ai-meets-next-gen-info-stealers-in-social-media-malvertising-campaigns/>.

¹⁸¹ Proofpoint - TA547 Targets German Organizations with Rhadamanthys Stealer -

<https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer>.

¹⁸² CNN - British engineering giant Arup revealed as \$25 million deepfake scam victim -

<https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html>.

¹⁸³ Group-IB - Face Off: Group-IB identifies first iOS trojan stealing facial recognition data - <https://www.group-ib.com/blog/goldfactory-ios-trojan/>.



Additionally, AI-powered cryptocurrency scams¹⁸⁴ are on the rise, with perpetrators using platforms like YouTube to trap unsuspecting victims.

Initial Access Brokers - IAB

Initial Access Brokers (IABs) maintained¹⁸⁵ ¹⁸⁶ their popularity, continuing to profit by providing initial access to cybercrime actors. The abundance of relatively easy-to-exploit **vulnerabilities** in internet-facing devices and the prevalence of **information stealers** have further boosted their popularity. Interestingly, some IABs have been utilised by State-nexus actors as well, highlighting the strategic importance of their services.

Rise of information stealers

The rise¹⁸⁷ of information stealers paralleled the popularity of IABs and downloaders. Information stealers are now **essential components in attack chains** for all threat actors, typically deployed through phishing, malvertising and misleading posts on social media¹⁸⁸. RedLine and Raccoon remain among the most common stealers, while new variants such as BunnyLoader and Stealc have emerged. The landscape also includes the Python-based NodeStealer¹⁸⁹ which targets Facebook business accounts and Predator AI¹⁹⁰, designed to target cloud services. Even macOS is not immune¹⁹¹, with stealers able to evade many static signature detection engines. It is almost certain that initial access brokers, downloaders and information stealers will continue to pose a significant challenge for defenders in the coming years.

XaaS

As-a-service offerings remained¹⁹² ¹⁹³ popular among cybercriminals due to their efficiency and profitability and several of these services received significant updates. **Phishing as a Service** (PhaaS) now commonly includes¹⁹⁴ ¹⁹⁵ MFA bypass techniques and branding for password managers. The rise of Drainer-as-a-Service¹⁹⁶ for deploying crypto drainers and Disinformation-for-Hire¹⁹⁷ ¹⁹⁸ for influence campaigns was also notable. New or evolving **Ransomware as a Service** (RaaS) offerings¹⁹⁹, such as RansomHub and Farnetwork, continue to emerge. Kryptina RaaS, a dedicated Linux attack framework, added²⁰⁰ a new twist by transitioning from a paid service to an openly available tool.

2.3 PRIVATE SECTOR OFFENSIVE ACTORS TRENDS

Surveillance and exploit development

¹⁸⁴ Avast - Avast Q1/2024 Threat Report - <https://decoded.avast.io/threatresearch/avast-q1-2024-threat-report/>.

¹⁸⁵ Mandiant - Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect - <https://www.mandiant.com/resources/blog/initial-access-brokers-exploit-f5-screenconnect>.

¹⁸⁶ Initial Access Brokers, Infostealers, and Everything Between Them - <https://underthebreach.medium.com/initial-access-brokers-infostealers-and-everything-between-them-f5d154a87f6c>.

¹⁸⁷ Verizon - 2024 Data Breach Investigations Report - <https://www.verizon.com/business/resources/reports/dbir/>.

¹⁸⁸ Cybereason - Unboxing Snake - Python Infostealer Lurking Through Messaging Services - <https://www.cybereason.com/blog/unboxing-snake-python-infostealer-lurking-through-messaging-service>.

¹⁸⁹ Palo Alto - NodeStealer 2.0 – The Python Version: Stealing Facebook Business Accounts - <https://unit42.paloaltonetworks.com/nodestealer-2-targets-facebook-business/>.

¹⁹⁰ SentinelOne - SentinelLabs 2023 Review - <https://www.sentinelone.com/blog/12-months-of-fighting-cybercrime-defending-enterprises-sentinel-labs-2023-review/>.

¹⁹¹ SentinelOne - A Deep Dive into Emerging Trends and Evolving Techniques - <https://www.sentinelone.com/blog/mac-os-malware-2023-a-deep-dive-into-emerging-trends-and-evolving-techniques/>.

¹⁹² Cisco - Why are there so many malware-as-a-service offerings? - <https://blog.talosintelligence.com/need-to-know-commodity-malware/>.

¹⁹³ Verizon - 2024 Data Breach Investigations Report - <https://www.verizon.com/business/resources/reports/dbir/>.

¹⁹⁴ Proofpoint - Unmasking Tycoon 2FA: A Stealthy Phishing Kit Used to Bypass Microsoft 365 and Google MFA - <https://www.proofpoint.com/us/blog/email-and-cloud-threats/tycoon-2fa-phishing-kit-mfa-bypass>.

¹⁹⁵ LastPass - Advanced Phishing Kit Adds LastPass Branding for Use in Phishing Campaigns - <https://blog.lastpass.com/posts/2024/04/advanced-phishing-kit-adds-lastpass-branding-for-use-in-phishing-campaigns>.

¹⁹⁶ SentinelOne - DaaS - <https://www.sentinelone.com/blog/the-rise-of-drainer-as-a-service-understanding-daas/>.

¹⁹⁷ ADMM - Disinformation-for-Hire - https://www.acice-asean.org/files/information%20centre%20reports/feb_24_info.pdf.

¹⁹⁸ Disinformation-for-Hire as Everyday Digital Labor: Introduction to the Special Issue - <https://journals.sagepub.com/doi/10.1177/20563051231224723>.

¹⁹⁹ Group-IB : Investigation into farnetwork, a threat actor linked to five strains of ransomware - <https://www.group-ib.com/blog/farnetwork/>.

²⁰⁰ SentinelOne - From Underground Commodity to Open Source Threat - <https://www.sentinelone.com/blog/kryptina-raas-from-underground-commodity-to-open-source-threat/>.



Commercial surveillance vendors (CSVs) are significantly taking the lead in browser and mobile device **exploitation**. These companies often²⁰¹ ²⁰² navigate legal and quasi-legal frameworks, typically concealed by layered corporate ownership structures and their geographical reach allows them to **exploit jurisdictional arbitrage**. **Complicating matters, governments** frequently²⁰³ ²⁰⁴ **become customers** of these vendors. Recent revelations²⁰⁵ have shown that the crisis surrounding the hacking of European Parliament phones is widening, raising concerns about confidential EU work. Such cases are not entirely new; journalists and human rights defenders have long been targeted by similar malware. Despite these challenges, some international efforts to counter these types of organisations are underway²⁰⁶ ²⁰⁷. However, it is very likely that without a coordinated response, these companies will remain central hubs for collecting vulnerabilities and developing exploits.

2.4 HACKTIVISTS' TRENDS

Conflict driven

Hacktivist activity, increasingly driven by ongoing geopolitical conflicts, has become a dynamic element in the cyber threat landscape. It has evolved²⁰⁸ into a mainstream phenomenon and is now **an inevitable dimension of political disputes**. The war in Ukraine continues to catalyse a surge in hacktivist activity, with numerous groups aligning themselves with either side of the conflict. Attacks are often **retaliatory**, aiming to disrupt services and send political messages. The conflict between Israel and Hamas further highlights²⁰⁹ the role of hacktivists in modern warfare. A notable trend is the **international reach** of these hacktivist activities, as well as the **overlapping interests** and tactics of groups involved in these conflicts. Groups associated with Iran and Russia began²¹⁰ ²¹¹ targeting Israeli government and media websites, while groups based in India attacked Palestinian government websites. A significant difference between the two conflicts was noted by Google²¹². In the Israel-Gaza region, there was no spike in cyber operations against Israeli targets before the attack, in stark contrast to Ukraine, which experienced a large increase in Russian cyber threat activity targeting Kyiv in the lead-up to the invasion.

In regards to the European Union according to ENISA, during the reporting period saw nearly 3,662 hacktivist incidents nearly all linked with the ongoing geopolitical crisis between Russia and Ukraine while a small percentage can be observed to be linked with cases from the other geopolitical crisis. The most active group has been NoName057(16) followed Cyber Army of Russia. Continuing on our previous reporting, it is very likely that hacktivism will continue to support a variety of political ideals, particularly in countries experiencing civil unrest or war.

Potential Links with State-nexus actors

A notable trend is the correlation between State-nexus actors and alleged hacktivists. A notable example is²¹³ CyberAv3ngers, a persona used by Iranian State-nexus actors to target critical

²⁰¹ Meta - Adversarial Threat Report: Countering the Surveillance-for-Hire Industry & Influence Operations - <https://transparency.meta.com/en-gb/metasecurity/threat-reporting>.

²⁰² Atlantic Council - A Glance into the Spyware Industry - https://github.com/blackorbird/APT_REPORT/blob/master/summary/2024/Atlantic-Council-American-University-Markets-Matter-A-Glance-into-the-Spyware-Industry.pdf.

²⁰³ EurActiv - Governments spying on citizens: Who is to blame, what can the EU do? - <https://www.euractiv.com/section/digital/opinion/governments-spying-on-citizens-who-is-to-blame-what-can-the-eu-do/>.

²⁰⁴ AI - A Web of Surveillance - <https://securitylab.amnesty.org/latest/2024/05/a-web-of-surveillance/>.

²⁰⁵ EDRi - Brussels rocked by major spyware scandal: Urgent call for ban - <https://edri.org/our-work/press-release-brussels-rocked-by-major-spyware-scandal-urgent-call-for-ban/>.

²⁰⁶ Treasury - Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium - <https://home.treasury.gov/news/press-releases/jv2155>.

²⁰⁷ US State Dpt - Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware - <https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware/>.

²⁰⁸ BlackBerry - Threat Intelligence Report - <https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report>.

²⁰⁹ Dark Reading - Cyber Operations Intensify in Middle East, With Israel the Main Target - <https://www.darkreading.com/cyber-risk/cyber-operations-intensify-in-middle-east-with-israel-the-main-target>.

²¹⁰ Politico - Hackers piled onto Israeli-Hamas - <https://www.politico.eu/article/israel-hamas-war-hackers-cyberattacks/>.

²¹¹ Time - Cyberattacks Targeting Israel - <https://time.com/6322175/israel-hamas-cyberattacks-hackers/>.

²¹² Google - Tool of First Resort - <https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf>.

²¹³ CISA - IRGC-affiliated cyber actors target US - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>.



infrastructure. The rise of these **hacktivist personas** serves²¹⁴ to cloak state participation in their operations and to influence public opinion, thereby obscuring direct state involvement. Cyber Army of Russia Reborn (CARR) has been linked to the Russian state operating under the APT44 umbrella²¹⁵. It is likely that some State-nexus actors will continue to refine this technique, using it as a convenient method to deny participation and manipulate viewpoints.

FUD - Fear, Uncertainty, and Doubt

Hacktivists continue to **amplify the impact of their operations** to influence public perception and social discourse. This self-promotion but also the coordinated promotion by affiliated hacktivist groups, whether through social media or other public forums, serves²¹⁶ to heighten fear, uncertainty and doubt (**FUD**) within the target audience.

Internet graffiti: DDoS and defacements

The stream of Internet graffiti, **DDoS** attacks and **defacements** remains a threat. Hacktivists maintained²¹⁷ ²¹⁸ their operational techniques for conducting DDoS attacks. While not novel, website defacements featured²¹⁹ prominently as an easy way to convey a message.

Ransomware, wipers and data theft

Hacktivists further **mimic cybercrime operators tactics**, such as using ransomware, wipers²²⁰ and relying on data theft²²¹. Ideology-motivated hacktivist groups are using²²² **ransomware** payloads to disrupt targets and draw attention to their political causes. Alongside the blending of hacktivism with State-nexus activity, it is likely hacktivists will increasingly adopt cybercrime tactics, sometimes with direct or indirect support from these State-nexus groups.

²¹⁴ SentinelOne - The Israel-Hamas War | Cyber Domain State-Sponsored Activity of Interest - <https://www.sentinelone.com/labs/the-israel-hamas-war-cyber-domain-state-sponsored-activity-of-interest/>.

²¹⁵ <https://services.google.com/fh/files/misc/apt44-unearting-sandworm.pdf>

²¹⁶ HackerNews - A New Age of Hacktivism - <https://thehackernews.com/2024/02/a-new-age-of-hacktivism.html>.

²¹⁷ NCC - Threat Monitor Report 2023 - <https://www.nccgroup.com/us/threat-monitor-report-2023/>.

²¹⁸ SentinelOne - Disinformation, DDoS and Scams - <https://www.sentinelone.com/blog/oct-2023-cybercrime-update-disinformation-ddos-and-scams-as-gangs-look-to-exploit-turmoil/>.

²¹⁹ SecAlliance - Russia-Ukraine war: Telegram-based hacktivism in 2023 - <https://www.secalliance.com/blog/russia-ukraine-war-telegram-based-hacktivism-in-2023>.

²²⁰ Blackberry - BiBi Wiper Used in the Israel-Hamas War Now Runs on Windows -

<https://blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows>.

²²¹ JPost - Hackers steal IDF patient records from cyberattack on Israeli hospital - <https://www.jpost.com/israel-news/defense-news/article-775843>.

²²² SentinelOne - Hacktivist Group Leverages Ransomware for Attention Not Profit - <https://www.sentinelone.com/blog/ikaruz-red-team-hacktivist-group-leverages-ransomware-for-attention-not-profit/>.





3. VULNERABILITIES LANDSCAPE

The analysis of the vulnerabilities landscape provides insights into the evolving landscape of software vulnerabilities and allows the reader to identify trends, patterns and emerging threats thus aiding the enhancement of cybersecurity strategies. By understanding the frequency, severity and types of vulnerabilities discovered, organisations can prioritise patching and mitigation efforts, allocate resources effectively and proactively address potential risks to their systems and data. This proactive approach helps to minimise the potential for security breaches, data breaches and other cyber-attacks, ultimately contributing to a more resilient and secure digital environment²²³.

Moreover, this work is meant to complement the annual ETL by providing a glimpse into the vulnerabilities that are often leveraged in cyber-attacks. The ETL is based on public sources and ENISA has tried to cross-correlate the analysis of the vulnerability landscape with that of the publicly disclosed incidents, to identify trends in the vulnerabilities exploited etc. However, unfortunately it is not common practice to disclose such information to the public and hence this much needed and useful analysis was not feasible. With the Network and Information Security Directive 2 (NISD 2) and Cyber Resilience Act, enhancements in both incident reporting and vulnerability management and disclosure are expected in the EU, which will hopefully enable us to conduct more in-depth and correlated analysis. In our exploration of the CVE Landscape, we considered the following definitions of key terms associated with vulnerability foreclosure:

*CVE*²²⁴ (*Common Vulnerabilities and Exposures*) is a standardized system designed for identifying and naming security vulnerabilities in various software and hardware products. It assigns a unique identifier to each vulnerability, making it simpler to track and reference vulnerabilities across different systems and databases.

CVSS^{225 226} (*Common Vulnerability Scoring System*) is a framework used to evaluate the severity of security vulnerabilities. It offers a numerical score that quantifies a vulnerability's impact and exploitability, helping organisations prioritise which vulnerabilities to address first.

CVSS score has already reached version 4.0²²⁷

*CNA*²²⁸ (*CVE Numbering Authority*) is an organisation or entity responsible for assigning CVE identifiers to vulnerabilities and ensuring their accuracy and consistency.

*CWE*²²⁹ (*Common Weakness Enumeration*) is a catalogue of common software and hardware weaknesses, security issues, and coding errors. It serves as a reference for known software security vulnerabilities and is instrumental in improving the understanding and mitigation of these security weaknesses during the software development process.

²²³ It should be noted that the CVE, CWE, OWASP, and CVSS frameworks have altered the trajectory of vulnerability reporting and data in the past: <https://www.first.org/events/colloquia/cardiff2023/program#pTime-and-Magnitude-Epoch-Fail-Forecasting-Vulnerabilities-Amid-Temporal-Discontinuity>

²²⁴ <https://cve.mitre.org/>.

²²⁵ <https://www.first.org/cvss/>.

²²⁶ <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>.

²²⁷ [CVSS v4.0 Specification Document \(first.org\)](https://www.first.org/cvss/v4.0-specification-document)

²²⁸ <https://cve.mitre.org/cve/cna.html>.

²²⁹ <https://cwe.mitre.org/>.



3.1 SUMMARY

During the time-frame under examination in this report, from **July 1st, 2023**, to **July 1st, 2024**, a total of **33,524** vulnerabilities were recorded in the NIST NVD. This represents a significant increase compared to the **24,690** vulnerabilities reported in the previous ETL document for the period between **July 1, 2022**, and **July 1, 2023**.

Additionally, it's noteworthy that within this specific time-frame, **123** out of the **33,524** published vulnerabilities are part of the 'CISA Known Exploited Vulnerabilities catalogue'²³⁰ (also referred to as KEV list). It is important to highlight that for a vulnerability to be included in the 'CISA Known Exploited Vulnerabilities Catalogue,' it must satisfy specific criteria such as having an ID, there should be evidence of active exploitation and a clear remediation action, such as a vendor-provided update, should be available.

3.2 ANALYSIS OF THE CVE NUMBERING AUTHORITIES (CNA²³¹)

In the section below, an analysis of the allocation of CVEs by CVE numbering authorities (CNAs) has been carried out. The aim of this analysis is to identify any discernible trends or patterns related to specific vendors, which can assist the reader in making informed decisions about prioritising patching activities. Within the EU and EFTA countries, there are 50 partner CNAs including ENISA. The following illustration presents the distribution of CVE numbers assigned by each CVE numbering organisation (CNA) for the specified period from **July 2023** to **July 2024**:

Figure 12: CVEs by CVE Numbering Authority (CNA) (Percentage of the total)

CVEs by CVE Numbering Authority 2023-2024

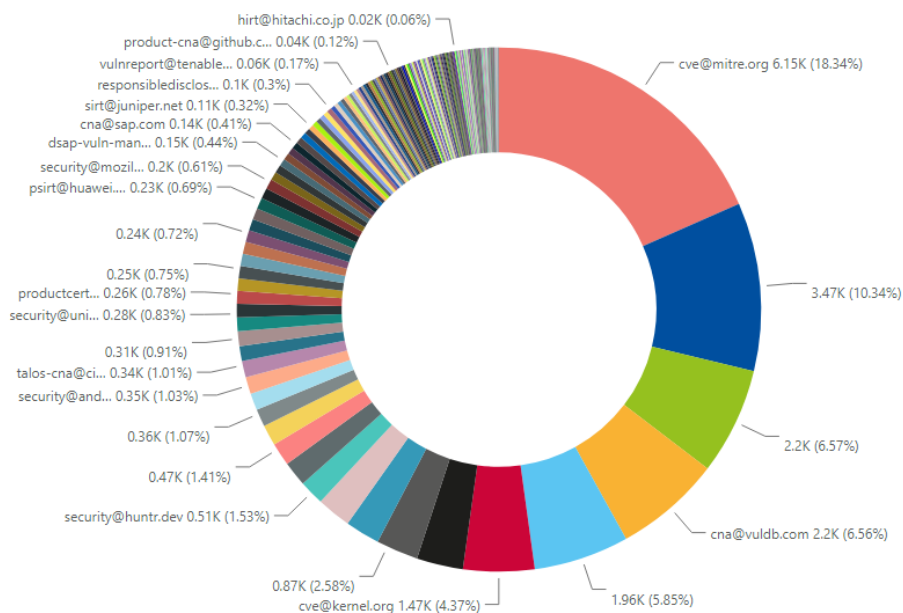


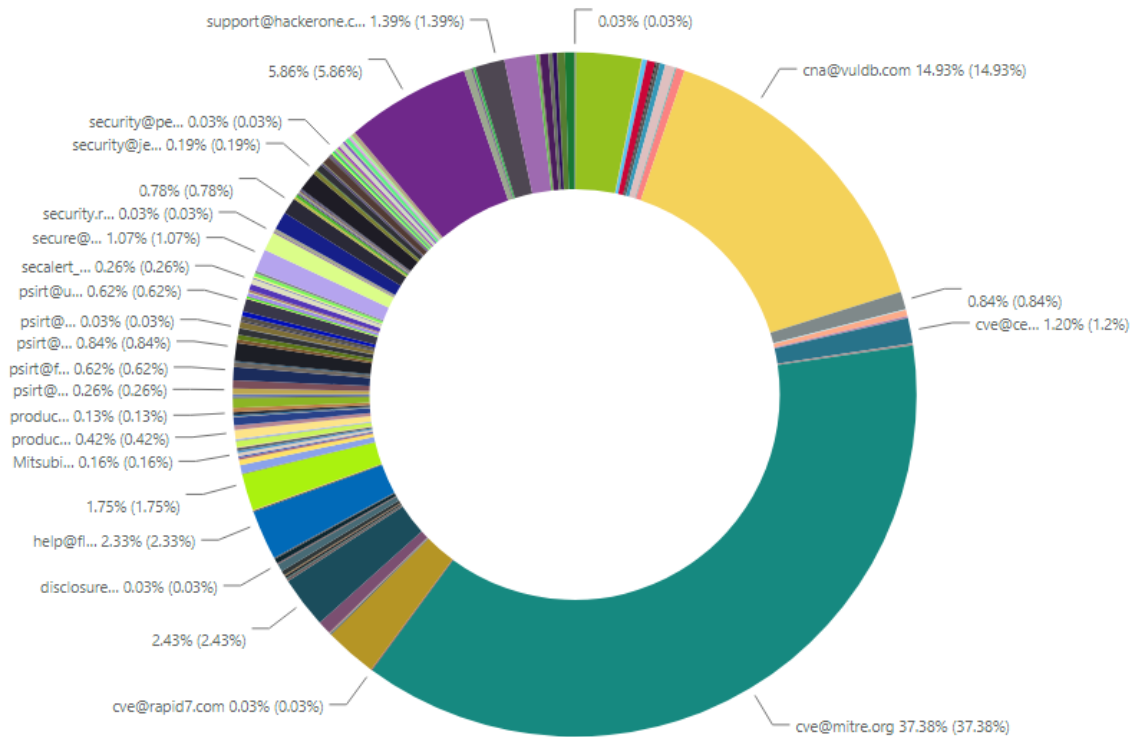
Figure 13: CVEs with CVSS greater than 9 assigned by the CNAs (Percentage of the total)

²³⁰ [Known Exploited Vulnerabilities Catalogue | CISA](#).

²³¹ CNAs are vendor, researcher, open source, CERT, hosted service and bug bounty provider organisations authorised by the CVE Programme to assign [CVE IDs](#) to vulnerabilities and publish [CVE Records](#) within their own specific scopes of coverage. <https://www.cve.org/ProgramOrganization/CNAs>.



Percentage of CVEs with CVSS score greater than 9 assigned by CNA 2023-2024



By comparing both figures (Figures 12 and 13), it becomes evident that the allocation of critical vulnerabilities with a CVSS score above 9, differs between the various CNAs. For example, MITRE, one of the two Top-Level Root CNAs, is responsible for one-third of the critical vulnerabilities in the overall count which is correlated also with the overall allocation of vulnerabilities.

3.3 ANALYSIS OF THE CVE LANDSCAPE

In this year's ETL report, a total of **19,754 vulnerabilities** were identified that had encoded their afferent severity score information. Out of the aforementioned vulnerabilities, 9.3% fell into the 'critical' category and 21.8% were categorised as 'high' according to their CVE base Severity tag.

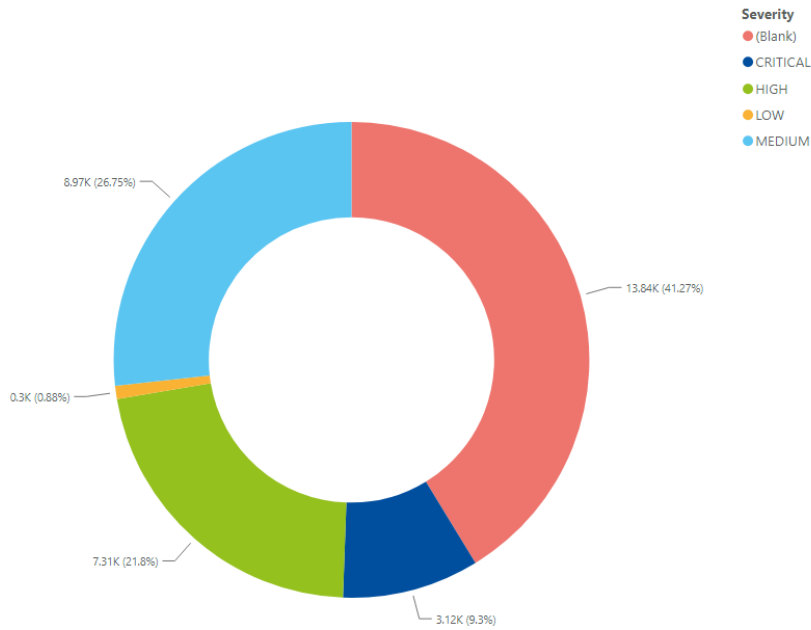
Among these vulnerabilities, it is noteworthy that approximately 123 of them were subsequently included in the CISA Known Exploited Vulnerabilities (KEV) list. This selection indicates that these particular vulnerabilities were actively targeted and exploited by malicious actors, making them of significant concern to the security community²³².

²³² <https://www.cisa.gov/known-exploited-vulnerabilities>.



Figure 14: Percentage of CVEs by Severity (Percentage of the total)

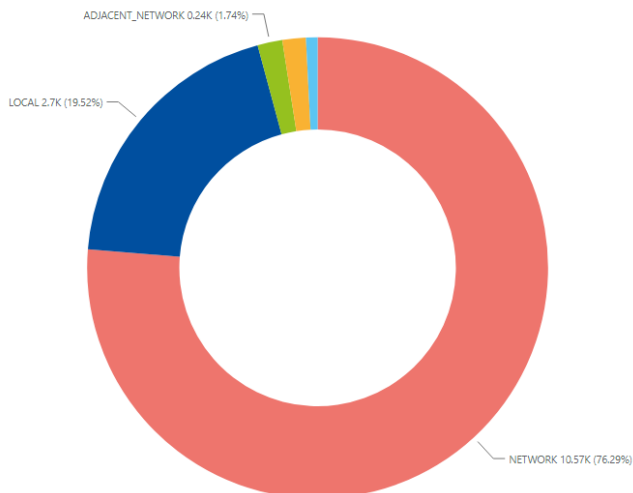
Percentage of CVEs and their severity 2023-2024



The donut chart, as depicted in Figure 14, offers a comprehensive view of the distribution of vulnerabilities by their severity tags LOW, MEDIUM, HIGH, or CRITICAL. The diagram includes vulnerabilities for which there is no specific severity information, tagged as 'Blank'. This additional category acknowledges that there are vulnerabilities for which the assessment of their severity is either pending, not yet determined or, for some other reason, has not yet been assigned. In essence, this section of the chart highlights the existing uncertainties or gaps in categorising these vulnerabilities based on their severity.

Figure 15: Number and percentage of CVEs by attack vector

Percentage of CVEs and their severity 2023-2024



It is crucial to underscore the importance of patching internet-facing applications that contain vulnerabilities rated as 'high' or 'critical'. This practice is essential to safeguard an organisation from potential attacks. In numerous instances, vulnerabilities falling into these categories may present a more accessible entry point for malicious actors seeking to breach systems and access data. Such breaches could result in financial losses, harm to an organisation's reputation or even lead to regulatory penalties. However, it is imperative not to disregard vulnerabilities with lower severity ratings, as they often serve as footholds in the later stages of cyber-attacks. It is worth noting that approximately 20% of vulnerabilities from the CISA KEV list fall into the 'medium' severity category.

In Figure 15, 76.29% of the vulnerabilities for which the attack vector information is available are exploitable via a Network.

Figure 16: CWEs 2023-2024

Top weaknesses 2023-2024

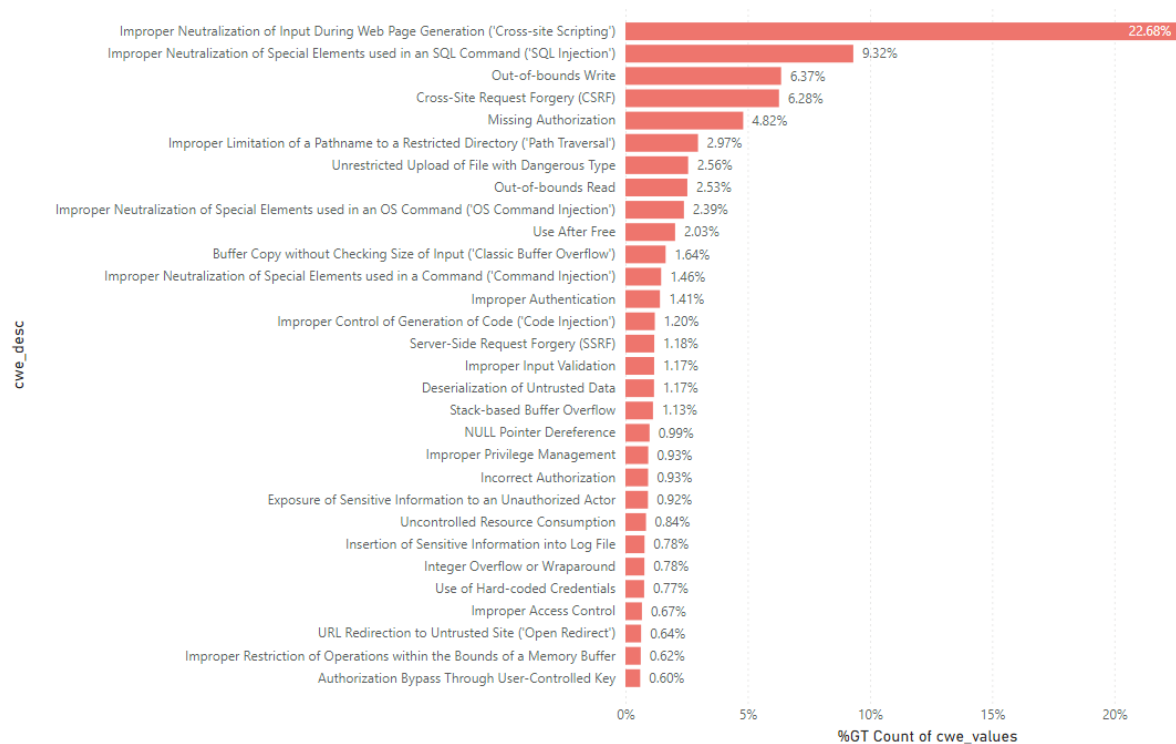


Table 1: MITRE TOP 25 CWEs 2023

Rank	ID	Name	Score	CVEs in KEV	Rank Change vs. 2022
1	CWE-787	Out-of-bounds Write	63.72	70	0
2	CWE-79	Improper Neutralisation of Input During Web Page Generation ('Cross-site Scripting')	45.54	4	0
3	CWE-89	Improper Neutralisation of Special Elements used in an SQL Command ('SQL Injection')	34.27	6	0
4	CWE-416	Use After Free	16.71	44	3



5	CWE-78	Improper Neutralisation of Special Elements used in an OS Command ('OS Command Injection')	15.65	23	1
6	CWE-20	Improper Input Validation	15.50	35	-2
7	CWE-125	Out-of-bounds Read	14.60	2	-2
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.11	16	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.73	0	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10.41	5	0
11	CWE-862	Missing Authorisation	6.90	0	5
12	CWE-476	NULL Pointer Dereference	6.59	0	-1
13	CWE-287	Improper Authentication	6.39	10	1
14	CWE-190	Integer Overflow or Wraparound	5.89	4	-1
15	CWE-502	Deserialisation of Untrusted Data	5.56	14	-3
16	CWE-77	Improper Neutralisation of Special Elements used in a Command ('Command Injection')	4.95	4	1
17	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.75	7	2
18	CWE-798	Use of Hard-coded Credentials	4.57	2	-3
19	CWE-918	Server-Side Request Forgery (SSRF)	4.56	16	2
20	CWE-306	Missing Authentication for Critical Function	3.78	8	-2
21	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronisation ('Race Condition')	3.53	8	1
22	CWE-269	Improper Privilege Management	3.31	5	7
23	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.30	6	2
24	CWE-863	Incorrect Authorisation	3.16	0	4
25	CWE-276	Incorrect Default Permissions	3.16	0	-5

The findings presented in Figure 16 correlate to a large extent with the list of the top 25 vulnerabilities in 2023²³³ published by MITRE, as well as with the previous year's ETL report. The recurring appearance of fundamentally similar software development flaws in the data, with a few exceptions, sheds light on the enduring challenges in secure software development. It underscores the limited progress made in addressing these vulnerabilities over time. While there are certainly outliers in the comparison and no absolute congruence, a broader view reveals striking resemblances between the types of vulnerabilities.

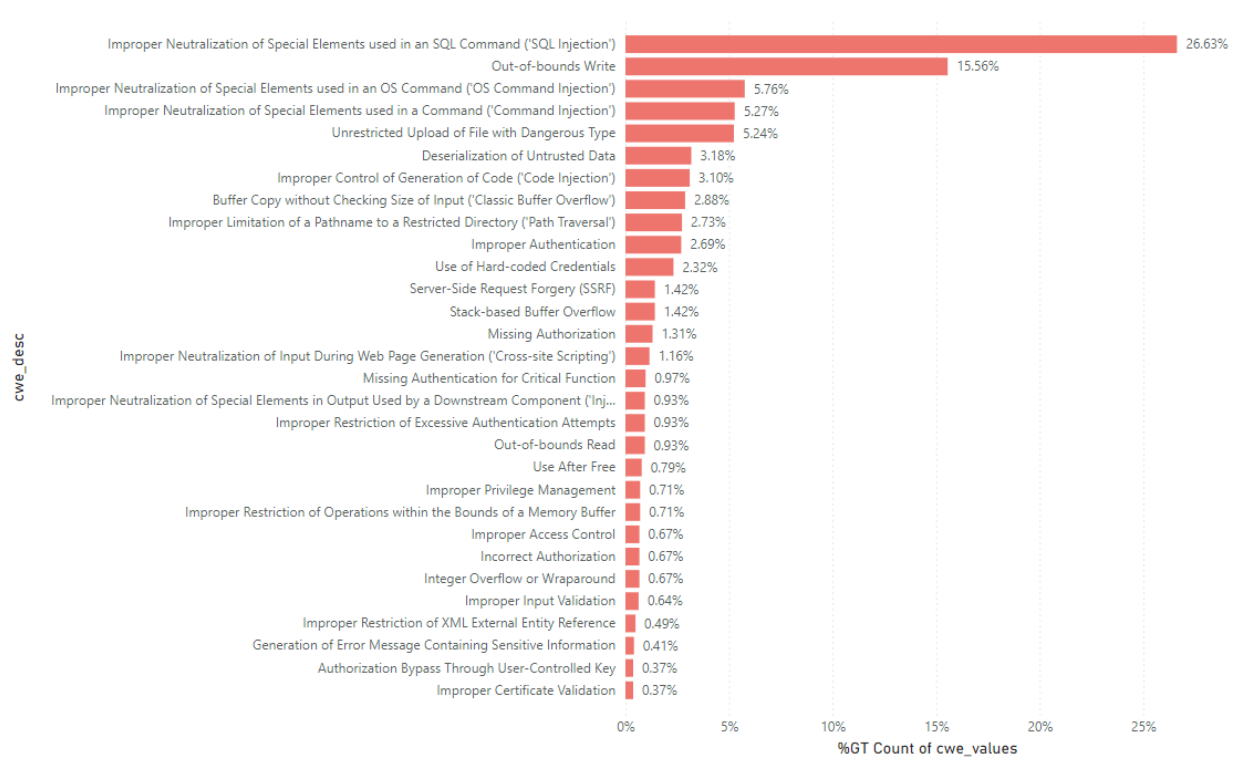
The figure below (figure 17) shows the top weaknesses (CWEs) that are responsible for a large chunk of critically severe vulnerabilities. In this instance, the data was appropriately filtered to focus on the 'critical' severity parameter.

²³³ <https://cwe.mitre.org/top25/index.html>.



Figure 17: Top CWEs by responsibility for critical severity (percentage of total)

Top weaknesses for critical vulnerabilities 2023-2024



According to the FIRST CVSS SIG, vulnerabilities that carry the CRITICAL base severity tag are those with a Common Vulnerability Scoring System version 3 (CVSSv3) score falling within the range of 9.0 to 10.0. These are the most severe vulnerabilities, indicating that they possess a high potential for exploitation and pose significant risks to systems and data.

Many of these weaknesses are specifically related to web vulnerabilities, which are often prime targets for attackers seeking unauthorised access. Web-related vulnerabilities encompass flaws affecting web applications, websites, and the underlying internet infrastructure.

In order to mitigate the risks posed by these critical vulnerabilities, organisations should strongly consider investing in secure software development practices and adopting relevant strategies. 'Secure-by-design and default' principles play a pivotal role in this context. These principles emphasise building software with security in mind from the very beginning and configuring systems in a secure manner by default. By incorporating secure development practices, organisations can proactively reduce the likelihood of critical vulnerabilities surfacing in their software or systems.

Recent efforts have been made by a consortium of international organisations to propose and advocate for good practices in secure software development²³⁴.

3.4 ANALYSIS OF KNOWN EXPLOITED VULNERABILITIES (KEV).

The CISA KEV catalogue²³⁵ is a dynamic catalogue of known exploited vulnerabilities that is updated with new vulnerabilities on a regular basis (the attackers never stop hence the list is constantly increasing). It is recommended that the catalogue of KEVs be used as a basis for

²³⁴ <https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default>.

²³⁵ [Known Exploited Vulnerabilities Catalogue | CISA](#).



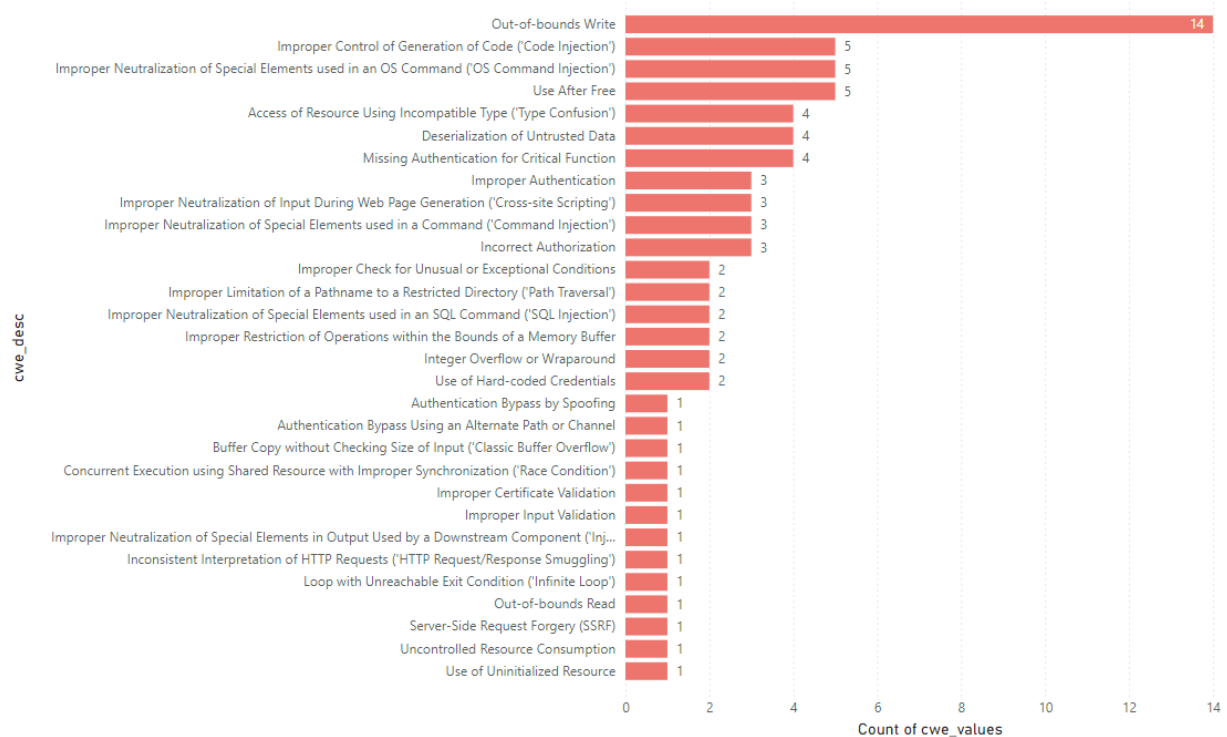
any organisation’s vulnerability management plans because those vulnerabilities have been observed in the wild by CISA to have been exploited or are under active exploitation.

In the timeframe of this year’s ETL (July 23 to July 24), 123 vulnerabilities were published in the KEV list; currently the entire CISA KEV list contains a total of 1,131 vulnerabilities.

The table below highlights the CWEs which account for part of the 123 vulnerabilities from the KEV list.

Table 2: CWEs responsible for KEVs 2023-2024

Top weaknesses for CISA KEV vulnerabilities 2023-2024

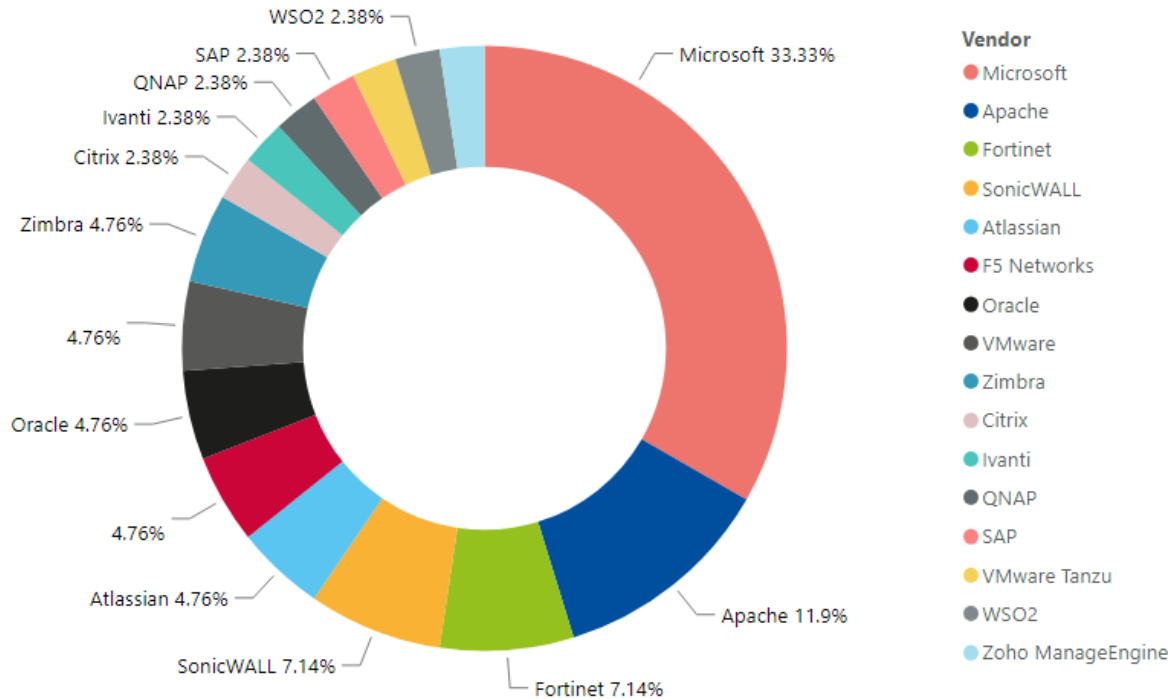


Another notable deliverable for the past year is the informative report titled *2022 Top Routinely Exploited Vulnerabilities*²³⁶, jointly published by CISA in collaboration with the Five Eyes partners, i.e. the United Kingdom, Australia, Canada, New Zealand, and the United States.

²³⁶ [2022 Top Routinely Exploited Vulnerabilities | CISA](#).



Figure 18: 2022 Top routinely exploited vulnerabilities by Vendors (2023 version hasn't been published)



In the ETL report from the previous year, we introduced the Exploit Prediction Scoring System (EPSS) which underwent a significant update at the beginning of 2024²³⁷ reaching to version 3.0. The EPSS score is designed to enhance the ability of organisations to prioritise system patching effectively. It quantifies the likelihood of a vulnerability being exploited within the next 30 days. It is important to note that the EPSS score is a momentary snapshot and can evolve over time as vulnerabilities progress.

3.5 BACKGROUND

In conducting the analysis of the CVE (Common Vulnerabilities and Exposures) landscape, several crucial data sources were used to ensure a comprehensive and well-informed analysis. These data sources played a pivotal role in shedding light on the state of vulnerabilities and security threats. Here are the primary sources used:

1. NIST NVD (National Vulnerability Database):

The NVD, maintained by the National Institute of Standards and Technology (NIST), stands as one of the foremost repositories for information regarding known vulnerabilities. It provides a comprehensive listing of vulnerabilities across a wide spectrum of software and hardware products. The database is continually updated to reflect the latest discoveries and assessments of vulnerabilities. You can explore the full listing here: [NVD Full Listing](#).

2. CISA Known Exploited Vulnerability Catalogue (KEV):

The CISA (Cybersecurity and Infrastructure Security Agency) Known Exploited Vulnerability Catalogue is a valuable resource that catalogues vulnerabilities that are actively exploited by malicious actors. The catalogue provides insights into vulnerabilities that are currently targeted and exploited in the cybersecurity landscape. A snapshot of this catalogue, as of August 12, 2022, was used to identify vulnerabilities that are actively leveraged in attacks. Further details on the KEV catalogue can be accessed here: [CISA KEV Catalogue](#).

²³⁷ [2302.14172 \(arxiv.org\)](https://arxiv.org/abs/2302.14172)



3. FIRST Exploit Prediction Scoring System (EPSS):

The FIRST (Forum of Incident Response and Security Teams) Exploit Prediction Scoring System, also known as EPSS, is an important tool for predicting the likelihood of a vulnerability being exploited. It offers a scoring system that assesses the potential risk associated with vulnerabilities. EPSS provides valuable data and statistics related to vulnerability predictions and exploits. To delve deeper into the details of EPSS, you can refer to these resources: [EPSS Details](#) and [EPSS Data and Stats](#).

By drawing insights from these sources, the analysis of the CVE landscape benefited from a well-rounded perspective on vulnerabilities, their severity, and their potential exploitation. This multifaceted approach allows for a more comprehensive understanding of the evolving cybersecurity threats and vulnerabilities that have an impact on the digital landscape.





4. RANSOMWARE

In ENISA's report on the Threat Landscape for Ransomware Attacks²³⁸, **ransomware** was defined as: *a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the assets' availability*. This definition covers the three key elements present in every ransomware attack:

- assets
- actions
- blackmail.

This generic yet descriptive definition was needed to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques and the various goals other than solely financial gains. This report also covers the four high-level actions (lock, encrypt, delete and steal) used by ransomware to impact the confidentiality, availability and integrity of the assets. It can serve as a reference to better understand this threat.

By contrast, the definition of ransomware in NIST describes ransomware as: *a type of malicious attack where attackers encrypt an organisation's data and demand payment to restore access. In some instances, attackers may also steal an organisation's information and demand additional payment in return for not disclosing the information to authorities, competitors or the public*²³⁹.

Following up on the established trend we have witnessed over the last few years, throughout the reporting period a substantial increase in ransomware-related incidents was observed, thus reaffirming the ongoing growth of the ransomware threat. Notably, the number of ransomware incidents has stabilised around the 1000 claims per quarter over the second quarter (Q2) of 2024 as seen in figure 18. It is worth mentioning that the incidents under analysis were as reported on DLSs (data leak sites).

²³⁸ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks>.

²³⁹ https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST_IR.8374-preliminary-draft.pdf.



Figure 19 ETL 2023 vs ETL 2024

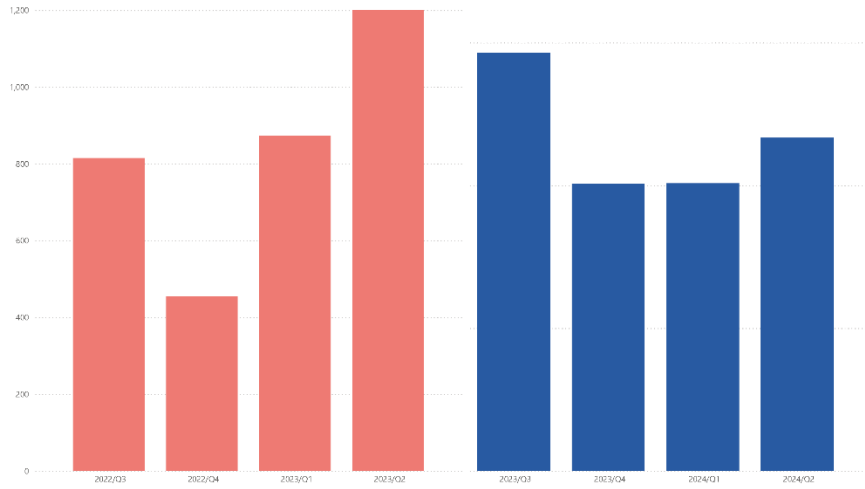


Figure 20: Time series of major incidents observed by ENISA (July 2023-June 2024)

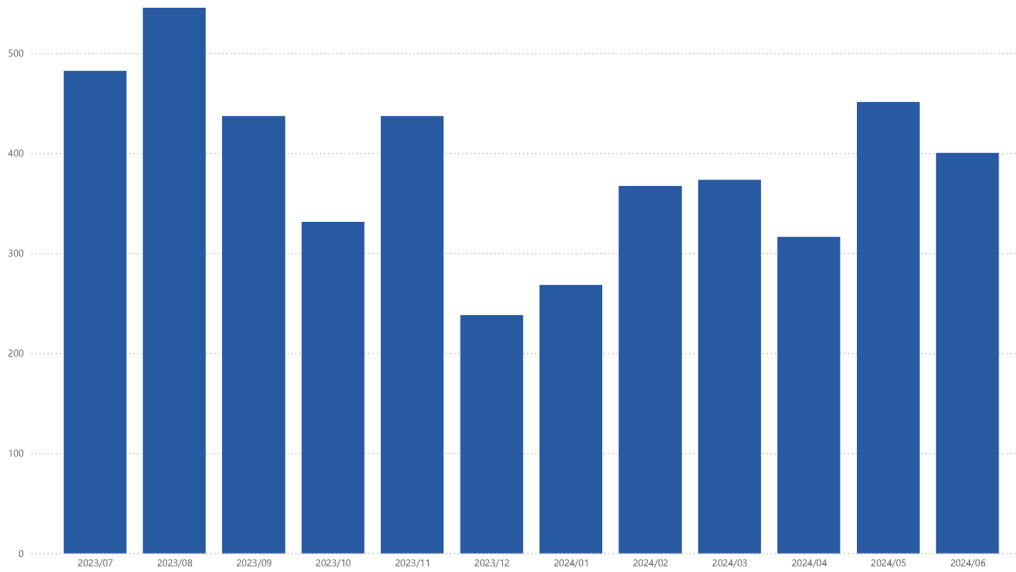
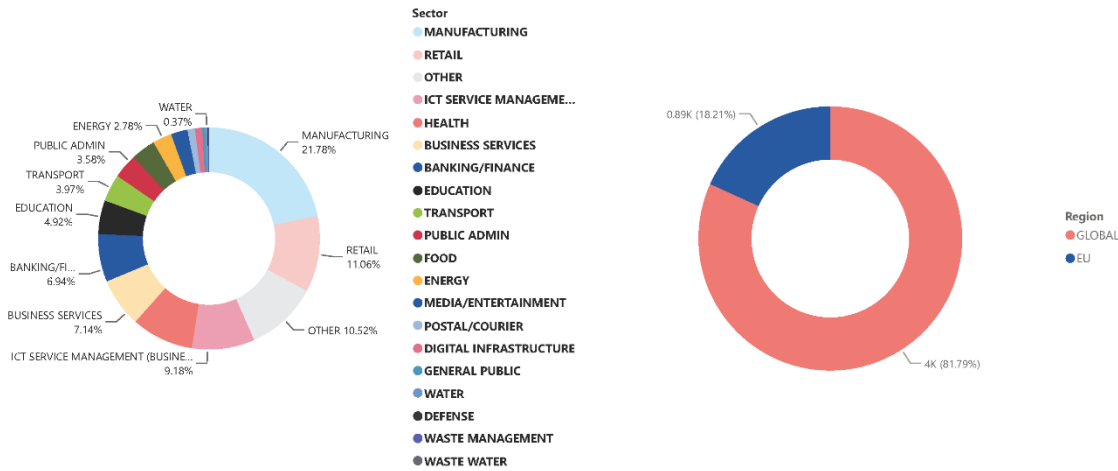
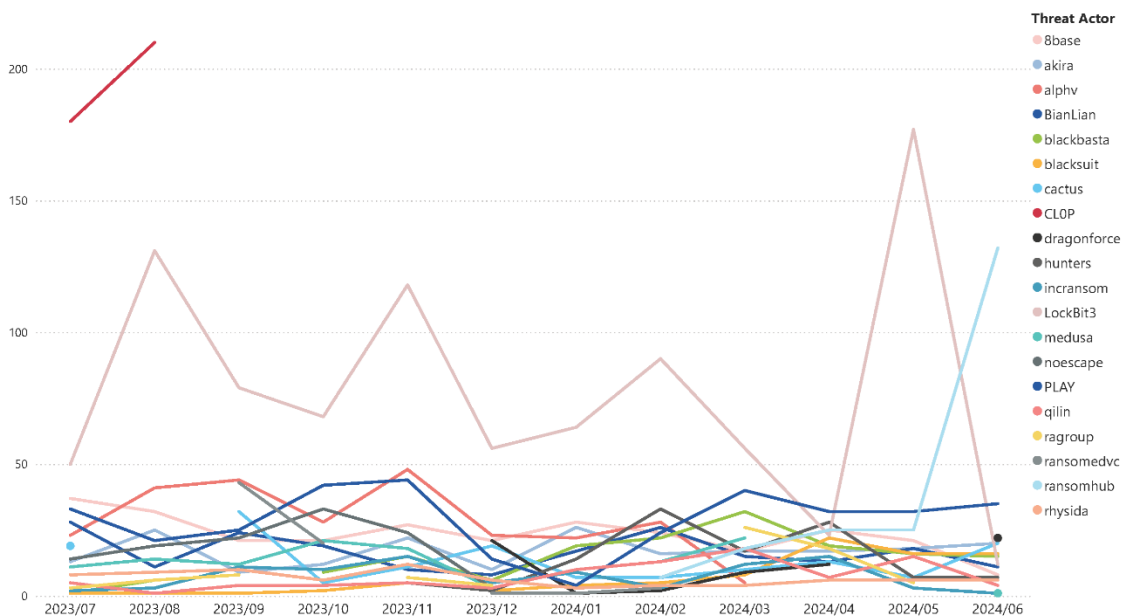


Figure 21 Breakdown of Sectors by threat type and region



In Figure 21, the timeline illustrates the activity of the most active ransomware groups as reported in their leak sites and the victims posted there. Notably, threat actor Lockbit maintained consistent activity throughout the entire period even though this RaaS provider was dismantled in an operation during February 2024. Despite the take-down operation, what followed was increased activity during the end of the reporting period which will be discussed in greater detail below. The rest of the ransomware groups follow a more stable timeline with Akira increasing activity during the end of the reporting period

Figure 22: Timeline of the 20 most active Ransomware groups during the reporting period

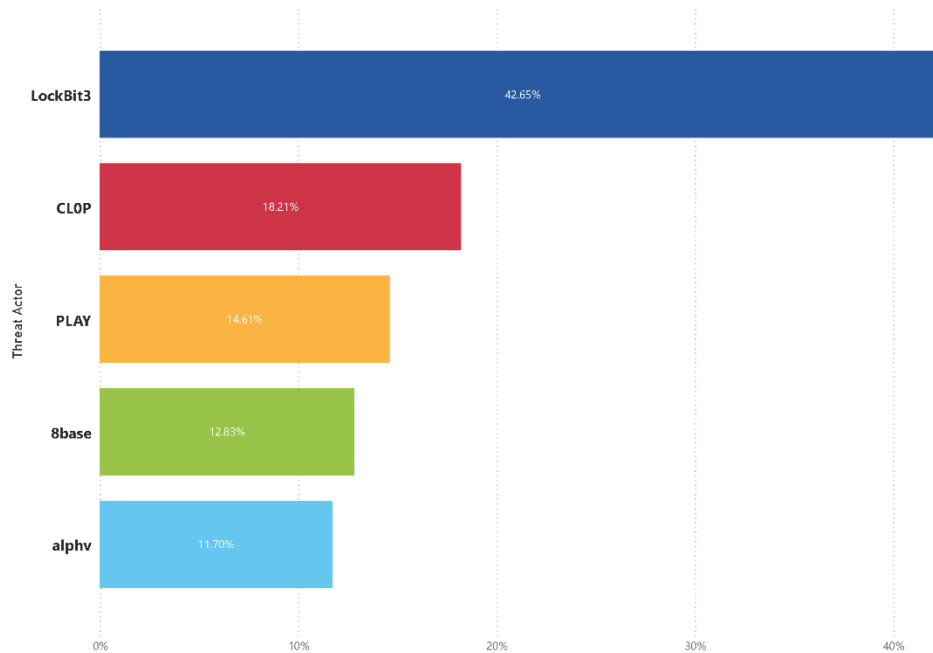


4.1 MOST ACTIVE RANSOMWARE STRAINS

LockBit, CIOP and PLAY were some of the top ransomware strains used in RaaS (Ransomware as a Service) and extortion attacks in terms of victim organisations, dominating the global landscape during the reporting period (Figure 21). LockBit accounted for nearly half the number of incidents that were reported. In addition, CIOP, while being one of the most active groups in 2023 (notably exploiting two different zero-days in their campaigns), has nonetheless remained inactive during the first semester of 2024. It is also noteworthy that PLAY remains a constant variant throughout the reporting period



Figure 23: Five Most active Ransomware groups on the Global Landscape



Ransomware attacks target a broad spectrum of industries, with the Industrial and Manufacturing sector being the most frequent, high-impact victim, followed closely by Retail and Digital Service Providers.

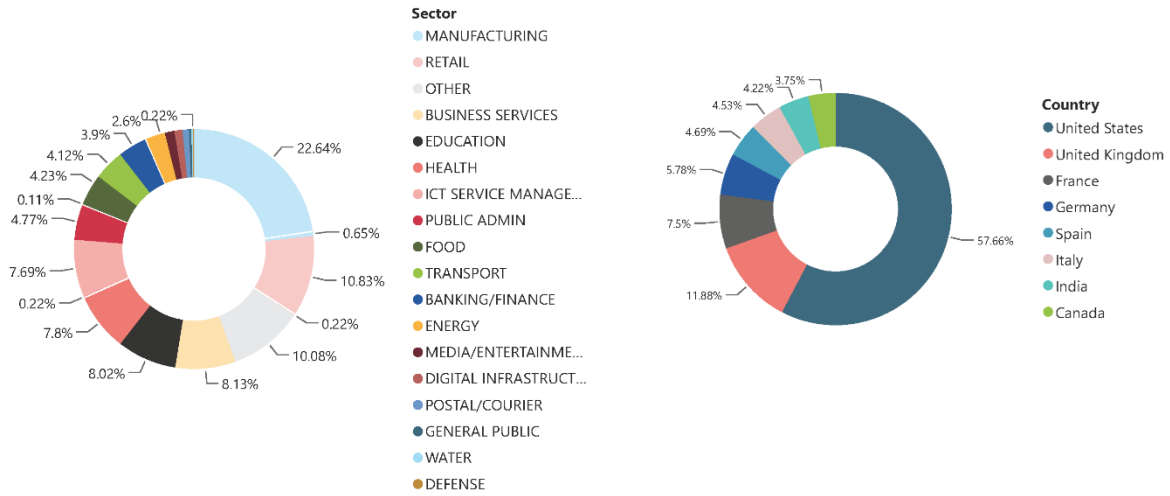
The industrial sector's heavy reliance on automation, supply chain operations, and critical infrastructure makes it a prime target for cybercriminals. Successful attacks can result in significant financial losses, operational disruptions, and reputational damage. Retailers are attractive targets due to the vast amounts of sensitive customer data they handle, including credit card information. This data can be stolen and sold on the dark web for substantial profits. Additionally, ransomware attacks can disrupt operations, leading to lost sales and ransom demands.

Digital Service Providers are also at risk due to their reliance on digital infrastructure and the value of their customer data. Successful attacks can result in service disruptions, loss of customers and reputational harm. Furthermore, supply chain attacks targeting this sector are increasingly common. The United States is the global epicentre for ransomware attacks, accounting for nearly half of all incidents worldwide during this period. Its diverse industrial landscape, critical infrastructure and presence of numerous large corporations create a lucrative environment for cybercriminals.

Figures 22, 23 and 24 present a breakdown of three ransomware strains. It is evident that, on a global scale and in terms of targeted sectors, LockBit and PLAY primarily focus on similar sectors in the majority of incidents. On the other hand, CL0P deviated and exhibited a significant concentration of attacks on Digital Service Providers as well as the Financial Sector. When considering the regional aspect, the majority of victims in all cases are in the USA, followed by various EU countries.



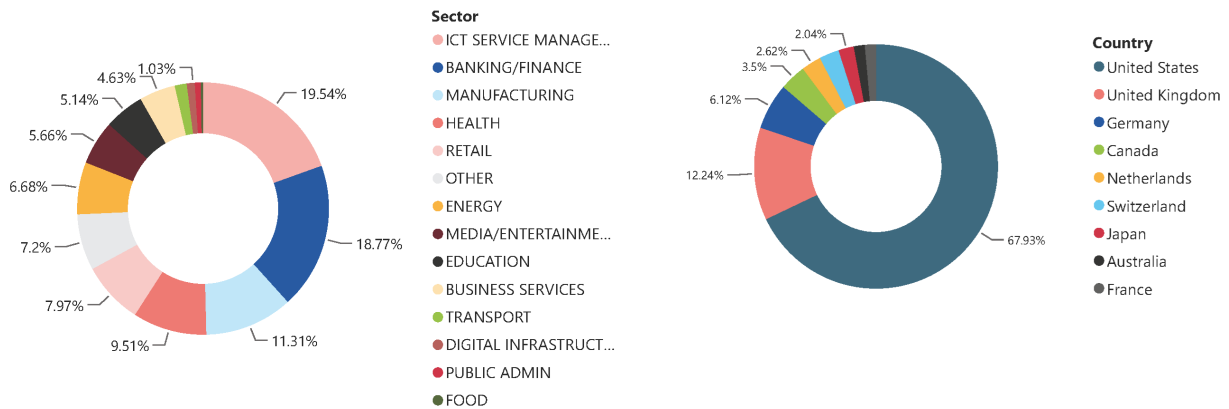
Figure 24: Lockbit break down by sectors and countries



936

No of potential victims

Figure 25: CL0P break down on sectors and countries

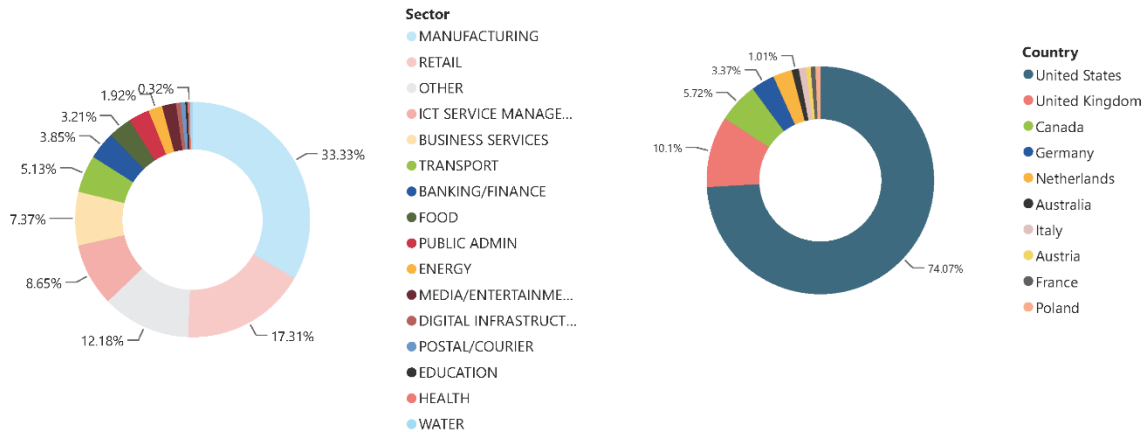


391

No of potential victims



Figure 26: PLAY break down on sectors and countries

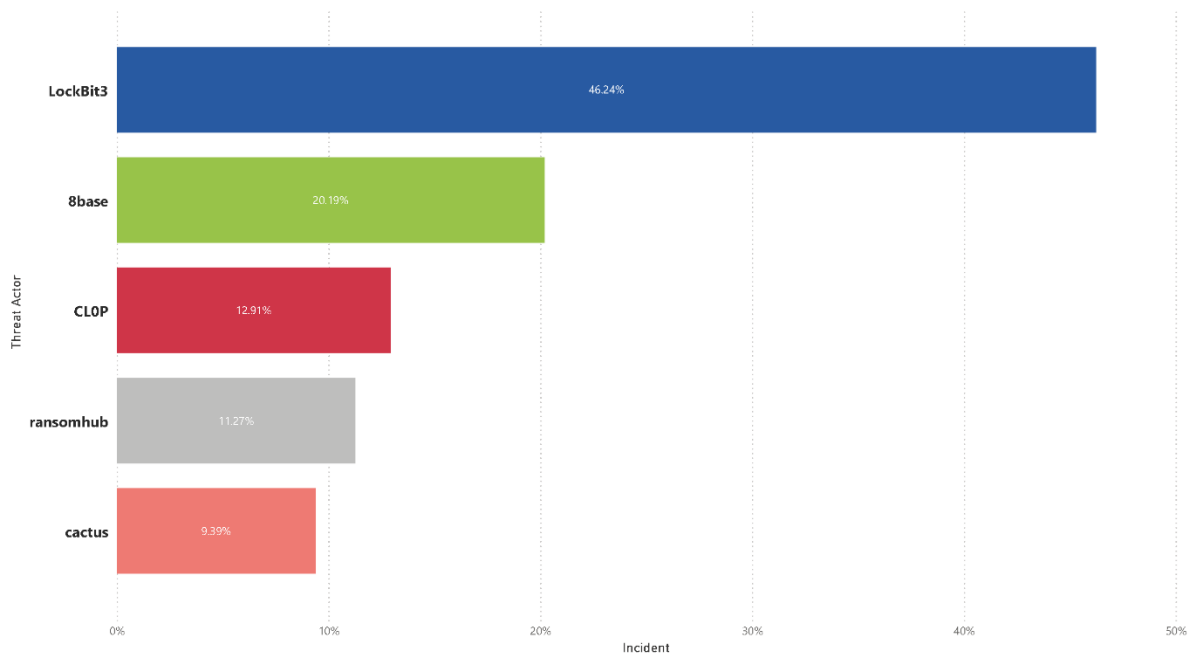


346

No of potential victims

In the context of the European landscape, it is notable that LockBit ransomware has again emerged as a prominent Ransomware-as-a-Service group, being responsible for more than half of the recorded ransomware incidents during the reporting period (Figure 25). Furthermore, two other ransomware groups, 8Base and Cl0p, have also played significant roles in this cybersecurity landscape, contributing to the complexity and diversity of ransomware attacks across the EU.

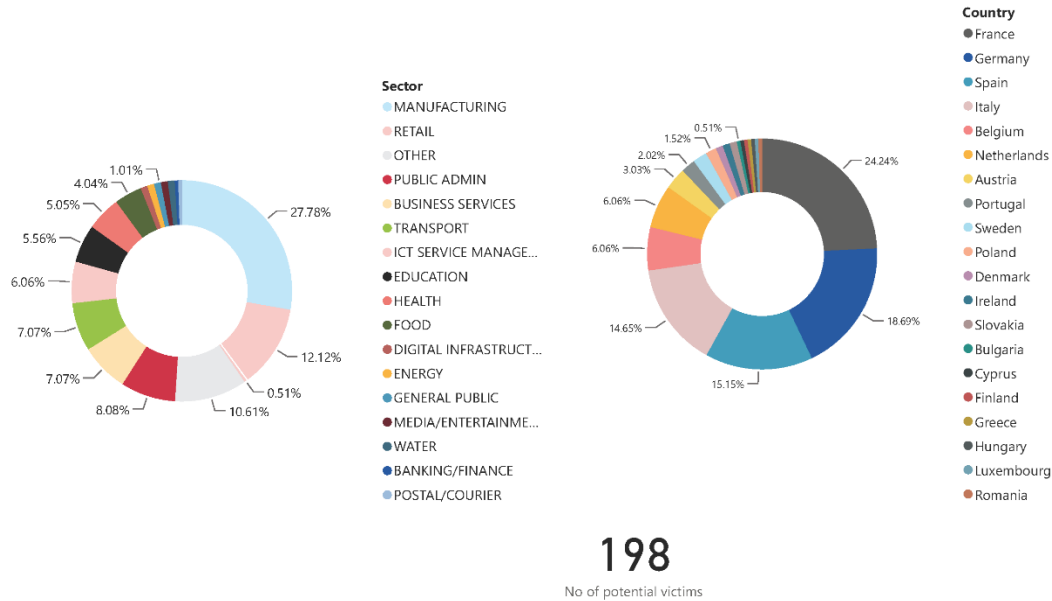
Figure 27: Five Most active Ransomware groups on the EU Landscape



In Figures 27, 28 and 29, we can observe a detailed visualization of the aforementioned three distinct ransomware groups, focusing on their operations in the EU.



Figure 28: Lockbit breakdown on countries and EU sectors



Notably, the most targeted sector varies across all three groups, indicating a diverse range of targets within each group's operations. However, this contrasts with the global perspective, where Lockbit and 8base have displayed a heightened focus on the manufacturing sector and the retail sector, while the CL0p group has directed its attention towards ICT service management.

Figure 29: 8Base breakdown on sectors and EU countries

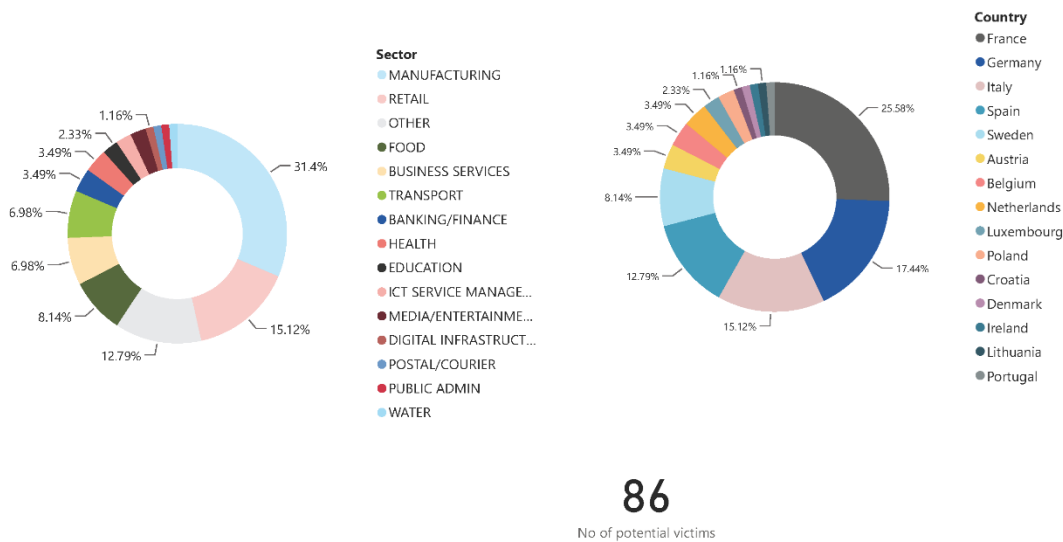
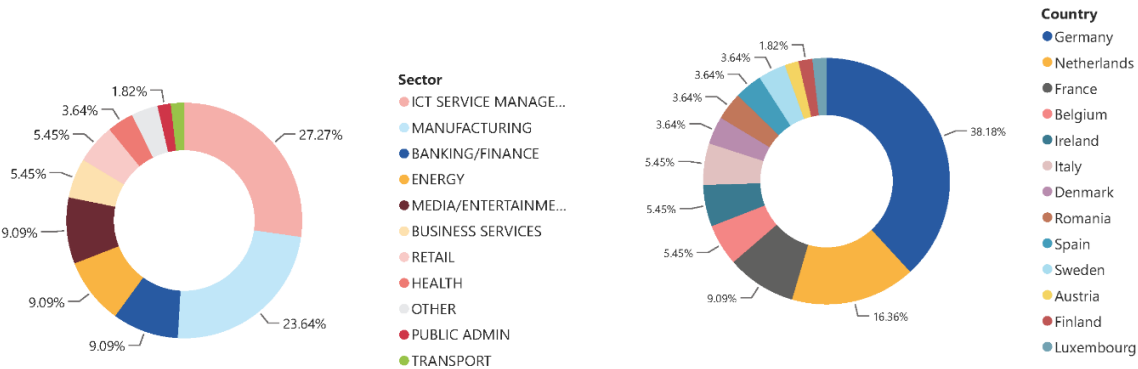


Figure 29: CL0P group breakdown on sectors and EU countries



55

No of potential victims

The information presented here has been derived by merging data collected from the leak sites associated with various extortion groups and supplementing it with Open-Source Intelligence (OSINT). Different statistics from different vendors also confirm LockBit as the most active ransomware gang in 2023²⁴⁰ with CIOp however accounting for more than half of all ransomware incidents during the second half of 2023²⁴¹.

4.2 LOCKBIT CIRCLE OF LIFE: RISE, FALL, POTENTIAL RESURGENCE WITH RECYCLED VICTIMS

LockBit rapidly ascended to prominence as the dominant ransomware group through its RaaS model, leveraging a vast affiliate network to launch frequent attacks. Targeting smaller businesses for quicker returns amplified its financial success. As reported in ENISA's previous ETL, LockBit consistently ranked as the most active ransomware family²⁴².

However, a coordinated law enforcement operation, named Operation Cronos²⁴³, struck a significant blow. On February 20, 2024, authorities seized LockBit's infrastructure, recovered decryption keys for thousands of victims, and took control of its data leak site. The indictment of key operator Dmitry Yuryevich Khoroshev on May 7, 2024²⁴⁴, further impacted the group.

Despite these setbacks, LockBit has demonstrated remarkable resilience. While the group has managed to reconstitute its operations, the extent of its resurgence has been exaggerated. A Trend Micro report revealed that a substantial portion of victims claimed on LockBit's new data leak site were either reuploads of previous attacks or misattributed to the group.²⁴⁵

While LockBit remains a formidable threat, its capacity to maintain its previous level of dominance is increasingly challenged by law enforcement actions and the revelation of inflated victim claims.

²⁴⁰ https://www.guidepointsecurity.com/wp-content/uploads/2023/04/GRIT_Ransomware_Report_Q1_2023.pdf.

²⁴¹ <https://www.reliaquest.com/blog/ransomware-q2-2023-victim-count-hits-new-heights/>.

²⁴² <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.

²⁴³ <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>.

²⁴⁴ <https://therecord.media/lockbitsupp-suspect-accused-lockbit-ransomware-gang>.

²⁴⁵ https://www.trendmicro.com/en_us/research/24/d/operation-cronos-aftermath.html.



4.3 RANSOM DEMAND VS. RANSOM PAYMENT

Ransomware attacks remained a persistent threat throughout the reporting period, with a consistent rate of incidents. While the frequency of attacks held steady, a notable shift emerged in victim behaviour. An increasing number of organisations declare to pay ransom demands, signalling a growing resilience against these cyber-attacks. When payments are made, they often fall short of the initial amounts demanded, indicating that successful negotiation tactics were employed by victims^{246 247 248}.

Several factors contribute to this evolving landscape. Enhanced cybersecurity measures, including robust backup and recovery strategies, have empowered organisations to withstand ransomware attacks without financial capitulation. Additionally, intensified law enforcement efforts against ransomware groups have created a more hostile environment for cybercriminals, reducing the perceived risk of refusing payment. As victims become more aware of the potential consequences of paying ransoms, such as reinfection and funding illicit activities, they are increasingly opting to explore alternative recovery paths.

However, the overall trend of decreased ransom payments was punctuated by a stark outlier. A record-breaking ransom payment of US\$75 million was extorted from a single company²⁴⁹, a staggering sum that nearly doubled the previous highest-known pay-out. This extraordinary incident underscores the immense financial risk posed by ransomware attacks and the potential for catastrophic consequences if organisations are unprepared²⁵⁰.

While the overall picture suggests a growing reluctance to pay ransoms, the reality remains complex. The decision to pay or not is influenced by various factors, including the nature of the business, the criticality of the encrypted data, and the organisation's risk tolerance.

4.4 LEAKS SITES – RECYCLING – DOUBLE-DIPPING

Even though it first appeared in 2020 during the reporting period, a trend known as 'double-dipping' has increased, where victims are targeted multiple times. This malicious practice involves re-victimizing organisations through various methods. Cybercriminals may exploit previously identified vulnerabilities or use stolen credentials to launch subsequent attacks on the same victim. Exfiltrated data can be repurposed for additional extortion attempts, such as selling it on the dark web or using it to blackmail the victim. Ransomware groups often exaggerate the amount of data stolen or falsely claim to have compromised specific systems to increase pressure on victims^{251 252}.

The practice of ransomware double-dipping has become increasingly prevalent. Cybercriminals employ advanced tactics to re-victimize organisations, often exploiting vulnerabilities or stolen credentials from previous attacks. Several ransomware groups have been observed re-selling stolen data on dark web marketplaces after an initial attack or even recycling the same victims on their leak sites. Ransomware operators frequently exaggerate stolen data or falsely claim compromised systems to increase pressure on victims. The number of victims on a data leak site is inherently incomplete, as those paying ransoms quickly aren't listed. Additionally, some groups post more non-paying victims, skewing the perception of risk²⁵³.

4.5 INCREASED OPERATIONS BY LAW ENFORCEMENT

²⁴⁶ <https://www.sophos.com/en-us/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state#:~:text=The%20average%20ransom%20payment%20came,of%20the%20initial%20ransom%20demand>.

²⁴⁷ <https://www.bleepingcomputer.com/news/security/ransomware-payments-drop-to-record-low-of-28-percent-in-q1-2024/>.

²⁴⁸ <https://www.helpnetsecurity.com/2024/04/19/ransomware-q1-2024-payments/>.

²⁴⁹ <https://www.bleepingcomputer.com/news/security/dark-angels-ransomware-receives-record-breaking-75-million-ransom/>.

²⁵⁰ <https://www.zscaler.com/resources/industry-reports/threatlabz-ransomware-report.pdf>.

²⁵¹ <https://thehackernews.com/2024/04/ransomware-double-dip-re-victimization.html>.

²⁵² <https://www.sentinelone.com/blog/ransomware-evolution-how-cheated-affiliates-are-recycling-victim-data-for-profit/>.

²⁵³ <https://www.bankinfosecurity.com/blogs/ransomware-groups-data-leak-blogs-lie-stop-trusting-them-p-3583>.



Law enforcement agencies significantly escalated their offensive against ransomware groups during this reporting period²⁵⁴. Notable operations include the takedown of Trigona by the pro-Ukraine group UCA in October 2023 even though this was not done by law enforcement²⁵⁵ and the dismantling of Ragnar Locker by multiple European law enforcement agencies in the same month²⁵⁶. In December 2023, the FBI temporarily disrupted BlackCat/ALPHV, a prominent RaaS, though the group later resurfaced under suspicion of an internal scam²⁵⁷.

LockBit in February 2024 during Operation Cronos²⁵⁸, when law enforcement compromised its infrastructure. Despite this, LockBit persists, employing questionable tactics such as data recycling and fabricated victim claims. The subsequent exposure of LockBitSupp's identity by law enforcement led to an increased volume of victim announcements on LockBit's data leak site and a reduced online presence for LockBitSupp.

4.6 SHIFTING FROM ENCRYPTION TO DATA EXTORTION CONTINUES – MOTIVATION VARIES FROM OPPORTUNISTIC TO BIG GAME

The trend of ransomware and extortion attacks continued to evolve and expand, posing a significant threat in this reporting period. This builds upon observations from the previous report, highlighting the continuous growth of this cybercrime. One interesting aspect on the cyber extortion was that the tactics employed go beyond traditional ransom demands. The ALPHV/BlackCat ransomware group has taken extortion to a new level by filing a fake SEC complaint against a victim who didn't pay. This showcases the evolving tactics cybercriminals use to pressure victims^{259 260}.

We noticed that 'big game hunting' is still relevant; actors such as the Dark Angels ransomware group, which operates the Dunghill data leak site, emerged around May 2022. The group has conducted some of the largest ransomware attacks yet has managed to attract minimal attention²⁶¹. Nevertheless, most threat groups go for an opportunistic approach as shown in the previous graphs by the variety of sectors and geographical spread. Their victims include smaller businesses, with less than 1,000 employees and are 4.2 times more likely to be impacted. This might be due to the sheer number of small businesses, making them easier targets in a broad 'harvest' by attackers aiming to hit anyone who is vulnerable²⁶².

²⁵⁴ <https://quointelligence.eu/2024/06/analyzing-shift-in-ransomware-dynamics/>.

²⁵⁵ https://twitter.com/UCA_ruhate/status/1714503030849032476.

²⁵⁶ <https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop>.

²⁵⁷ <https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant>.

²⁵⁸ <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>.

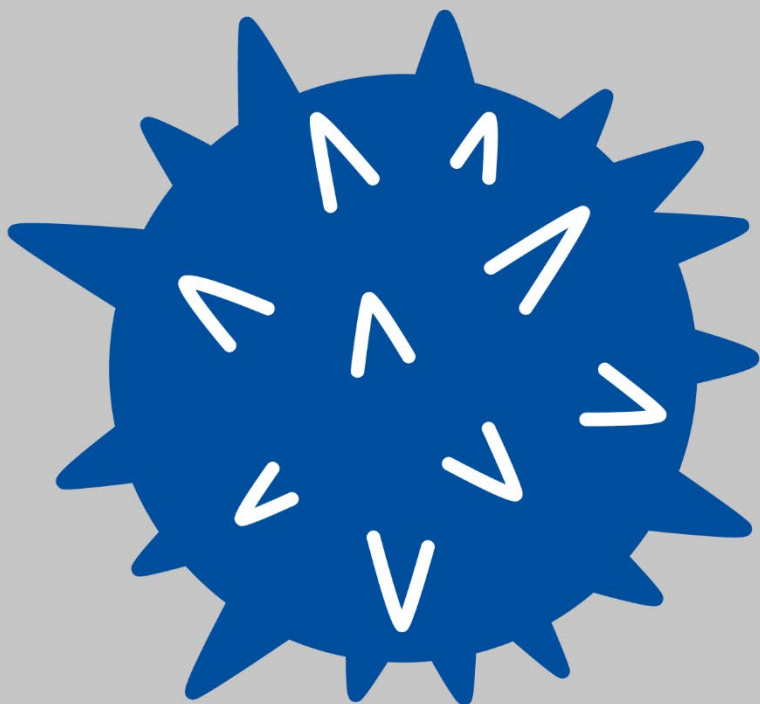
²⁵⁹ <https://www.bleepingcomputer.com/news/security/ransomware-gang-files-sec-complaint-over-victims-undisclosed-breach/>.

²⁶⁰ <https://www.reliaquest.com/blog/q2-2024-ransomware/>.

²⁶¹ <https://www.zscaler.com/resources/industry-reports/threatlabz-ransomware-report.pdf>.

²⁶² <https://www.reliaquest.com/blog/q2-2024-ransomware/>.



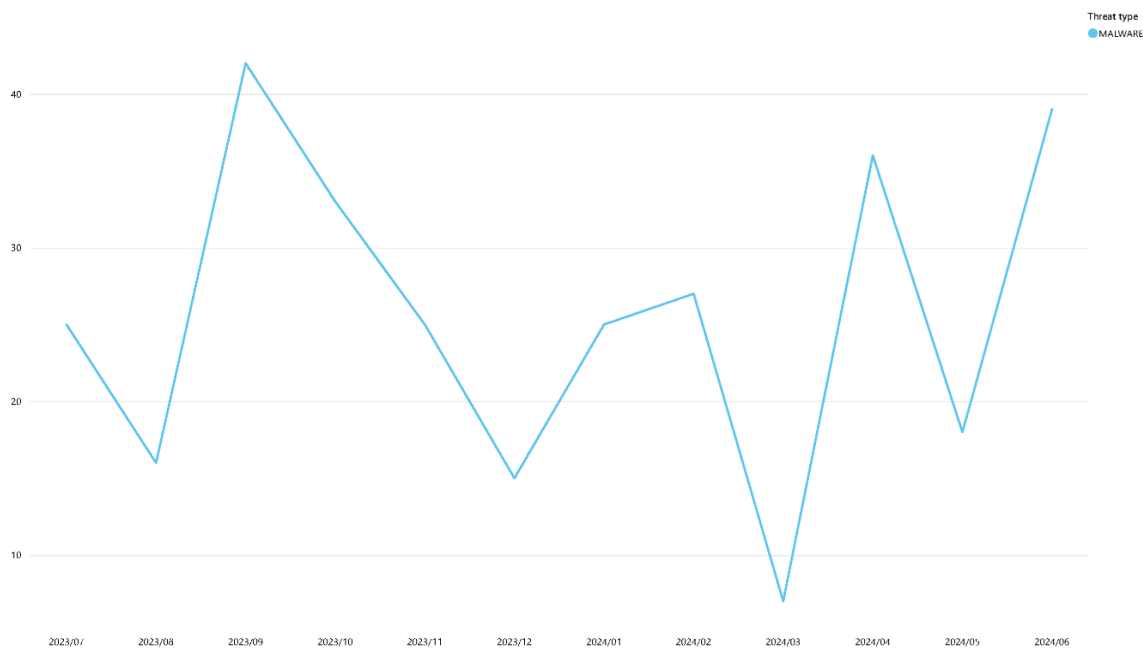


5. MALWARE

Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system²⁶³. Examples of malicious code include viruses, worms, trojan horses or other code-based entities that infect a host²⁶⁴. Malicious actors develop malware or acquire it through **Malware-as-a-Service (MaaS)** to carry out malicious cyber campaigns and support their operations, gaining and retaining control over assets, evading defences and conducting post-compromise actions²⁶⁵. Consistent with previous ETL reports, we classify malware as a distinct prime threat compared to ransomware, given the significant prevalence of ransomware strains across the landscape and their particular motivation that necessitates dedicated and focussed attention. At the same time, the threat of malware remains at a high level, with threat actors continuously evolving their approaches and inventing new means, TTPs and malware families to make it more difficult for defenders and cybersecurity professionals to implement proportionate mitigation controls.

Depending on the goal of the threat actor, malware functionality can range from getting control over **systems** and **networks** (e.g. botnets), over **data** (e.g. information stealing), to allowing **remote access** to infected networks (e.g. Remote Access Trojans (RATs)) and installing other **malicious software** onto the victims' devices (e.g. downloaders). Based on ENISA's dataset, Information stealers were found to be again one of the most frequent sightings during the reporting period. We have noted a significant uptick in incidents related to malware, as illustrated in Figure 31. We can also discern a more detailed breakdown of these threats based on sectors and regions, shown in Figure 32.

Figure 30: Time series of major incidents observed by ENISA (July 2023-June 2024)



²⁶³<https://csrc.nist.gov/glossary/term/malware>.

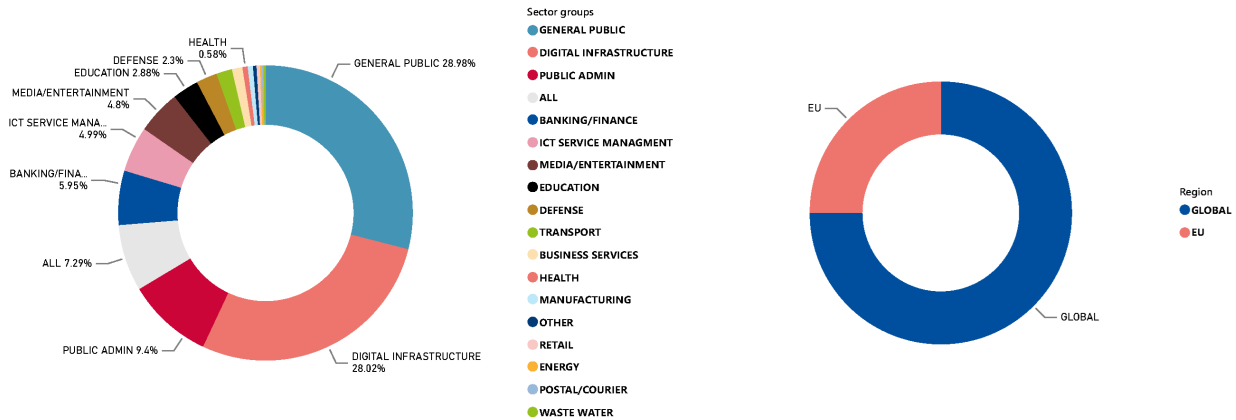
²⁶⁴<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>.

²⁶⁵<https://attack.mitre.org/techniques/T1587/001/>.



It is noteworthy that malware has experienced a resurgence, particularly through infostealers. This increase is linked to numerous discoveries of campaigns from different state-linked actors and the growth of XaaS (Anything as a Service).

Figure 31: Breakdown of Sectors by threat type and region



5.1 MALWARE INFORMATION STEALERS PERSIST AND EVOLVE

Reports indicate a rise in overall malware detections. Information stealers, a type of malware that pilfers sensitive data, continue to be a significant concern. According to information from multiple sources^{266 267} and from data collected by ENISA itself as seen in figure 31, the most common information stealers throughout 2023 and 2024 were:

- **RedLine:** A malware that steals saved credentials, autofill data and banking information appeared in 2020, and saw a wide distribution in different cyber-attacks. Most of the time, however, it was aimed against single users, as its functionality fits best for this purpose. Key targets for the RedLine are data in cryptocurrency wallets, both from desktop versions and browser plugins. Still, it can gather other data, such as FTP/VPN configurations and session tokens for apps such as Discord or Steam.²⁶⁸
- **Raccoon Stealer:** a password stealer and crypto stealer that targets autofill logs, cryptocurrency wallets. In its scope are browser autofill files, cookies and online banking credentials, on top of the ability to pluck cryptocurrency wallets²⁶⁹.
- **Vidar:** A trojan malware that can steal sensitive information via a computer. It offers a modular approach towards data stealing. It also performs self-destruction after successful data exfiltration. Additionally, it is often spread in a bundle with other malware, such as STOP/Djvu ransomware. Methods of selling it to cybercriminals, however, are less unique – it uses Telegram channels dedicated to malware promotion²⁷⁰.
- **Agent Tesla:** a Remote Access Trojan (RAT) written in .NET that has been around since 2014²⁷¹. Initial access brokers (IAB) often use it to exploit corporate networks. This access is then resold to affiliated threat actors, as part of a Malware-as-a-Service (MaaS) business model
- **FormBook malware (also known as xLoader):** similar characteristics to the above to the strains but is known for its form-grabbing techniques to extract data directly from website HTML forms.²⁷²

²⁶⁶ <https://socradar.io/top-10-stealer-logs/>.

²⁶⁷ <https://gridinsoft.com/blogs/infostealer-malware-top/>.

²⁶⁸ <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/>

²⁶⁹ <https://gridinsoft.com/blogs/infostealer-malware-top/>.

²⁷⁰ <https://cybelangel.com/how-have-infostealers-evolved-in-2024/>.

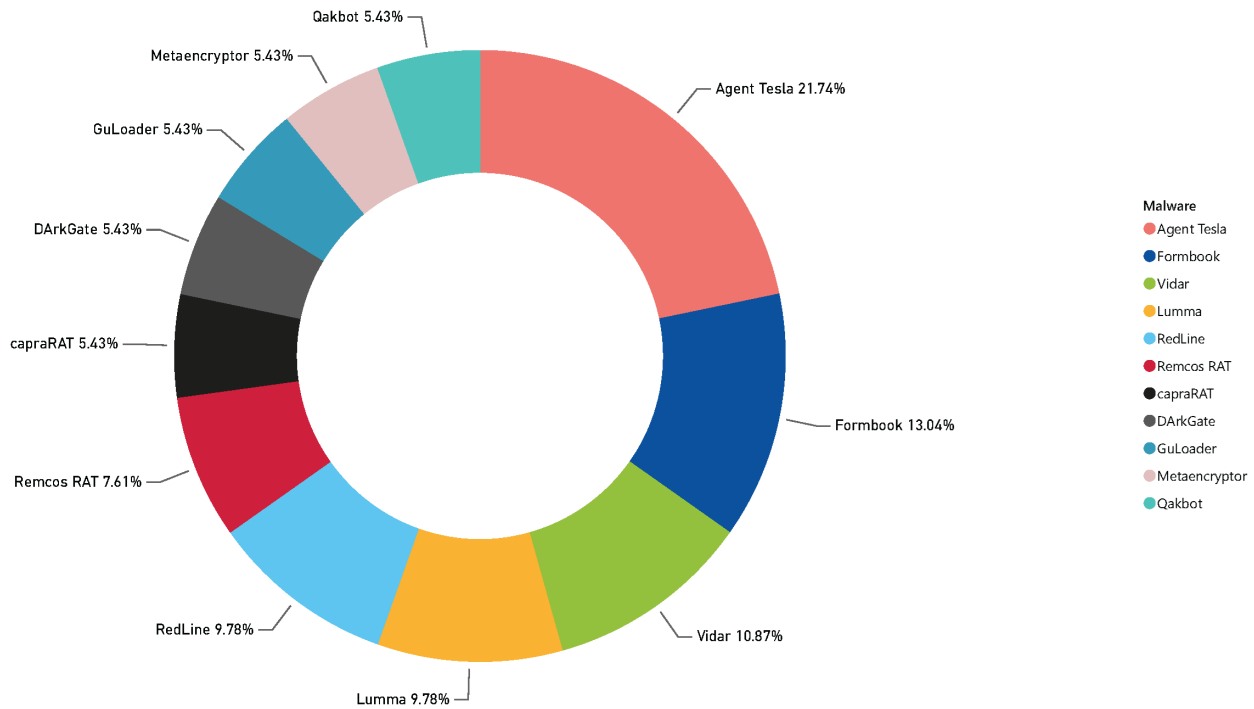
²⁷¹ <https://attack.mitre.org/software/S0331/>.

²⁷² <https://any.run/malware-trends/formbook>



- Lumma Stealer :²⁷³ offered as a malware-as-a-service and it target cryptocurrency wallets, login credentials, and other sensitive information on a compromised system

Figure 32: Most active 10 malware strains



While these top five remain dominant, Information stealers are growing more complex even while the top threats remain familiar.

5.2 NEW TECHNIQUES AS MALWARE DELIVERY MECHANISMS

During the reporting period we noticed Malware being delivered through various methods. Fileless malware, evading traditional antivirus, exploits system tools to execute payloads. Social engineering tricks users into downloading malware through phishing. Malvertising embeds malware in online ads, expanding the attack surface. Additionally, attackers are still using methods like OneNote files, password-protected archives, and deceptive HTML phishing pages more than ever especially after the disabling of Macros in Microsoft files. In addition, watering-hole attacks²⁷⁴ ²⁷⁵ compromise websites to infect visitors, and supply chain attacks target partners to infiltrate larger networks²⁷⁶.

However, a concerning trend that was seen continuously exploitation of zero-day by threat actors. These previously unknown vulnerabilities, for example the quite recent CVE-2024-3400 vulnerability which was incorporated by the cryptominer malware RedTail and is capable of exploiting a variety of devices and applications, demonstrate the versatility of zero-day attacks²⁷⁷.

Another example involves a phishing email containing a malicious SVG file. Clicking the attachment triggers a download of a ZIP file containing an obfuscated Batch file. This elaborate

²⁷³ <https://any.run/malware-trends/lumma>

²⁷⁴ <https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html>

²⁷⁵ <https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/>

²⁷⁶ <https://inquest.net/blog/top-malware-delivery-tactics-watch-out-2023/>

²⁷⁷ <https://www.akamai.com/blog/security-research/2024-redtail-cryptominer-pan-os-cve-exploit>



scheme ultimately delivers the Venom RAT malware, enabling attackers to install plugins and maintain control over victim environments²⁷⁸.

Lastly during this reporting period an increase has been observed in the use of trojanized libraries in software development.²⁷⁹ This trend is likely due to the growing popularity and reliance on open-source libraries in software development. As more developers use these libraries, the potential for malicious actors to target them increases.

5.3 MOBILE MALWARE

During this reporting period a surge in mobile banking trojans was observed, with a concomitant increase in the complexity of their attack vectors. Research indicates a 200% year-over-year growth in malware families targeting banking applications, expanding from 10 to 29 distinct families and from 600 to 1,800 affected applications globally²⁸⁰.

These malicious payloads incorporate a diverse range of functionalities, including Automated Transfer Systems (ATS) to facilitate unauthorised transfers of funds, Telephone-based Attack Delivery (TOAD) for social engineering, screen sharing capabilities for remote device control, and the leveraging of Malware-as-a-Service (MaaS) models for rapid threat distribution²⁸¹.

Emerging threats such as GoldPickaxe²⁸², capable of synthesising deepfake videos using stolen facial recognition data, and Brokewell²⁸³, a Trojan with extensive device takeover capabilities, underscore the evolving nature of the threat landscape in mobile banking. Additionally, the Grandoreiro²⁸⁴ banking trojan, employing advanced obfuscation techniques and targeting a broad spectrum of financial institutions, exemplifies the increasing sophistication of these attacks.

5.4 MALWARE-AS-A-SERVICE

Malware-as-a-Service (MaaS) offerings have become a significant and rapidly evolving threat, particularly since mid-2023. These services provide easy access to a wide range of advanced malware, including information stealers, botnets, and remote access trojans (RATs), at competitive prices. Notably, some MaaS vendors even offer 'malware-for-hire' models, handling the attack execution for clients²⁸⁵.

MaaS thrives on continuous innovation, constantly updating malware to bypass security measures and evade detection (observed since June 2023). Some platforms mimic legitimate software by providing customer support and software updates. Indicators of compromise (IOCs) will vary depending on the specific malware deployed, but suspicious network traffic originating in June 2023 or later, unauthorised remote access attempts and unknown software processes are common signs. MaaS actors often exploit unpatched vulnerabilities in systems and software.

The impact of MaaS is multifaceted. Information stealers, a prominent MaaS offering, target sensitive data such as login credentials and financial information, potentially leading to significant financial losses. Compromised systems can expose sensitive data, impacting individuals and organisations alike. Additionally, deployed malware can disrupt critical systems and operations. Observations since June 2023 highlight the use of MaaS platforms to distribute

²⁷⁸ <https://www.fortinet.com/blog/threat-research/scrubcrypt-deploys-venomrat-with-arsenal-of-plugins>.

²⁷⁹ <https://blog.phylum.io/persistent-npm-campaign-shipping-trojanized-jquery/>

²⁸⁰ <https://www.helpnetsecurity.com/2024/01/03/banking-trojans-mobile-devices/>.

²⁸¹ <https://www.helpnetsecurity.com/2024/01/03/banking-trojans-mobile-devices/>.

²⁸² <https://www.welivesecurity.com/en/eset-research/eset-threat-report-h1-2024/>.

²⁸³ <https://www.threatfabric.com/blogs/brokewell-do-not-go-broke-by-new-banking-malware>.

²⁸⁴ <https://securityintelligence.com/x-force/grandoreiro-banking-trojan-unleashed/>.

²⁸⁵ [Malware as a Service: An Emerging Threat in 2023 - Flare](#).



threats such as Bandit Stealer (information stealer), Lumma Stealer (targets crypto wallets and 2FA), DarkGate²⁸⁶ and other remote access trojans (RATs)^{287 288 289}.

5.5 IMPACT OF LAW ENFORCEMENT ACTIONS

On May 27th and 29th, 2024, a coordinated international law enforcement effort known as Operation Endgame disrupted the activities of multiple dropper malware families. These families, including Bumblebee, IcedID, Pikabot, Smokeloader, SystemBC, and Trickbot, played a crucial role in facilitating ransomware attacks.

Deployed during the first stage of malicious attacks, these droppers have been used to harvest information, maintain control of compromised machines and deploy additional malware families, including ransomware. After deploying malware, the droppers remain inactive or remove themselves. Bumblebee was mainly used for payload delivery, IcedID evolved from a banking trojan to support other cybercrimes, Pikabot was used for data theft, remote access and the deployment of ransomware, while SystemBC provided anonymous communication with command-and-control (C&C) servers^{290 291}.

Late last year, the FBI dismantled a vast network of compromised home and small office routers used by Chinese state-sponsored hackers. Dubbed 'Volt Typhoon', these hackers exploited hundreds of US-based routers with the 'KV Botnet' malware to mask their origins while targeting critical infrastructure within the US and other countries²⁹².

Finally, in August of 2023²⁹³, Qakbot, one of the largest and longest-running botnets to date, was taken down following a multinational law enforcement operation spearheaded by the FBI and known as Operation 'Duck Hunt'. The botnet (also known as Qbot and Pinksliptbot) was linked by law enforcement to at least 40 ransomware attacks against companies, healthcare providers and government agencies worldwide, causing hundreds of millions of dollars in damages according to conservative estimates. However, a small revival was noticed through phishing campaigns just three months later²⁹⁴. Eradicating malware is not a one-time win. Qbot's resurgence highlights the ongoing challenge of staying ahead of adaptable cybercriminals who exploit new technologies.

²⁸⁶ <https://decoded.avast.io/threatresearch/avast-q1-2024-threat-report/>.

²⁸⁷ <https://flare.io/learn/resources/blog/malware-as-a-service/>.

²⁸⁸ <https://darktrace.com/blog/the-rise-of-the-lumma-info-stealer>.

²⁸⁹ <https://www.trellix.com/blogs/research/the-continued-evolution-of-the-darkgate-malware-as-a-service/>.

²⁹⁰ <https://www.securityweek.com/trickbot-and-other-malware-droppers-disrupted-by-law-enforcement/>.

²⁹¹ <https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem>.

²⁹² <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>.

²⁹³ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-242a>.

²⁹⁴ <https://twitter.com/MsftSecIntel/status/1735856754427047985>





6. SOCIAL ENGINEERING

Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons²⁹⁵. While we will discuss this in the context of cybersecurity, notice that social engineering is also used in the physical, non-technological realm. In social engineering, the attacker will in fact exploit the human factor, often also considered as the weakest link in any security chain, for its malicious purpose²⁹⁶. To do so, the attacker will often pose (impersonation or persuasion) as a trusted person or source to gain its victim's trust. Different techniques are used today to achieve these goals²⁹⁷:

Phishing aims to trick recipients into clicking and revealing sensitive information such as passwords, credit card numbers or personal data. Attackers use deceptive emails, messages or links to websites that appear legitimate. **Spear-phishing** is like phishing but highly targeted. To appear even more convincing, attackers customise messages based on specific information about the organisation or specific target. Often, open-source information gathering (OSINT) is used by threat actors to investigate their target.

Smishing is an attack that uses mobile text messages (SMS), impersonating a reputable company or trustworthy actor. The term is a combination of SMS (short message service) and phishing.²⁹⁸

Vishing is a form of phishing that occurs over voice communications, usually phone calls. Attackers impersonate trusted entities and persuade victims to reveal sensitive information. With the rise of AI, it has become much easier to generate audio from a baseline recording. Next to these phishing techniques, we also discuss approaches used by attackers to convince targets, including but not limited to²⁹⁹:

Pretexting is the approach when a malicious actor creates a fabricated scenario or *pretext* to obtain information. Pretexting often involves **impersonation**, where the actor pretends to be someone else, either online or in person, to gain trust and manipulate the target into disclosing confidential information or taking specific actions.

Business Email Compromise (BEC) leverages pretexting by using existing email chains to convince a victim to perform an action. In addition CEO fraud, a sub-set subset of business email compromise (BEC), leverages pretexting by impersonating a company's CEO or high-ranking executive to con other employees, partners, or vendors into a scam.

During this reporting period, a noteworthy increase in social engineering incidents was observed towards the end of H2 2023, as illustrated in Figure 32. Moreover, a more granular view of these threats taking into account sectors and regions is available. One crucial takeaway is that social engineering campaigns, in various forms, persist as a substantial threat to users as evidenced in Figure 33.

²⁹⁵ <https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering>.

²⁹⁶ https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html.

²⁹⁷ <https://www.consilium.europa.eu/en/policies/cybersecurity/cybersecurity-social-engineering/>.

²⁹⁸ <https://bics.com/press-releases/bics-blocks-87-million-euros-worth-of-fraud-attacks/>.

²⁹⁹ <https://www.consilium.europa.eu/en/policies/cybersecurity/cybersecurity-social-engineering/>.



Figure 33: Time series of major incidents observed by ENISA (July 2023-June 2024)

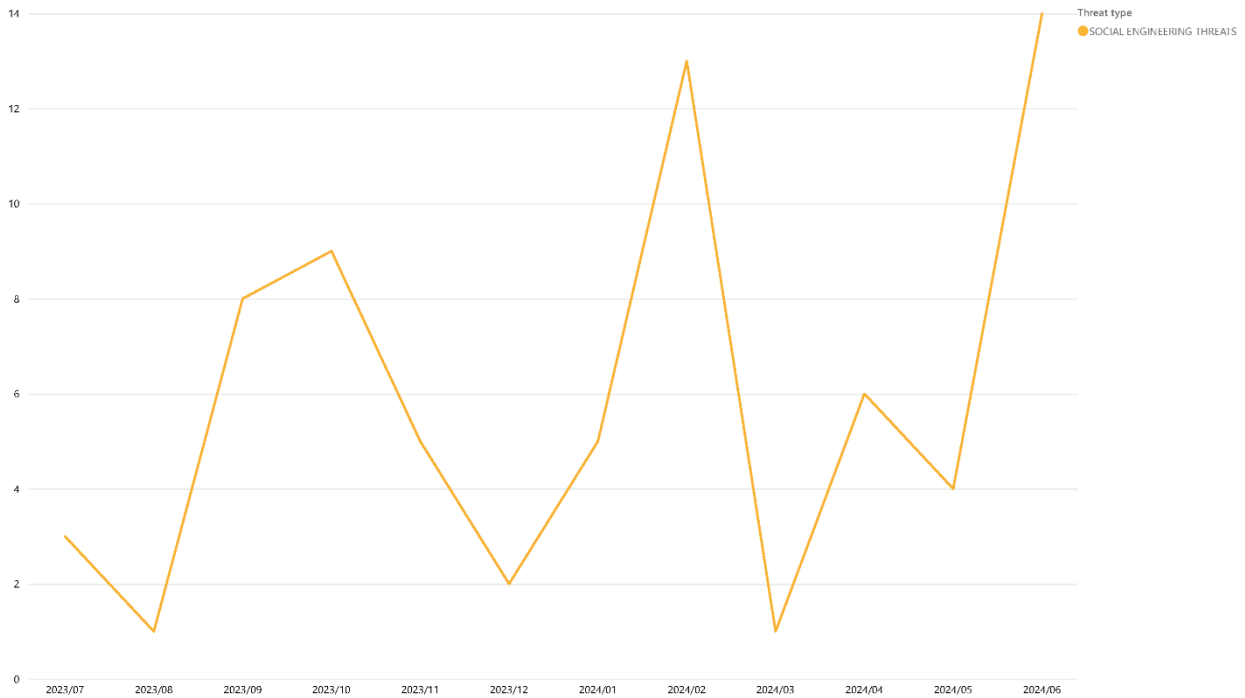
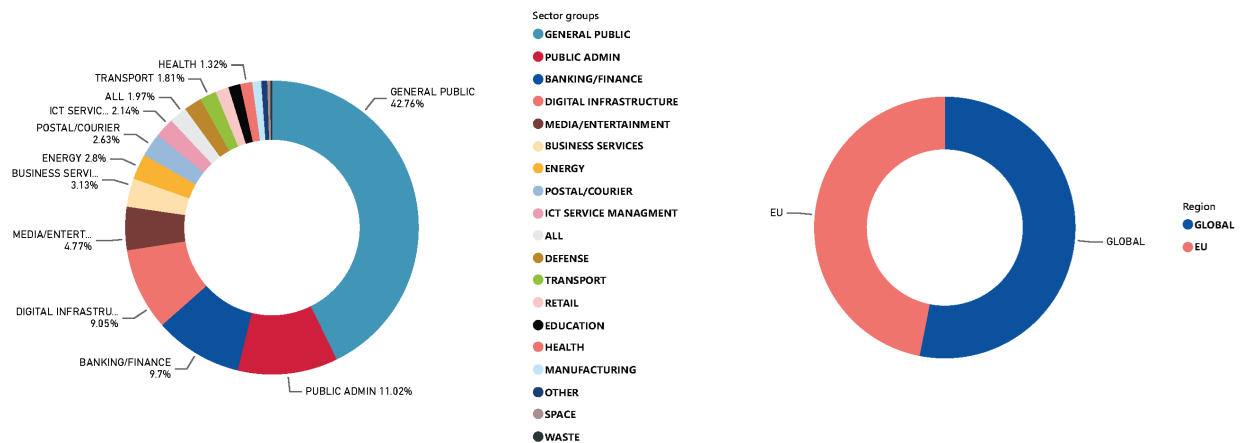


Figure 34: Break down of Sectors by threat type and region



6.1 PHISHING INCIDENTS REMAIN A MOST IMPORTANT INITIAL VECTOR

Phishing and pretexting via email continue to be the leading cause of cybersecurity incidents. According to Verizon, phishing and pretexting accounts for 73% of breaches of social engineering incidents. Business email compromise, which falls under pretexting in the Verizon statistics, continues to have an important financial impact. While the median transaction remained stable, it still accounts for 50K USD in losses. An important addition in this report is that, of all the victims who reached out to law enforcement, they were able to get back 79% of their losses in half of the cases.³⁰⁰ The FBI reports that, in 2023, they received more than 22,000 complaints relating to Business Email compromise with adjusted losses of over 2.9

³⁰⁰ 2024 Data breach Investigations Report – Verizon.



billion USD³⁰¹. IBM reports, throughout 2023, an average cost of 4.67M USD for a data breach with Business email compromise as the initial attack vector. Social Engineering as an initial vector is reported as having an average cost of 4.55M USD in general. Phishing in general was reported as most prevalent attack vector (16%) and the second most expensive at USD 4.76M USD, while 17% originated through business email compromise³⁰².

Another IBM report also concludes that a total of 30% of the incidents they managed in 2023 were related to phishing³⁰³. Also for 2023, Mandiant saw exploits used as the most prevalent initial infection vector (38% of intrusions) followed by phishing in second place. However, phishing declined globally in 2023, with 17% of intrusions, compared to 22% in 2022. When looking at EMEA specifically, we can see phishing attacks falling back to 16% of intrusions for 2023³⁰⁴.

Avast states that on the mobile device landscape, more than 90% of all threats blocked in the last quarter of 2023 originated from scams and similar threat types (which includes phishing at 30%, scams at 45%, and others)³⁰⁵. In the Q1 2024 Phishing Activity Trends Report, the APWG (Anti-Phishing Working Group) observed almost five million phishing attacks throughout 2023, marking it as a record year. In the first quarter of 2024, APWG observed just under 1 million phishing attacks, the lowest quarterly total since Q4 2021. This number is significantly lower than the 1.6 million attacks seen in Q1 2023, which was the highest quarter recorded in APWG's historical observations. Overall, the number of attacks per month remained stable from June 2023 to March 2024³⁰⁶. These observations are not all aligned, but they do show that a decline in phishing was ongoing from 2023 to 2024.

Apart from initial access vectors, phishing also dominates the ranks of cybercriminals. Phishing is the top digital crime type identified by the FBI³⁰⁷ by far, followed by personal data breach, non-payment / non-delivery, extortion and the tech support categories.

6.2 TOP PHISHING BRANDS

Check Point Research identified the following top spoofed brands based on their overall appearance in brand phishing events during Q4 2023: Microsoft (33%), Amazon (9%), Google (8%), Apple (4%), Wells Fargo (3%)³⁰⁸. For Q1 2024 we mainly saw an increase for Microsoft and LinkedIn: Microsoft (38%), Google (11%), LinkedIn (11%), Apple (5%), DHL (5%)³⁰⁹.

IBM reports similar data, although not identical. For 2023, the most spoofed brands included Google, Telegram, Microsoft, Visa and Apple³¹⁰.

In these Check Point statistics, Microsoft maintains a leading position as the most frequently impersonated brand, accounting for 38% of all brand phishing attempts. Considering the market share of Microsoft and Google in the Desktop Operating Systems, Cloud and Office productivity, this is no surprise. An interesting observation is the notable rise in the impersonation of LinkedIn, which emerged as a significant target in Q1 2024, accounting for 11% of brand phishing attempts. This indicates a shift in cybercriminal strategies, possibly targeting professional networks to exploit personal and corporate information. In the section on *Social engineering through job search platforms* we will continue to elaborate on this topic.

³⁰¹ FBI 2023 Internet Crime Report.

³⁰² IBM – Cost of a data breach report 2023.

³⁰³ IBM X-Force Threat Intelligence Index 2024.

³⁰⁴ Mandiant M-Trends 2024 Special Report.

³⁰⁵ Avast Q1 2024 Threat Report.

³⁰⁶ APWG Trends Report Q1 2024.

³⁰⁷ https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

³⁰⁸ Check Point - Brand Phishing Report 2023.

³⁰⁹ Check Point - Brand Phishing Report 2024.

³¹⁰ 2024 IBM X-Force Threat Intelligence Index.



6.3 TRUSTED ENTITIES IMPERSONATION PHONE CALLS.

Several EU countries have published alerts³¹¹, warning about social engineering over the phone along with USA-based CISA³¹². This is an example of the type of phishing called vishing, which occurs over phone calls, with attackers impersonating a trusted entity, trying to persuade victims to reveal sensitive information. Scammers were impersonating CISA employees, demanding their victims send money. One month earlier, the US Federal Trade Commission (FTC) released a similar press release, warning about phone-based social engineering³¹³. According to this release, the median loss to FTC impersonators increased from 3,000 USD in 2019 to 7,000 USD in 2024.

According to the 2023 Internet Crime Report, published by the Federal Bureau of Investigation (FBI), more than 14,000 complaints were filed concerning government impersonation scams. This represents an increase of 63% in reported cases compared to previous years. The financial impact of these schemes is equally alarming, with reported losses amounting to almost 400M USD. It is important to note that these figures only account for incidents involving government institutions within the United States and are based solely on reported cases, likely underestimating the true scale of the problem. Note that these impersonation calls are still manual and performed by a human. With the rise of AI generated synthetic voices, this type of attack can become more automated and grow to a much larger scale.

The European Union Agency for Law Enforcement Cooperation (EUROPOL) maintains an online list³¹⁴ with links to the law enforcement agencies of each member state, where cybercrimes can be reported. However, for Europe, there is currently no consolidated data publicly available regarding the number of social engineering incidents through the impersonation of government services.

6.4 SCATTERED SPIDER TARGETED BY LAW ENFORCEMENT

In June 2024, a 22-year-old man from the UK was arrested in Spain for allegedly being part of the cybercriminal group known as Gold Harvest, also referred to as Scattered Spider. This operation is said to be a joint operation between the FBI and the Spanish Police^{315 316}. Scattered Spider stands out for its social engineering attacks and distinctive composition compared to typical cybercriminal organisations. Throughout 2023, the group used SMS phishing (smishing), voice phishing (vishing) to harvest credentials, and phone calls towards helpdesks to manipulate support staff into resetting passwords or multi-factor authentication (MFA) for targeted accounts. They also used previous intrusions at telecom companies to perform SIM swaps, enabling interception of one-time password (OTP) codes. The group targeted IT and INFOSEC employees, presumably because of their access to security applications and documentation that facilitate lateral movement and further account compromises. A smaller number of attacks focused on employees with access to financial resources^{317 318}.

6.5 SOCIAL ENGINEERING THROUGH JOB SEARCH PLATFORMS

Social engineering attacks are increasingly targeting job listing platforms, exploiting the trust inherent in recruitment processes. Cybercriminals and nation-state actors use advanced social engineering tactics to deceive both job seekers and employers, resulting in financial loss, espionage and compromised security.

³¹¹ [NCSC name abused in phishing campaign | News item | National Cyber Security Centre](#)

³¹² <https://www.cisa.gov/news-events/alerts/2024/06/12/phone-scammers-impersonating-cisa-employees>.

³¹³ <https://www.ftc.gov/news-events/news/press-releases/2024/03/federal-trade-commission-warns-scammers-pretending-be-agency-staff>.

³¹⁴ <https://www.europol.europa.eu/report-a-crime/report-cybercrime-online>.

³¹⁵ <https://x.com/vxunderground/status/1801839138263441431>.

³¹⁶ https://murciatoday.com/video-fbi-take-down-uk-hacker-in-spain-for-stealing-27m-usd-of-bitcoins_1000077536-a.html.

³¹⁷ CrowdStrike - Global Threat report 2024.

³¹⁸ https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf.



One of the prominent trends is the creation of fake companies and personas to engage potential targets. Threat actors set up seemingly legitimate businesses with detailed online presences, including websites, social media profiles, and employee personas. These fake entities are used to lure job seekers into downloading malicious software or to infiltrate organisations by getting hired under false pretences. This tactic has been notably used by North Korean groups such as Moonstone Sleet, which used fake companies to trick developers into running malware loaders disguised as skills tests³¹⁹.

Phishing remains a core method. Attackers use recruitment-themed emails and messages that appear highly credible, often personalised with the target's information. These phishing attempts commonly include job offers, interview requests or task assignments that involve downloading malicious files. The 'Contagious Interview'³²⁰ campaign by Lazarus exploited these tactics by posing as recruiters to distribute cross-platform infostealers during fake job interviews³²¹.

Multi-stage infection chains are used to progressively compromise targets. Initial contact may be benign, such as an email or job application, but subsequent interactions introduce malicious elements. For example, the 'Dev Popper' campaign begins with a seemingly legitimate coding task that, when executed, downloads additional malicious payloads, including remote access trojans (RATs)³²². Furthermore, attackers increasingly tailor their campaigns to specific sectors and roles, such as software development, IT and finance, to maximize the impact of their attacks. The 'WarmCookie'³²³ campaign, for instance, targets individuals with job offers that seem relevant to their current employment, increasing the likelihood of engagement³²⁴.

6.6 BYPASSING MFA

Multi-factor authentication is being actively bypassed in social engineering attacks. MFA spamming or *bombing* consists of repeatedly sending MFA push notification prompts, causing the victim to eventually accept it, inadvertently, or just to be able to use the phone again (*MFA fatigue*). This type of attack was noticed in March 2024, targeting Apple iPhone (and Watch) users³²⁵. Cisco Talos investigated their global attack dataset, including 15,000 catalogued push-based attacks from June 2023 to May 2024. Most push-based attacks were unsuccessful, as they are either ignored or reported by users, and only 5% of the sent push attacks were accepted by users. For the users who did accept fraudulent pushes, it typically did not take many attempts, between one and five push requests. Only a very small number were subjected to a 'bombardment' of 20 to 50 requests. On the global scale an interesting finding is that most fraudulent push attempts were sent between 10:00 UTC and 16:00 UTC, aligning slightly ahead of US working hours, and mirroring the target users' working day routines³²⁶.

There has also been a rise in compromises of cloud-based identities secured with multi-factor authentication (MFA). Particularly concerning is the growing use of web proxy or adversary-in-the-middle (AiTM) phishing pages, which can bypass many MFA implementations by stealing sensitive session tokens. Attackers commonly use credential-harvesting forms or phishing pages to collect login details from their victims. These phishing sites, designed to mimic popular login portals, pass the user's credentials and MFA codes to the attacker. AiTM phishing pages go beyond standard credential-harvesting techniques by using infrastructure designed to defeat typical MFA methods. Unlike traditional phishing forms, AiTM pages function as a reverse web

³¹⁹ SC Magazine. (2023). North Korea's 'Moonstone Sleet' targets victims with malicious tools.

<https://www.scmagazine.com/news/north-koreas-moonstone-sleet-targets-victims-with-malicious-tools>.

³²⁰ Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors (paloaltonetworks.com)

³²¹ Dark Reading. (2023). DPRK Hackers Masquerade as Tech Recruiters, Job Seekers.

<https://www.darkreading.com/threat-intelligence/dprk-hackers-masquerade-as-tech-recruiters-job-seekers>.

³²² Bleeping Computer. (2024). Fake job interviews target developers with new Python backdoor.

<https://www.bleepingcomputer.com/news/security/fake-job-interviews-target-developers-with-new-python-backdoor/>.

³²³ Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors (paloaltonetworks.com)

³²⁴ Dark Reading. (2024). WarmCookie Cyberattackers' Backdoor for Initial Access.

<https://www.darkreading.com/cyberattacks-data-breaches/warmcookie-cyberattackers-backdoor-initial-access>.

³²⁵ https://twitter.com/parth220_/status/1771589789143478471.

³²⁶ <https://blog.talosintelligence.com/how-are-attackers-trying-to-bypass-mfa/>.



proxy, sitting between the victim and the legitimate login portal, intercepting not only credentials and MFA codes but also the critical post-authentication session token.³²⁷

6.7 CALL-BACK PHISHING

In last year's ENISA ETL report, we discussed call-back phishing as a hybrid technique combining standard phishing or spear-phishing with vishing, mainly used to bypass technical restrictions when sending a malicious link or file, and to improve the success rate of a spear-phishing campaign by increasing the perceived trustworthiness. For example, the attackers include a phone number into a phishing e-mail, which makes the victim less likely to consider it spam and, thus, the victim is lured into calling³²⁸.

In November 2022, Palo Alto identified the Luna Moth call-back phishing campaign and associated it to the Silent Ransom Group threat actor³²⁹. An FBI notification from November 2023 states that since the previous June, the Silent Ransom Group (SRG) has been conducting callback phishing data theft and extortion attacks, by sending victims a phone number in a phishing attempt, usually relating to pending charges on the victims' account³³⁰.

An analyst publication details how these call-back methods are used by different actors and that they are powered by fraudulent call centres for the delivery of the initial malicious payload³³¹.

6.8 THE USE OF ARTIFICIAL INTELLIGENCE IN SOCIAL ENGINEERING CAMPAIGNS

The use of generative AI has been normalised for end-users and malicious actors. The quality of generated text, images, audio and video has increased strongly over time. Generative AI supports the creation of tailored phishing campaigns, where attackers leverage open-source information from their victims, to create luring and convincing bait text.

Another use case for threat actors is the generation of deep fakes, synthetic images, audio and videos that are almost indistinguishable from reality. In the section on *whaling* and *vishing*, we already mentioned the social engineering case where a finance worker transferred \$25M USD after being in a video call with his CFO and other employees. However, the malicious actor used deepfake technology and all participants of the call were in fact synthetic generations. Today, indeed, threat actors can clone human speech and audio to carry out this type of attack.

Last year's ETL report already warned about the potential of generative AI on the cybersecurity landscape. Back then, real-time deepfake tools were not good enough to be used in a social engineering campaign. This year, based on the current number of incidents, the impact is still limited, but we have a first incident involving convincing generated synthetic video. According to CrowdStrike, a Chinese information operations campaign took place in 2023, likely using images produced using generative AI, and achieved significant engagement on major social media platforms. Besides State-nexus actors, hacktivist groups started using generative AI last year to develop a spam tool for promoting pro-Azerbaijan messages³³².

³²⁷ [M-Trends 2024 | Google Cloud](#)

³²⁸ ENISA ETL Report 2023.

³²⁹ <https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/>.

³³⁰ <https://www.ic3.gov/Media/News/2023/231108.pdf>.

³³¹ <https://www.hhs.gov/sites/default/files/baza-r-call-campaigns-analyst-note.pdf>.

³³² CrowdStrike – Global threat report 2024.





7. THREATS AGAINST DATA

Today, in fact, we live in an interconnected society where cloud, edge and IoT technologies and applications produce huge amounts of data every second³³³. Threats against data aim to block access to data and manipulate (e.g. poison) data to interfere with system behaviour.

A data breach is defined in the GDPR as *any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed* (article 4.12 GDPR). Technically speaking, threats against data can be mainly classified as data breach or data leak. Though often used as interchangeable concepts, they entail fundamentally different concepts that mostly lie in how they happen^{334 335}.

Data breach is an intentional cyber-attack executed by a cybercriminal to gain unauthorised access to release sensitive, confidential or protected data. In other words, a data breach is a deliberate and forceful attack against a system or organisation to steal data.

Data leak is an event (e.g. due to misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data. It does not consider intentional attacks and is sometimes called data exposure.

In addition to data leaks and data breaches, the increasing adoption of ML/AI models at the core of novel distributed systems and decision-making, and the recent spread of large language models (LLM) and generative AI (see Section 7.8 for more details), put data manipulation under the spotlight. Data manipulation attacks modern systems affecting the accuracy of their results either at training (i.e. data poisoning) or inference (i.e. adversarial attacks) time, undermining trust in IT/production systems and society overall, as follows.

Data manipulation is a category of attacks that aims to manipulate trustworthy data into untrustworthy, bugged data, targeting the accuracy and performance of ML/AI as well as the perception of reality by people. It includes **data poisoning**, training-time attacks that manipulate the training set to reduce the accuracy of the trained model or cause the misclassification of specific data points at inference time, **adversarial attacks**, inference-time attacks that consist of specially crafted data points that are routed to the ML model to cause a faulty or wrong inference (misclassification)³³⁶, and **information manipulation**, an intentional attack that creates or shares false or misleading information, targeting people's perception of a specific event.

Threats against data consistently rank high among the leading threats in the ETL and this trend continued during the reporting period of the ETL 2024 report³³⁷. In the last few years, adversaries explored a series of new techniques, and exploited the increasing online presence and use of online services by the general public, as well as the increasing migration to cloud computing and the pervasiveness of ML/AI solutions and models. As already observed in ETL2022 and ETL2023, identity theft is one of the major data breach attacks (in terms of impact and value), where malicious actors use stolen personal data to impersonate a user and cause damage to a target system. Moreover, given the significance of (private and sensitive) data, adversaries are combining more advanced threats to data, such as phishing, ransomware or

³³³ <https://www.domo.com/learn/infographic/data-never-sleeps-11>.

³³⁴ <https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference/>.

³³⁵ <https://www.upguard.com/blog/data-breach-vs-data-leak#:~:text=Simply%20put%2C%20a%20data%20leak,Apps%20data%20leak%20in%202021.>

³³⁶ <https://ieeexplore.ieee.org/document/10175648>.

³³⁷ ITRC 2023 Data Breach Report.

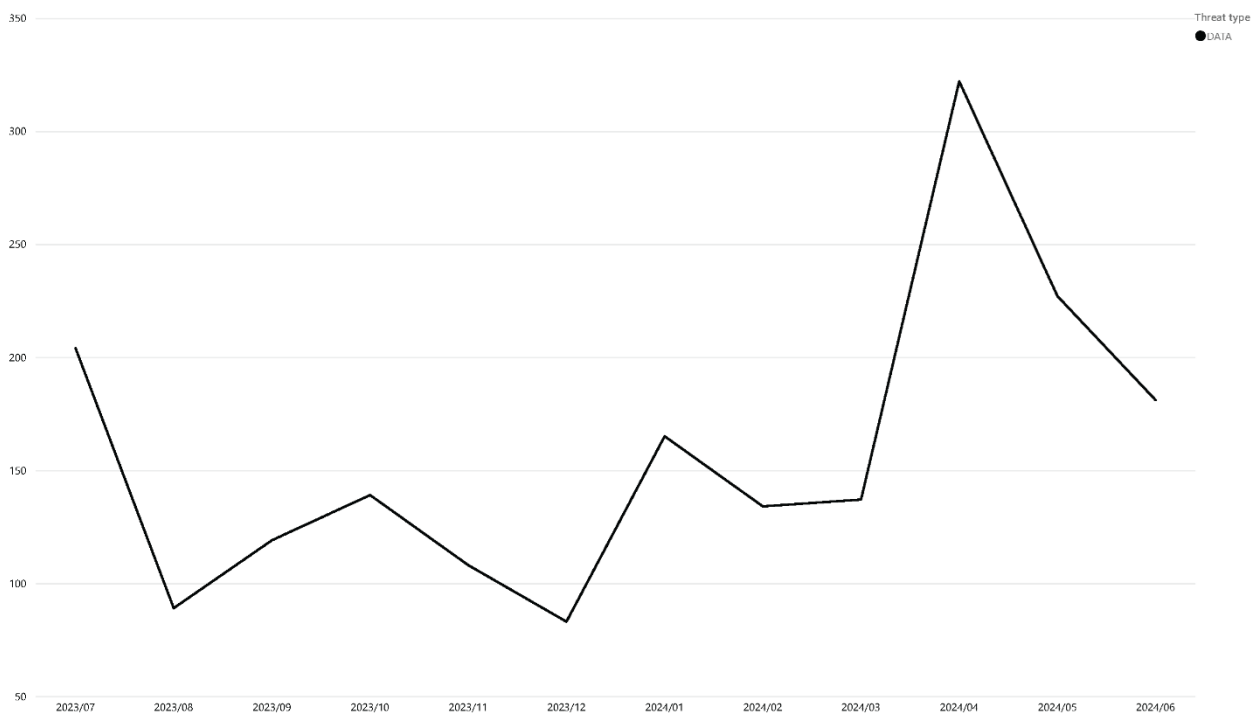


supply chain attacks as well as distributed denial of services and information manipulation. Also, pushed by cloud enhancements, the intended target of a data breach can be separated four, five or six degrees from the real target system/software³³⁸. Finally, given the massive role assumed by ML/AI models in the operations of modern systems, adversaries are focusing on decreasing the accuracy and performance of ML/AI models by launching new attacks, including data poisoning and prompt injection, which focus on generative AI and LLMs as preferred targets.

During this reporting period, we witnessed an increase in the number of reported data compromises (78% increase with respect to 2022) and individuals impacted³³⁹. In this context, we observed an increase in the exploitation of vulnerabilities pushed by MOVEit^{340 341 342} and the impact of system and human errors that more than tripled in 2023³⁴³.

Following up the overall cybersecurity landscape overview in Chapter 1, the following Figures (figure 35 and figure 36) provide a deeper insight into the timeline of observed incidents related to data threats during the reporting period, as well as their break down by sectors and by geographical spread.

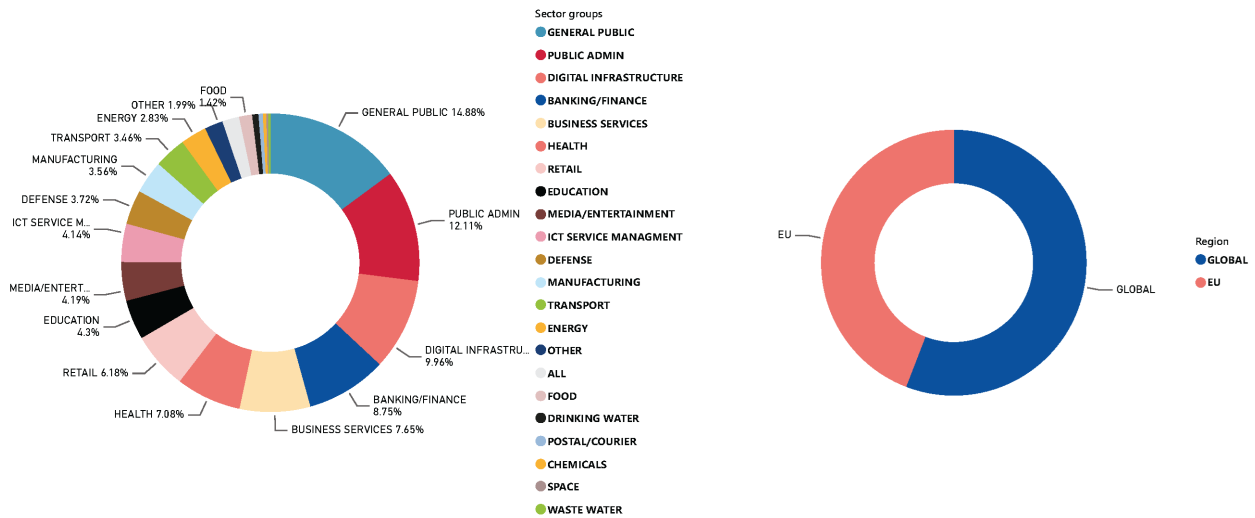
Figure 35: Time series of major incidents observed by ENISA (July 2023 - June 2024)



³³⁸ Experian - 11th 2024 Data Breach Industry Forecast.
³³⁹ ITRC 2023 Data Breach Report.
³⁴⁰ Experian - 11th 2024 Data Breach Industry Forecast.
³⁴¹ <https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/>.
³⁴² M-Trends - 2024 Special Report, Mandiant.
³⁴³ 2023 ITRC Annual Data Breach Report.



Figure 36: Break down of Sectors by threat type and region



7.1 TRENDS

Data becomes an invaluable target for cybercriminals who may want to affect the operations of a system or obtain financial gain. Since 2004, the total number of breached accounts has reached 17.2 billion (number accessed 18 June 2023), with approximately 6.5 billion being unique email addresses³⁴⁴ according to Surfshark. In more detail, each email address is breached three times on average with 82 unique addresses breached per 100 people and 215 accounts breached per 100 people on average. These numbers are on an increasing trend, confirming Microsoft's statement in 2022 that: *Data breaches are inevitable*³⁴⁵.

Data threats in general and data breaches in particular are widening, targeting almost all organisations and populations. In 2023, ITRC reported a record in the number of reported data compromises in the USA (see Section 7.3 for more details). Data breaches, particularly data exfiltration, are increasing in speed, with data exfiltrated in hours, not days. The median time in 45% of the cases for non-extortion attacks is less than a day³⁴⁶.

Thales reported in its 2024 data threat report that 93% of respondents (3,000 organisations worldwide) observed increased data threats. Also, Thales discussed the centrality of compliance claiming that, in 2024, organisations failing a compliance audit reported a breach history in 84% of the cases, 31% with a breach in the previous 12 months. By contrast, organisations passing compliance audits had a breach history in 21% of the cases, with 3% reporting a breach in the previous 12 months.

According to IBM Security, the mean time to identify and contain breaches is stable at 277 days, with a decrease of 1.45% (3 days) in the mean time to identify a breach and an increase of 4.11% (3 days) in the mean time to contain a breach³⁴⁷.

7.2 COSTS OF A DATA BREACH

According to the *Cost of a Data Breach Report 2023* the average total cost of a data breach increased by 2.3% from USD 4.35 million in 2022 to USD 4.45 million in 2023, with a total increase of 15.3% since 2020 and a continuous increase since 2017 (except for 2020). At the same time, a similar trend was observed for the cost of a single record, reaching USD 165 in 2023 (USD 164 in 2022), with an increase of 10.3% since 2020, the only year with a cost

³⁴⁴ <https://surfshark.com/research/data-breach-monitoring>.

³⁴⁵ Microsoft Digital Defense Report 2022.

³⁴⁶ Unit41 PaloAlto Networks, Incident Response Report 2024.

³⁴⁷ IBM Security - The Cost of a Data Breach Report 2023.



decrease. In regards to the EU, in Germany alone³⁴⁸ the damage caused by these attacks has risen by around 29 percent from 205.9 billion euros to 266.6 billion euros. This also exceeds the previous record of 223.5 billion euros from 2021.

Extensive use of security AI and automation reduces the average total cost of a data breach by USD 1.76 million, and the time to identify and contain a breach by 108 days. The average cost also decreases when a DevSecOps paradigm and incident response (IR) planning and testing are used³⁴⁹.

Observed costs change according to the region impacted. The first three spots remained the same for 2022, with the USA, Middle East, Canada having an average cost of USD 9.48 million, USD 8.07 million, and USD 5.13 million, respectively. The highest in Europe is Germany with USD 4.67 million in the fourth spot. According to Experian, the USA and Canada are also among the most targeted countries, with the UK reaching the third spot³⁵⁰.

7.3 IDENTITY THEFT AND SYNTHETIC IDENTITY

The adage *identity is the new perimeter* has been well received by security experts and practitioners and reflects a significant shift in the approach to cybersecurity. Traditionally, organisations relied heavily on network perimeters—firewalls, secure gateways and other boundary defences—to protect their digital assets. However, as the nature of work has evolved with cloud computing, remote work and mobile devices, these traditional boundaries have become less relevant. Instead, the focus has shifted towards identity as a critical security aspect.

In this context, identity abuse, theft and fraud as well as the use of stolen credentials are among the most important sources of concern³⁵¹ and actions at the roots of data breaches^{352 353 354}.

The problem of identity abuse is further complicated by the complexity of identity management that mixes *i*) workforce identity and access management (workforce IAM) and *ii*) customer identity and access management (CIAM)³⁵⁵ and by the increasing reliance on cloud resources³⁵⁶ (see Section 7.7 for more details). According to Thales³⁵⁷, 16% of all accesses are done by external customer identities. Furthermore, Verizon links the decrease of 16% in the total number of individuals impacted to an increasing trend in which attackers use specific information and identity-related fraud and scams³⁵⁸.

This landscape is further worsening due to the increasing evidence that identity criminals are pairing stolen personal information with Generative AI tools and LLMs³⁵⁹. The goal is to make phishing and social engineering attacks more effective and of higher quality, able to target specific businesses or individuals. In this context, a new wave of identity crimes is emerging led by impersonation and synthetic identity.

7.4 DATA BREACH NOTICES AND REGULATORY REQUIREMENTS

In ETL2023, we observed a *substantial decrease in the number of data breach notices, resulting in an important lack of transparency. If almost 100% of notices mentioned attack vectors or details in 2018-2020, decreasing to 93% in 2021, in 2022 this number took a huge hit*

³⁴⁸ [Federal Office for the Protection of the Constitution - Federal Office for the Protection of the Constitution - Presentation of the Bitkom study "Economic Protection 2024". \(verfassungsschutz.de\)](#)

³⁴⁹ IBM Security - The Cost of a Data Breach Report 2023.

³⁵⁰ Experian - 11th 2024 Data Breach Industry Forecast.

³⁵¹ Thales, 2024 Data Threat Report.

³⁵² 2024 Data Breach Investigations Report.

³⁵³ ArcticWolfLabs, ArcticWolfLabs Threat Report 2024.

³⁵⁴ https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf#page=13&zoom=auto,-274,51.

³⁵⁵ Thales, 2024 Data Threat Report.

³⁵⁶ <https://www.tenable.com/blog/cybersecurity-snapshot-a-look-back-at-key-2023-cyber-data-for-genai-cloud-security>.

³⁵⁷ Thales, 2024 Data Threat Report.

³⁵⁸ 2023 ITRC Annual Data Breach Report.

³⁵⁹ ITRC Q1 2024 Data Breach Analysis.



to 58%. This trend accelerated in 2023³⁶⁰. The number of breach notices lacking information about the root cause of an attack nearly doubled year-over-year (more than 98%), with more than 1,400 public breach notices missing information about an attack vector in 2023, 716 in 2022. In this context, only 54% of notices come with actionable information of a data breach; the probability that public companies are hiding actionable information is higher.

Comparing figures in the USA and Europe a crisp difference in the approach to notification emerges with an average of 12.3 data breaches reported each business day in 2023 in the USA, 912 reported each business day in 2022 in Europe³⁶¹. One possible reason is that in the USA there is no single definition of data breaches requiring a notice, often mandated in state law, in contrast with the GDPR in Europe. On top of that, the Federal government in the US has its own set of terms and requirements, adding complexity and making compliance difficult and costly. In Q1-2024³⁶², 68% of year-on-year data breach notices in the USA did not include the root cause, while the total number of notices almost doubled year-on-year.

Market uncertainty, new regulatory requirements, and geopolitical tensions have added substantial risks to data (breach) management and protection³⁶³. In this context, regulations and laws continuously evolve, adding further complexity to data breach management. For instance, in July 2023, the US Securities & Exchange Commission released rules requiring *registrants to disclose material security events*; in the same period, the EU adopted the EU-US Data Privacy Framework (DPF), as a successor of Privacy Shield Framework (2015) and US-EU Safe Harbor Framework (2000). Different guidelines and regulations about artificial intelligence are also coming, such as the first European AI Act. In this complex environment, Wipro cybersecurity³⁶⁴ analysed the stringency of data privacy laws in 23 countries around the world according to data breach notification requirements and overseas data transfer restrictions. Their findings show that 70% of countries *demonstrated greater stringency in breach notification laws, while 17 countries (74%) demonstrated stringency in international data transfers*.

7.5 CLOUD COMPUTING AND DATA BREACHES

Also in this reporting period, the fundamental role of cloud computing as a preferred solution for application and data distribution and delivery requires a careful consideration of data breach attacks in the cloud^{365 366 367 368 369}. A total of 47% of the data in cloud is in fact sensitive³⁷⁰. Multi-cloud adoption is decreasing slightly from an average number of cloud providers of 2.26 per respondent last year to 2.02 this year, while still showing a substantial impact with 51% having two cloud providers and 25% having three cloud providers³⁷¹. Banking, financial services, and insurance respondents moved from an average of 2.02 cloud providers to an average of 2.03.

Thales in its *2023 Data Threat Report: Global Edition*³⁷² reported *cloud assets such as SaaS applications, cloud-based storage, and cloud infrastructure management are the biggest targets for attack*. In particular, 31% of respondents prioritised SaaS applications as the leading attack target in the cloud, followed by cloud storage (30%) and cloud management infrastructure (26%). In this context, a major cause of data breaches in the cloud is still the human factor. In addition, Thales in its *2024 Cloud Security Study: Global Edition* observes that 44% of

³⁶⁰ 2023 ITRC Annual Data Breach Report.

³⁶¹ 2023 ITRC Annual Data Breach Report.

³⁶² ITRC Q1 2024 Data Breach Analysis.

³⁶³ Thales 2024 Data Threat Report (DTR).

³⁶⁴ State of Cybersecurity Report 2023 - Cyber Resilience in an Age of Continuous Disruption, Wipro cybersecurity.

³⁶⁵ IBM Security – Cost of a Data Breach Report.

³⁶⁶ Experian - 11th 2024 Data Breach Industry Forecast.

³⁶⁷ Google, Threat Horizons Q3 2023 - Threat Horizons Report.

³⁶⁸ <https://cloudsecurityalliance.org/press-releases/2023/06/05/new-cloud-security-alliance-survey-finds-saas-security-has-become-a-top-priority-for-80-of-organizations>.

³⁶⁹ Thales, 2024 Cloud Security Study: Global Edition.

³⁷⁰ Thales, 2024 Cloud Security Study: Global Edition.

³⁷¹ Thales, 2024 Data Threat Report: Global Edition.

³⁷² Thales, 2024 Data Threat Report: Global Edition.



respondents reported an attack compared to 14% in the previous year³⁷³. In more detail, user error is at the first spot with 31% and failure to apply multi-factor authentication to privileged accounts reaches a substantial 17%³⁷⁴. Exploitation of known vulnerabilities is at 28% and the exploitation of zero-day/new/unknown vulnerabilities is at 24%³⁷⁵. According to PaloAlto networks, 76% of organisations do not enforce MFA for console users, and 58% of organisations do not enforce MFA for root or admin users³⁷⁶. Also, Cloud Security Alliance claimed that 55% of organisations in its survey *stated they recently experienced a SaaS security incident, which resulted in ransomware, malware, data breaches, and more*³⁷⁷.

According to IBM, data stored in the cloud were a frequent target of data breaches in 2023³⁷⁸. 82% of all data breaches involved data stored in the cloud, with 39% of data breaches spanning across multiple environments (e.g. cloud and on premises) and 27% targeting data stored in the cloud only. Data breaches involving the public cloud and multiple environments have higher costs (USD 4.75 million and USD 4.57 million respectively) than attacks on private cloud and on premises (USD 3.98 million and USD 3.99 million respectively). Similarly, the time to identify and contain a data breach in the public cloud (276 days) and multiple environments (291 days) are larger than the time required on premises (232 days) and in the private cloud (235 days).

To conclude, Cloud Security is a top priority and concern both now (65%) and in the future (72%), the first driver for digital sovereignty and a challenge to compliance and privacy³⁷⁹.

7.6 AI AND THE SURGE OF AI CHATBOTS: SOURCE AND TARGET OF ATTACKS

The spread of (generative) AI and ML at the core of modern IT systems makes data poisoning attacks quite popular. Data poisoning attacks are becoming the most critical vulnerability and threat in (generative) AI and ML, since attackers have access to greater computing power and new tools^{380 381 382}, making the manipulation of elections and data breaches possible³⁸³.

The disruptive impact and the exponential adoption of generative AI chatbots such as OpenAI ChatGPT, Microsoft Copilot and Google Bard, all built around data sharing and analysis, continued in 2023 further shaping how we work, live and play^{384 385}. AI chatbots, as well as large language models, require huge amounts of data to be trained properly and achieve high-quality data generation.

AI chatbots are, at the same time, a powerful tool in the hands of cyber-attackers aiming at data breaches, a powerful tool in the hands of cyber defenders (GenAI for security), and a preferred target for cybercriminals as they are very susceptible to prompt injection and data poisoning, such as malicious data injection into the training datasets (security for GenAI)^{386 387 388 389 390}. As already reported in ETL 2023, a new wave of risks is coming, requiring global cooperation and discussions on inclusive AI governance, as stressed during the G7 summit in 2023³⁹¹. In response to this, the EU has put forward a proposal to regulate AI – the so-

³⁷³ Thales, 2024 Cloud Security Study: Global Edition.

³⁷⁴ Thales, 2024 Data Threat Report: Global Edition.

³⁷⁵ Thales, 2024 Cloud Security Study: Global Edition.

³⁷⁶ Unit41 PaloAlto Networks, Incident Response Report 2024.

³⁷⁷ <https://cloudsecurityalliance.org/press-releases/2023/06/05/new-cloud-security-alliance-survey-finds-saas-security-has-become-a-top-priority-for-80-of-organizations>.

³⁷⁸ IBM Security – Cost of a Data Breach Report.

³⁷⁹ Thales, 2024 Cloud Security Study: Global Edition.

³⁸⁰ <https://blog.barracuda.com/2024/04/03/generative-ai-data-poisoning-manipulation>.

³⁸¹ <https://fedtechmagazine.com/article/2024/01/unpacking-ai-data-poisoning>.

³⁸² <https://www.cobalt.io/blog/data-poisoning-attacks-a-new-attack-vector-within-ai>.

³⁸³ NIS Cooperation Group Publication, Compendium on Elections Cybersecurity and Resilience.

³⁸⁴ <https://www.forbes.com/sites/bernardmarr/2024/02/05/five-generative-ai-chatbots-everyone-should-know-about/>.

³⁸⁵ McKinsey & Co.'s 'The state of AI in 2023: Generative AI's breakout year'.

³⁸⁶ ENISA Threat Landscape 2023.

³⁸⁷ <https://www.wired.com/story/generative-ai-prompt-injection-hacking/>.

³⁸⁸ <https://siliconangle.com/2024/05/21/immersive-labs-warns-generative-ai-bots-highly-vulnerable-prompt-injection-attacks/>.

³⁸⁹ Unit41 PaloAlto Networks, Incident Response Report 2024.

³⁹⁰ Thales – 2024 Data Threat Report.

³⁹¹ <https://www.consilium.europa.eu/en/press/press-releases/2023/05/20/g7-hiroshima-leaders-communique/>.



called AI Act³⁹². The proposal has a risk-based approach centred on people that evaluates, among other criteria, the risks posed by AI systems to health and safety, or the fundamental rights of natural persons, and imposes obligations accordingly. Other countries, such as China and the USA, are also working on regulating AI^{393 394}.

AI chatbots are also targets of data breach attacks. ImmersiveLabs^{395 396} claims that the risk introduced by prompt injection attacks is huge, where individuals can input specific instructions into AI chatbots to retrieve sensitive information and possibly expose organisations to data leaks. For instance, during the Immersive Labs Prompt Injection Challenge in June-September 2023, *88% of prompt injection challenge participants successfully tricked the GenAI bot into giving away sensitive information*³⁹⁷. Also, in general, non-cybersecurity professionals and those unfamiliar with prompt injection attacks can trick bots³⁹⁸. This still happens when chatbots are strengthened with security measures, with users crafting more complex prompts forcing GenAI into revealing confidential information; this results in a scenario where no protocols exist to fully prevent prompt injection attacks, nor a clear definition of liability when generative AI is used. This scenario is introducing new challenges and the need for proper, stringent policies on data governance and robust solutions for cybersecurity³⁹⁹.

Netskope in its report *Cloud & Threat Report: AI Apps in the Enterprise* shows a huge trend in the sharing of sensitive data in generative AI chatbots. Source code is the most common type of sensitive data shared in ChatGPT, 158 incidents per 10,000 users a month, followed by regulated data (e.g. financial and healthcare data, PII), intellectual property excluding source code, and passwords and keys, usually embedded in source code⁴⁰⁰.

In this context, Amazon's Q generative AI chatbot possibly experienced the leaking of confidential data (e.g. the location of AWS data centres) and also suffered from severe hallucinations⁴⁰¹. Similarly, ChatGPT leaked sensitive user data as a result of a possible hack⁴⁰². Samsung banned the use of generative AI from its premises⁴⁰³.

Finally, generative AI can be used as a supporting tool for both attackers and defenders. According to the UK National Cyber Security Centre⁴⁰⁴: *Artificial intelligence (AI) will almost certainly increase the volume and heighten the impact of cyber-attacks over the next two years*. It is used as a support for malicious attacks such as phishing, malware generation and misinformation^{405 406}. More in detail, hackers are using GenAI to create new zero-day ransomware and malware, improve the quality of their artifacts during phishing attacks, as a personal assistant to train hackers themselves, and to support the evasion of defence systems and the generation of deepfakes⁴⁰⁷.

On the other side, AI can also be used to detect and respond to AI threats, such as data breaches, malicious content creation, and AI bias⁴⁰⁸. However, a human-in-the-loop is

³⁹² <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>.

³⁹³ <https://carnegieendowment.org/research/2024/02/tracing-the-roots-of-chinas-ai-regulations?lang=en>.

³⁹⁴ <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>.

³⁹⁵ ImmersiveLabs, 'Dark Side of GenAI' report.

³⁹⁶ <https://siliconangle.com/2024/05/21/immersive-labs-warns-generative-ai-bots-highly-vulnerable-prompt-injection-attacks/>.

³⁹⁷ <https://www.immersivelabs.com/dark-side-of-genai-report/>.

³⁹⁸ <https://www.insurancebusinessmag.com/uk/news/technology/how-generative-ai-is-reshaping-conversations-around-liability-495285.aspx>.

³⁹⁹ <https://www.insurancebusinessmag.com/uk/news/technology/how-generative-ai-is-reshaping-conversations-around-liability-495285.aspx>.

⁴⁰⁰ <https://cybermagazine.com/articles/sensitive-data-like-passwords-and-pii-shared-to-ai-chatbots>.

⁴⁰¹ <https://www.datacenterdynamics.com/en/news/amazons-q-generative-ai-chatbot-leaks-location-of-aws-data-centers/>.

⁴⁰² <https://www.spiceworks.com/tech/artificial-intelligence/news/chatgpt-leaks-sensitive-user-data-openai-suspects-hack/>.

⁴⁰³ https://cybernews.com/security/chatgpt-samsung-leak-explained-lessons/#google_vignette.

⁴⁰⁴ <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>.

⁴⁰⁵ 2023 ITRC Annual Data Breach Report.

⁴⁰⁶ <https://www.tenable.com/blog/cybersecurity-snapshot-a-look-back-at-key-2023-cyber-data-for-genai-cloud-security>.

⁴⁰⁷ <https://www.forbes.com/sites/forbestechcouncil/2023/10/16/generative-ai-is-the-next-tactical-cyber-weapon-for-threat-actors/>.

⁴⁰⁸ <https://www.tenable.com/blog/cybersecurity-snapshot-a-look-back-at-key-2023-cyber-data-for-genai-cloud-security>.



mandatory to oversee important decisions in the detection and response to a given threat⁴⁰⁹. Also, although the adoption of generative AI is clear among organisations, only 21% employ usage policies, just 38% are mitigating their cybersecurity risks and 28% are mitigating their compliance risks⁴¹⁰.

7.7 ADDITIONAL TRENDS

- 67% of breaches have been reported by a benign third-party or by the attackers themselves. In the latter case, the cost of a breach rises by USD 1 million compared to internal detection (which counts for 33% only of all reports)⁴¹¹.
- The adoption of high levels of DevSecOps reduces the cost of a data breach by USD 1.68 million, IR planning and testing by USD 1.49 million⁴¹².
- The cost of a data breach increases by USD 1.26 million in critical infrastructure organisations⁴¹³.
- Mega breaches, attacks with more than one million compromised records, are rare but have a huge impact. For instance, in France, an attack on France's Employment Agency could have affected users who registered over the past 20 years, representing the potential exposure of the data of 43 million users⁴¹⁴. However, in 2023, their cost decreased reaching USD 323 million for attacks with compromised records of between 50 to 60 million⁴¹⁵.
- According to Thales, about 70% of enterprises are unable to classify more than 50% of their sensitive data⁴¹⁶.
- In Europe, more than 386 cases of public database leaks were notified in 2023; only 3.4% of them contained passwords. France, Spain and Italy were the most impacted⁴¹⁷.
- According to CrowdStrike⁴¹⁸: *While ransomware remains the tool of choice for many big game hunting (BGH) adversaries, data-theft extortion continues to be an attractive — and often easier — monetisation route, as evidenced by the 76% increase in the number of victims named on BGH dedicated leak sites (DLSs) between 2022 and 2023.*
- According to Netskope⁴¹⁹, sensitive data are released to genAI apps as much as eight times per working day. In addition, *for every 10,000 enterprise users, an enterprise organisation is experiencing approximately 183 incidents of sensitive data being posted to the app per month.*

⁴⁰⁹ Mandiant, Cyber Snapshot report issue 4.

⁴¹⁰ McKinsey & Co.'s 'The state of AI in 2023: Generative AI's breakout year'.

⁴¹¹ IBM Security – Cost of a Data Breach Report.

⁴¹² IBM Security – Cost of a Data Breach Report.

⁴¹³ IBM Security – Cost of a Data Breach Report.

⁴¹⁴ <https://www.infosecurity-magazine.com/news/french-employment-agency-data/>.

⁴¹⁵ IBM Security – Cost of a Data Breach Report.

⁴¹⁶ Thales – 2024 Data Threat Report.

⁴¹⁷ HI-TECH CRIME TRENDS REPORT 2023/2024, EUROPEAN CYBER THREAT LANDSCAPE, GROUP-IB.

⁴¹⁸ CrowdStrike Global Threat Report 2024.

⁴¹⁹ <https://cybermagazine.com/articles/sensitive-data-like-passwords-and-pii-shared-to-ai-chatbots>.





8. THREATS AGAINST AVAILABILITY: DENIAL OF SERVICE

Availability is the target of a plethora of threats and attacks, among which Distributed Denial of Service (DDoS) stands out.

Distributed Denial of Service (DDoS) targets system and data availability and, though it is not a new threat (it celebrates its 25th anniversary in 2024), it plays a significant role in the cybersecurity threat landscape^{420 421}. Attacks occur when system or service users cannot access relevant data, services or other resources. This can be accomplished by exhausting the system or service and their resources or by overloading the network infrastructure⁴²².

In the last few years, the COVID-19 pandemic and recent wars in Ukraine and the Palestinian Territories substantially modified the threat landscape and all of society, with an increase in state-sponsored and politically motivated attacks and attacks on the critical infrastructures of countries. The year 2022 saw a return of the hacktivist (with political motivations)⁴²³, whose activities increased in 2023 and embraced recent 'conflicts or tensions' including Russia-Ukraine^{424 425}, Taiwan-China⁴²⁶ and Israel-Hamas-Iran^{427 428 429}. In this context malicious actors and groups demonstrated an impressive ability to advance their technical skills and better adapt to the new norm.

DDoS attacks have maintained a stable form over the years, though some interesting points on their evolution may be noted. In the last few years, wars had the widest impact on DDoS, monopolising and influencing DDoS like never before. This trend was reinforced this year with the comeback of hacktivism.

During the reporting period, DDoS attacks grew in scale⁴³⁰, thanks to the availability of DDoS-for-Hire services and tools that reduce the effort of launching DDoS. The trend in the increasing frequency of DDoS attacks also continued, with a predominance of L3/4 (Network and Transport layer according to OSI Model) attacks and the trend in using DDoS as a smokescreen to cover other types of attacks. In 2023, the role of cloud computing as a threat vector increased, as it provides a suitable environment for the creation and execution of VM botnets and their corresponding DDoS attacks, which are becoming increasingly advanced, complex and tech-savvy⁴³¹. This complements the evolution of DDoS in the last few years towards mobile and sensor-based scenarios, where the availability of devices and sensors have become a preferred target of attack due to their limited resources (e.g. battery).

⁴²⁰ Federal Office for Information Security (BSI), The State of IT Sec in Germany, September 2020.

⁴²¹ Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020. <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>.

⁴²² CISA, Understanding Denial-of-Service Attacks, November 2019. <https://www.uscert.gov/ncas/tips/ST04-015>.

⁴²³ <https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivist>.

⁴²⁴ <https://stormwall.network/ddos-report-stormwall-q4-2023>.

⁴²⁵ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁴²⁶ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁴²⁷ CISCO Talos, Year in Review, 2023.

⁴²⁸ <https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/>.

⁴²⁹ <https://www.netscout.com/threatreport/>.

⁴³⁰ Gcore Radar: DDoS Attack Trends, Q3-Q4 2023.

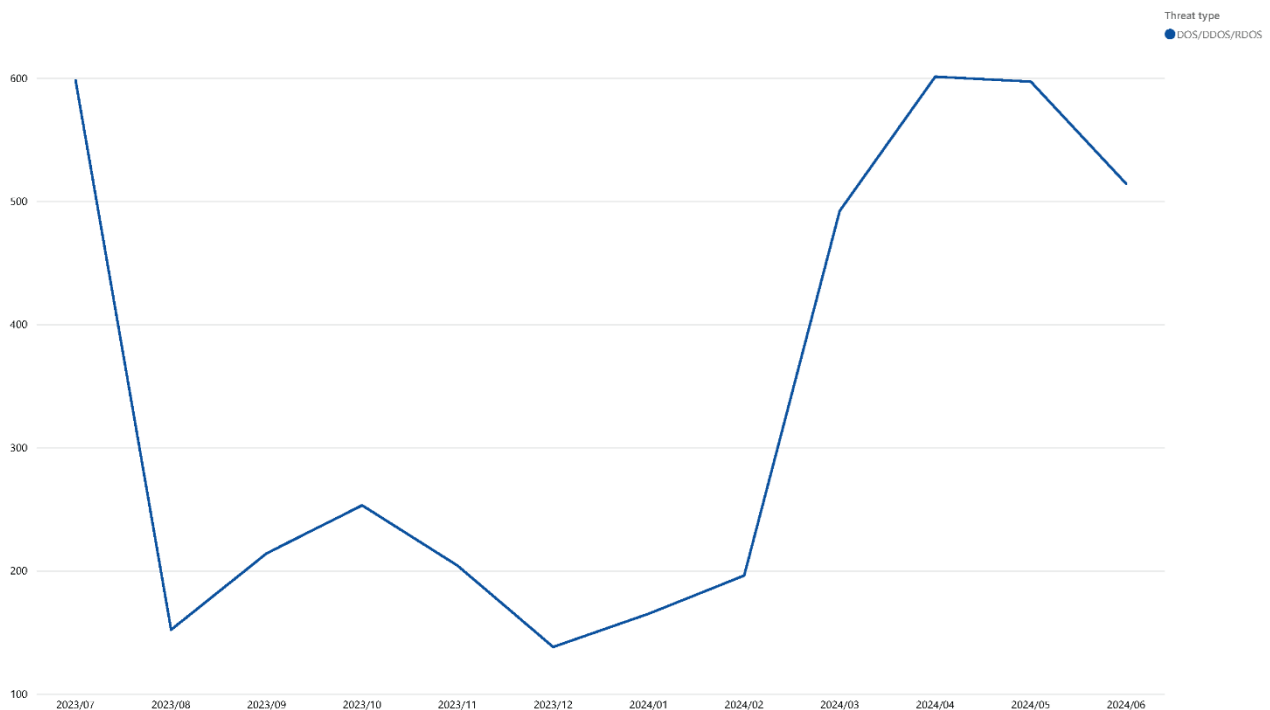
⁴³¹ Microsoft Digital Defense Report 2023.



Also in this reporting period, a significant upsurge in Distributed Denial of Service (DDoS) incidents became apparent in both numbers and dimensions with the turn of the year⁴³² ⁴³³, as depicted in Figure 37. This increase is again due to the growing influence of hacktivism among groups⁴³⁴ opposing various regimes and the ongoing geopolitical tensions worldwide, which have increased in numbers and intensity.

From a regional perspective, the trend observed in 2022 grew in 2023 with a higher proportion of DDoS attacks directed at EMEA in general and European Union (EU) member states in particular, as depicted in Figure 38.

Figure 37: Time series of major Incidents observed by ENISA (July 2022-June 2023)



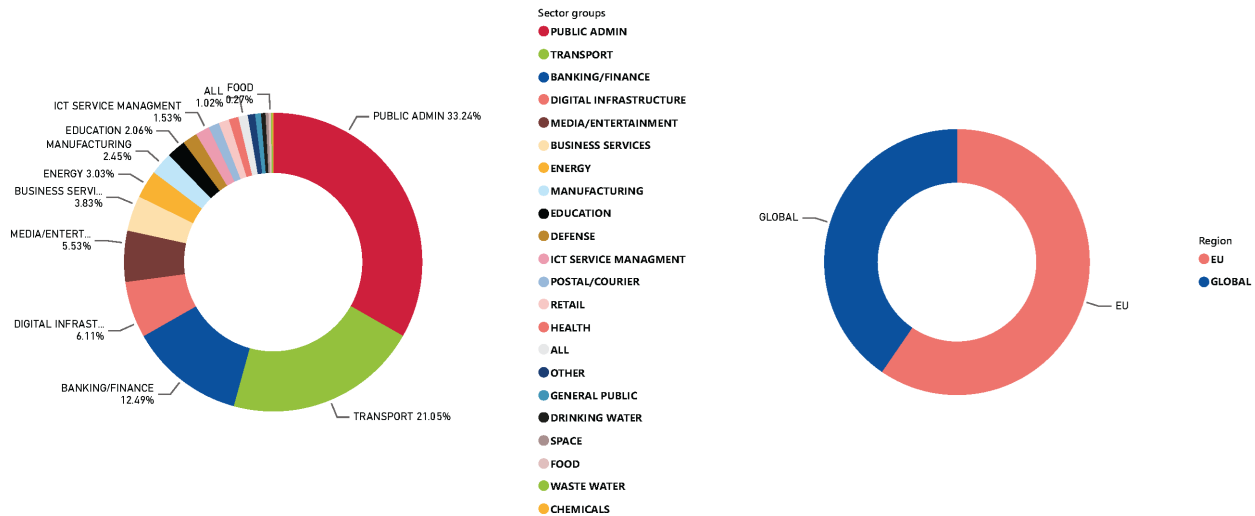
⁴³² Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023.

⁴³³ Gcore Radar DDoS Attack.

⁴³⁴ <https://www.imperva.com/resources/resource-library/reports/2024-imperva-ddos-threat-landscape-report/>



Figure 38: Break down of sectors by threat type and region



8.1 ATTACKS ARE GETTING LARGER, MORE COMPLEX, AND LESS EXPENSIVE

The trend in the increasing frequency, size and complexity (e.g. multi-vector attacks) of DDoS attacks was also confirmed in 2023^{435 436 437}, with thousands of hyper-volumetric DDoS attacks at unseen rates^{438 439}. Akamai observed an unprecedented surge in size, with security vendors and their web sites massively attacked by DDoS⁴⁴⁰. At the same time, the increasing spread of cybercrime-as-a-service ecosystem (see Section 1.2), as well as advanced tools⁴⁴¹, are reducing the cost of launching DDoS attacks at scale⁴⁴².

DDoS reached an average of 1,700 attacks per day according to Microsoft, and 13 million attacks worldwide⁴⁴³. According to Gcore⁴⁴⁴, attacks of unprecedented power were observed in 2023, with a 100% plus increase in the peaks of attack volume in the last three years, from 300Gbps in 2021 to 1.6Tbps in 2023. The attack duration varied from three minutes to nine hours with an average of about one hour. According to StormWall, the number of attacks increased by 63% pushed by geopolitical tensions and war, with the biggest peaking at 1.4Tbps. Google mitigated the largest attack built on HTTP/2 rapid reset which peaked at 398 million rps⁴⁴⁵.

On the same wave, CloudFlare observed thousands of hyper-volumetric HTTP DDoS attacks in Q3 2023, many of which exceeded 100M rps (the largest at 200M rps, eight times larger than the previous record in 2022 when the average attack rate was 30M rps) with an increase of 65% in HTTP DDoS attack traffic and 15% on all DDoS attacks quarter on quarter⁴⁴⁶. In the same period L3/4 DDoS attacks had a minor increase, reaching 2.1M attacks in Q3. The largest attack peaked at 2.6 Tbps and was a UDP flood launched by a Mirai-variant botnet. Mirai-variant botnet is still a common vector of attack and was also involved in the largest attack in Q4 2023

⁴³⁵ Microsoft Digital Defense Report 2023.

⁴³⁶ Gcore Radar: DDoS Attack Trends, Q3-Q4 2023.

⁴³⁷ <https://stormwall.network/ddos-attack-report-2023>.

⁴³⁸ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁴³⁹ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁴⁴⁰ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁴⁴¹ <https://stormwall.network/ddos-attack-report-2023>.

⁴⁴² Microsoft Digital Defense Report 2023.

⁴⁴³ https://www.netscout.com/threatreport/wp-content/uploads/2024/04/Threat_Report_2H2023.pdf - <https://www.netscout.com/threatreport/ddos-threat-intelligence-report/#netscout-visibility>.

⁴⁴⁴ Gcore Radar: DDoS Attack Trends, Q3-Q4 2023.

⁴⁴⁵ <https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps>.

⁴⁴⁶ <https://blog.cloudflare.com/ddos-threat-report-2023-q3>.



that peaked at 1.9 Tbps⁴⁴⁷. In addition, 2024 started with a massive 4.5 million DDoS attacks during Q1, a 50% year-on-year increase^{448, 449}.

In general, most of the attacks are still short (less than 10-20 minutes), small in bandwidth (less than 500mbps), and size (less than 50 pps)^{450 451 452 453}. In Q4 2023, 2% of network-layer DDoS attacks lasted more than an hour and exceeded 1GB ps; 1% of the attacks exceeded 1 million packets per second. In this scenario, however, network-layer DDoS attacks exceeding 100 million packets per second increased by 15% quarter on quarter.

8.2 DDOS FOR HIRE SERVICES

DDoS-for-Hire allows large-scale attacks to be launched by unskilled users having access to DDoS services⁴⁵⁴. Providers can launch attacks on their clients' behalf or provide tools for launching them⁴⁵⁵. DDoS-for-Hire combined with the simplicity of building botnets thanks to the availability of a multitude of insecure devices is a perfect mix for implementing large and disruptive attacks. Larger volumes with greater intensity are pushing the scenario to its extreme⁴⁵⁶.

The dimension of this problem is resulting in an increasing effort in trying to limit DDoS-for-Hire. Europol announced in December 2022 that a joint international law enforcement operation had taken control of about 50 sites that were offering DDoS-for-Hire services to threat actors. The operation called Power Off involved law enforcement from the USA, the UK, the Netherlands, Poland and Germany⁴⁵⁷.

This effort continued in 2023 with the shutdown of 48 DDoS-for-hire service platforms by law enforcement, with six people investigated^{458 459}. This activity is vital to reduce the impact of DDoS-for-hire on the ability of an attacker to launch complex and distributed attacks at low cost.

Despite these notable results, the number of DDoS-for-hire platforms is increasing by 20% on a year on year basis⁴⁶⁰. Continuous monitoring and tracking, on one side, and proactive activities for platform shutdown, on the other side, are a necessity to limit the impact of DDoS.

8.3 DDOS AND CYBERWARFARE

2022 was the year of the return of the hacktivist⁴⁶¹. The DDoS landscape was initially affected by the geopolitical changes introduced by Russia's invasion of Ukraine on 24 February 2022, which then affected the entire reporting period last year⁴⁶². A significant part of the DDoS-related attacks concerned this event and involved actors at different layers, from state-sponsored to simple users, devoting their resources to the cyberwar.

This year the trend continued and strengthened, maintaining a strong connection with cyberwarfare⁴⁶³. In addition to the hacktivism targeting the Russia-Ukraine conflict, this year hacktivism arose in other geographical areas, and especially in the war that followed Hamas'

⁴⁴⁷ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁴⁴⁸ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁴⁴⁹ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁴⁵⁰ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁴⁵¹ <https://stormwall.network/ddos-report-stormwall-q4-2023>.

⁴⁵² <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁴⁵³ <https://ddos-guard.net/info/protect?id=51722>.

⁴⁵⁴ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁴⁵⁵ Microsoft Digital Defense Report 2022.

⁴⁵⁶ <https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivism>.

⁴⁵⁷ Cyber Security Brief (December 2022), January 3, 2023 - Version: 1.0, TLP: CLEAR.

⁴⁵⁸ Microsoft Digital Defense Report 2023.

⁴⁵⁹ <https://www.bleepingcomputer.com/news/security/fbi-seized-domains-linked-to-48-ddos-for-hire-service-platforms/#:~:text=The%20US%20Department%20of%20Justice%20has%20seized%2048,to%20easily%20conduct%20distributed%20denial%20of%20service%20attacks>.

⁴⁶⁰ Microsoft Digital Defense Report 2023.

⁴⁶¹ <https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivism>.

⁴⁶² <https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/>.

⁴⁶³ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.



attack on Israel in October 2023 and later involved Iran^{464 465 466}. Politically motivated hacktivist groups started supporting both sides of the war and claimed responsibility for a variety of attacks including DDoS^{467 468}. Application-layer DDoS attacks in Q4 2023 showed a quarter-on-quarter increase of 1,126% in traffic targeting web sites in the Palestinian Territories, with 1.3 billion DDoS requests and 90% of the traffic attacking the banking domain; a quarter-on-quarter increase of 27% in traffic targeting Israeli web sites, with 2.2 billion HTTP DDoS requests and mostly attacking newspaper, media and computer software domains⁴⁶⁹. On the network layer, the same trends emerged, Palestine being the most targeted territory after China with 68% of traffic (470 TB) being DDoS attacks and Israel in 9th place with 9.83% (2.4 TB). The frame widened at the beginning of 2024 with the explicit involvement of Iran in military operations⁴⁷⁰. In Q4 2023, with the approaching the general election in Taiwan and increasing tensions with China, the DDoS attack traffic targeting Taiwan grew by 3,370% compared to 2022⁴⁷¹.

In this battleground, old (e.g. Killnet, REvil, NoName057 and Anonymous Sudan^{472 473}) and new (e.g. Cyber Army of Russia Reborn) groups showed themselves to be increasingly tech-savvy and politically motivated, changing the landscape of ETL2023 when attacks by Killnet, Anonymous Sudan, and lesser-known groups were mostly uncoordinated and unsophisticated attacks at the outset, suggesting that their main intent was to raise media attention for their cause (Ideology).

Cyber hacktivism has also been accompanied by protests and demonstrations that escalated into disorders in many countries in the world (including Europe and the US)⁴⁷⁴.

8.4 DOS ATTACKS ON CRITICAL INFRASTRUCTURE

With the rise in geopolitical tensions and wars, traditional DDoS attacks have been accompanied by an increasing number of attacks and events that targeted critical infrastructure like ISP and telecommunication providers. Attacks and events include cable cuts, military actions, cyber-attacks, government directed power outages and technical problems⁴⁷⁵. This can all be seen as a kind of DoS on Internet availability.

According to AccessNow^{476 477}, Internet shutdowns are now a global phenomenon with conflicts being the leading driver for such shutdowns. Natural disasters are a new entry as drivers for Internet shutdowns and are causing increasing concerns. In 2023, a record of 283 Internet shutdowns (41% increase) were observed targeting 39 different countries and divided into the following categories: 73 due to conflicts, 63 protests, 12 exams, 5 elections and 4 natural disasters.

Attacks are getting larger with 41.3% of shutdowns (117) affecting people in more than one state, province or region. Taking conflicts into consideration, 6 out of 8 shutdowns in Ukraine observed by AccessNow have been caused by Russia; 16 shutdowns in Palestine have all been caused by Israel. Earthquakes in Turkey and Iraq, and floods in Libya were also the causes of shutdowns during natural disasters. CloudFlare also identified air-strikes as a common cause of

⁴⁶⁴ CISCO Talos, Year in Review, 2023.

⁴⁶⁵ <https://stormwall.network/ddos-report-stormwall-q4-2023>.

⁴⁶⁶ CrowdStrike Global Threat Report 2024.

⁴⁶⁷ CISCO Talos, Year in Review, 2023.

⁴⁶⁸ https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf.

⁴⁶⁹ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁴⁷⁰ <https://www.port.ac.uk/news-events-and-blogs/blogs/us-sanctions-on-iranian-hackers-highlight-growing-concern-about-the-islamic-republics-cyberwarriors>.

⁴⁷¹ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁴⁷² <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁴⁷³ <https://www.akamai.com/lp/soti/high-stakes-of-innovation>.

⁴⁷⁴ <https://www.netscout.com/threatreport/>.

⁴⁷⁵ <https://blog.cloudflare.com/q1-2024-internet-disruption-summary>.

⁴⁷⁶ <https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf>.

⁴⁷⁷ <https://www.accessnow.org/campaign/keepiton/>.



energy outages and Internet shutdowns in Ukraine and observed several such shutdowns in Palestine from October 2023 onwards⁴⁷⁸.

Moreover, this year⁴⁷⁹ ⁴⁸⁰, Internet shutdowns are strongly coupled with grave violations of human rights (51 shutdowns in 11 countries). Also, in various cases, shutdowns are becoming the usual procedure, as in 53 shutdowns across 25 countries in 2023. For instance, shutdowns in Tigray, Ethiopia, have already lasted for 1,153 days, 864 days in dozens of townships across Myanmar and 694 days in Panjgur, Pakistan.

In addition, Cyber Army of Russia Reborn has been targeting operational technology (OT) in the EU and in other countries like Ukraine⁴⁸¹ and USA ⁴⁸². In the beginning of the year, the group has taken credit for multiple water utilities in the US, a wastewater plant in Poland, and a hydroelectric dam in France.⁴⁸³

Finally, according to CrowdStrike⁴⁸⁴, pro-Palestine hackers have targeted critical infrastructure in Israel, including disruptive activity against energy-distribution infrastructure and water pumps. DDoS attacks have also been launched against utility companies.

8.5 DDOS ATTACKS AS A SMOKESCREEN AND HORIZONTAL ATTACKS

DDoS attacks are increasingly used as a distracting tactic, which are followed by more impactful attacks. For instance, in 2022, Imperva observed DDoS attacks followed by Account Takeover attacks (ATOs), Bot attacks or attacks on API endpoints to infiltrate sensitive data: [...] *how large service disruptions often came in parallel with other attack vectors, where, whether intentional or not, DDoS was used as a smokescreen to pivot the defending team's attention away from a simultaneous attack, such as an ATO or phishing*⁴⁸⁵. This scenario often sees DDoS as a decoy for more serious types of attacks such as espionage, increasing business risks and impacting reputation, compliance and supply chain operations⁴⁸⁶.

This trend was confirmed in 2023 by StormWall who reported a 54% increase in the use of DDoS as a means to distract⁴⁸⁷ and by Akamai claiming that attacks on the banking and financial industries were aimed mainly at hitting reputations or distracting security experts while ransomware⁴⁸⁸, data theft and cyber espionage⁴⁸⁹ attacks were being launched. In 2023, multi-vector attacks involved more than 14 vectors acted as smokescreens for triple-extortion attacks (see Section 1.6).

8.6 RANSOM DENIAL OF SERVICE (RDoS)

Threat actors continued leveraging **Ransom Denial of Service (RDoS)** to conduct extortion-based DoS attacks that are financially motivated. RDoS aims to identify vulnerable systems that become the target of the attack and put in place different activities that result in a final request to pay a ransom. RDoS can come in two flavours: i) attack first, ii) extort first. Type i) describes a scenario where a DDoS attack is implemented and a ransom is demanded to stop it. Type ii) describes a scenario where an extortionary letter and proof of harm in the form of a small-scale DoS attack is sent with a demand for a ransom. RDoS attacks are even more dangerous than

⁴⁷⁸ <https://blog.cloudflare.com/q1-2024-internet-disruption-summary>.

⁴⁷⁹ <https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf>.

⁴⁸⁰ <https://www.accessnow.org/campaign/keepiton/>.

⁴⁸¹ <https://slovenia.mfa.gov.ua/en/news/russian-group-cyber-army-russia-reborn-announced-cyber-attacks-critical-infrastructure-slovenia-due-position-countrys-government-regarding-support-ukraine>

⁴⁸² <https://www.state.gov/sanctioning-members-of-the-cyber-army-of-russia-reborn/>

⁴⁸³ <https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearting-sandworm/>

⁴⁸⁴ CrowdStrike 2024 Global Threat Report.

⁴⁸⁵ <https://www.imperva.com/blog/lift-the-ddos-smokescreen-investigate-underlying-attacks/>.

⁴⁸⁶ <https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists>.

⁴⁸⁷ <https://stormwall.network/ddos-attack-report-2023>.

⁴⁸⁸ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁴⁸⁹ https://www.fsisac.com/hubfs/Knowledge/DDoS/FSISAC_DDoS-HereToStay.pdf.



traditional DDoS since they can be completed even if the attacker does not have sufficient resources⁴⁹⁰.

The simplicity of RDoS attacks and extortion tools built on DDoS-as-a-Service (aka DDoS-for-Hire in Section 1.2) are the basis for the adoption of RDoS⁴⁹¹. Thanks to DDoS-as-a-Service, in fact, launching a RDoS attack is increasingly simple while it is still difficult to spot its origin. Spreading malware instead requires more effort in terms of time and planning⁴⁹².

RDoS has moved tactics from double-extortion to quadruple-extortion^{493 494 495 496}. In triple-extortion tactics, *threat actors encrypt and steal data, and also threaten to engage in a distributed denial of service (DDoS) attack against the affected organisation*^{497 498 499}. In quadruple extortion attacks^{500 501}, *ransomware cybercriminals extend the range of the attack to business partners and clients to increase pressure on the victim, with the possibility of business disruptions caused by the ransomware attack*.

According to Unit42⁵⁰², less than 2% of the ransomware cases are RDoS on the global scale. In fact, more effective ransom attacks are available when the assessed objective of the attacker is financial (coercing payment). Cloudflare also observed a decrease in the number of reported RDoS at 8% in Q3 2024⁵⁰³. Finally, according to Akamai⁵⁰⁴, in 2023, gaming and gambling industries were the target of DDoS attacks and triple extortion.

8.7 APPLICATION VS NETWORK ATTACKS

Application attacks have been continuously increasing over the last few years. The role of hyper-volumetric HTTP DDoS attacks has increased since they began in August 2023 with a huge wave of attacks built on the HTTP/2 Rapid Reset vulnerability (CVE-2023-44487)^{505 506}. For example, the largest attack Google ever mitigated peaked at 398 million requests per second⁵⁰⁷. However, 2023 saw a drop of 20% in the number of HTTP DDoS attacks with respect to 2022, a total of 5.2 million HTTP DDoS attacks consisting of over 26 trillion requests. This decrease was particularly sharp in Q4 with a decrease of 18% quarter-on-quarter. In 2024, HTTP/2 has been exploited to execute DDoS, especially the HTTP/2 continuation flood⁵⁰⁸. In this context, Microsoft confirmed that its systems were hit by an application-layer DDoS attack launched by hacker group Storm-1359 that caused disruption in Microsoft 365 (including Outlook on the web and OneDrive) and Azure Portal⁵⁰⁹.

By contrast, the number of network-layer DDoS attacks showed a sharp increase of 85% with respect to 2022 with 8.7 million attacks and 80 PB of traffic. Only considering Q4 2023, Cloudflare observed a 175% year-on-year and 25% quarter-on-quarter increase in network-

⁴⁹⁰ CloudBric, DDoS Extortion Campaigns (Ransom DDoS, or RDoS) To Watch Out For, <https://www.cloudbric.com/blog/2020/11/ddos-rdos-extortion-ransomware-campaign/>.

⁴⁹¹ <https://www.networkcomputing.com/network-security/ransom-ddos-phenomenon-pay-or-get-knocked-offline>.

⁴⁹² Neustar Security, Cyber Threats & Trends: Securing Your Network Pandemic-Style, 2020, <https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pdf>.

⁴⁹³ Unit42, Ransomware Threat Report 2022_1650614560.

⁴⁹⁴ IBM X_Force Threat Intel Index 2022.

⁴⁹⁵ ISSUE 8: FINDINGS FROM 2ND HALF 2021 NETSCOUT THREAT INTELLIGENCE REPORT.

⁴⁹⁶ The Global Economic Forum, The Global Risks Report 2022 17th Edition, 2022.

⁴⁹⁷ https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.

⁴⁹⁸ IBM X_Force Threat Intel Index 2022.

⁴⁹⁹ BleepingComputer, 'US and Australia warn of escalating Avaddon ransomware attacks', <https://www.bleepingcomputer.com/news/security/us-and-australia-warn-of-escalating-avaddon-ransomware-attacks/>, 2021.

⁵⁰⁰ Insikt Group, THREAT ANALYSIS 2022 Annual Report.

⁵⁰¹ The Global Economic Forum, The Global Risks Report 2022 17th Edition, 2022.

⁵⁰² https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.

⁵⁰³ Unit42, Ransomware and Extortion Report, 2023.

⁵⁰⁴ Unit42, Ransomware and Extortion Report, 2023.

⁵⁰⁵ <https://blog.cloudflare.com/ddos-threat-report-2023-q3>.

⁵⁰⁶ <https://www.netscout.com/threatreport/>.

⁵⁰⁷ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁵⁰⁸ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁵⁰⁹ <https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps>.

⁵¹⁰ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵¹¹ <https://www.helpnetsecurity.com/2023/06/19/microsoft-365-azure-ddos/>.



layer DDoS attacks. In this context, DDoS attacks observed a huge increase of 28% in 2023⁵¹⁰, 80% year-on-year in Q1 2024⁵¹¹.

2023 saw a comeback of UDP-based attacks, according to Gcore, with UDP floods reaching 62% of the DDoS attacks⁵¹². TCP floods accounted for 16% and ICMP attacks for 12%. Other attacks, including SYN, SYN+ACK and RST floods, accounted for 10%. QRatorLab confirmed a similar picture with UDP-based attacks reaching 55% of the DDoS attacks in 2023.

CloudFlare presented a stable share between application and network attacks at the end of 2023, the beginning of 2024 where 37% (1.7 million) were HTTP DDoS attacks, 33% (1.5 million) were DNS DDoS attacks, 30% (1.3 million) were other L3/4 DDoS attacks⁵¹³.

8.8 BOTNETS, CLOUD AND DDOS

As discussed in ETL2023 and ETL 2022, the rapid adoption of the cloud and its movement towards edge computing increased the attack surface and the opportunity for cybercriminals⁵¹⁴. This migration has been further boosted by remote working, online education, business resilience and environmental sustainability initiated by COVID-19.

Today, the cloud is one of the main threat vectors. It is used to build botnets launching DDoS attacks, is a target of DDoS attacks itself and is also used as a defensive mechanism through various tools. According to Microsoft⁵¹⁵, attackers targeted discounted Azure subscriptions across regions to implement DDoS. Up to 40 regions (with US regions the most exploited at 70%, European ones following at 15%) have been affected by account compromises every month, to build botnets on a global scale. According to CloudFlare, cloud computing boosted the generation of botnets that launch HTTP/2 attacks generating 5,000 times more force per botnet, supporting the generation of hyper-volumetric DDoS attacks with botnets using 5-20 thousand nodes. This compares to IoT-based botnets involving millions of nodes⁵¹⁶.

IoT botnets, which were the most adopted in 2021 and 2022, are gradually being complemented by VM botnets running on the cloud or botnets built on computers and servers^{517 518}, though they maintain a remarkable role in DDoS^{519 520}. Botnets have an important role in the DDoS scenario accounting for almost half of the attacks⁵²¹.

The increasing size of DDoS attacks requires increasing power to implement defensive actions from detection to protection⁵²². In this context, the role of cloud surge as a primary defence against DDoS due to the need for the scalability and elasticity required to counteract attacks, which have a global reach, necessitates close proximity to attack sources. The cloud is the hosting infrastructure for many DDoS Protection Providers such as for instance Cloudflare, Akamai, Project Shield and AWS Shield to name but a few.

As already remarked, cloud computing can also become the target of an attack. For instance, application-layer attacks can force the cloud resources of a target to scale horizontally⁵²³. This is slightly different from traditional DDoS attacks and forces victims to employ more resources to counteract service denial. This scenario results in financial loss due to increased cloud bills and,

⁵¹⁰ <https://stormwall.network/ddos-attack-report-2023>.

⁵¹¹ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵¹² Gcore Radar: DDoS Attack Trends, Q3-Q4 2023.

⁵¹³ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵¹⁴ Accenture-2021-Cyber-Threat-Intelligence-Report fornito da ENISA.

⁵¹⁵ Microsoft Digital Defense Report 2023.

⁵¹⁶ <https://blog.cloudflare.com/ddos-threat-report-2023-q3>.

⁵¹⁷ Microsoft Digital Defense Report 2023.

⁵¹⁸ <https://www.nexusguard.com/file/nexusguard-ddos-trend-report-2024>.

⁵¹⁹ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁵²⁰ <https://vercara.com/resources/2023-ddos-statistics-and-trends>.

⁵²¹ <https://stormwall.network/ddos-attack-report-2023>.

⁵²² Microsoft Digital Defense Report 2023.

⁵²³ https://blog.qrator.net/en/2023-ddos-attacks-statistics-and-observations_186#:~:text=The%20rating%20of%20attack%20bandwidth,TCP%20flood%20%2D%20471.21%20Gbps.



indeed, denial of service could result in the exhaustion of financial resources. In Q4 2023, a massive DDoS attack targeted a European cloud provider. The attack, built on the Mirai botnet, was launched from 18 thousand unique IP addresses and reached a peak of 1.9Tbps.

8.9 DDOS ATTACKS SPREAD

Geographical Spread

The geographical spread of DDoS attacks in 2023, as analysed in *Gcore Radar: DDoS Attack Trends, Q3-Q4 2023*, indicates that the USA (24%) and Indonesia (17%), followed by The Netherlands (12%), Thailand (10%) and Colombia and Russia (8%) are at the top of the ranking as source countries of DDoS attacks⁵²⁴.

The analysis done by Microsoft indicates that the USA (54%) and Europe (14%) are at the top of the ranking as target countries of DDoS attacks, with India moving from second to fifth and the UK relegated to the ninth position⁵²⁵.

Cloudflare analysed the geographical spread of DDoS attacks, distinguishing between the application (L7) and network/transport (L3/L4) layers. The findings in Q3 2023⁵²⁶, Q4 2023⁵²⁷, and Q1 2024⁵²⁸ can be summarised as follows.

- **Application Layer (L7) – Source Country:** In Q3/Q4 2023, the USA confirmed its lead (15% plus), for the fifth consecutive quarter, followed by China, Brazil, Germany and Indonesia as the most relevant sources of DDoS attacks considering the total amount of traffic generated by application-layer DDoS attacks. In Q1 2024, the USA regained the lead (19.98%) followed by China (7.73%), Germany, Indonesia and Brazil. When comparing the DDoS traffic to the entire traffic in the country, among the biggest countries, China reached the 4th and 7th spot in Q3 and Q4 respectively in 2024, while Argentina reached the 6th spot in Q4 2024.
- **Application Layer (L7) – Target Country:** When considering the target of a DDoS attack at the application layer, the total amount of traffic, in Q3 2023, put the United States (4.867%), Singapore (3.12%), and China (2.208%) into the top spots. In Q4 2023, Singapore (4%), the USA (3.70%) and Canada (2.24%) were at the top spot considering absolute traffic values, followed by Taiwan (0.64%) with a huge increase of 847% year-on-year and 2,858% quarter-on-quarter pushed by tensions with China. Q1 2024 saw a sharp increase in the USA as a target country at 10.19%, followed by China and Canada at under 4%. When comparing the DDoS traffic to the entire traffic in the country, Singapore and Italy reached the 4th and 5th spots respectively in Q4 2023.
- **Network Layer (L3/4) – Source Country:** In Q3 2023, the USA still took the first spot as the most relevant source of DDoS attacks, substantially increasing its total attack traffic (by 36.6%). Also in Q1 2024, the USA confirmed its lead by increasing to 40.8%, followed by Germany at only 5.8%⁵²⁹. Vietnam (38.14%) was the second largest source of attack traffic in Q3 2023; Paraguay (57.4%) was the second in Q4 2023 and Q1 2024.
- **Network Layer (L3/4) – Target Country:** In Q3 2023, China reached the top of the rankings in both absolute numbers (29.22% of the total attack traffic), followed by

⁵²⁴ Gcore Radar: DDoS Attack Trends, Q3-Q4 2023.

⁵²⁵ <https://www.infosecurity-magazine.com/blogs/2022-ddos-yearinreview/>.

⁵²⁶ <https://blog.cloudflare.com/ddos-threat-report-2023-q3>.

⁵²⁷ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁵²⁸ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵²⁹ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.



the USA (3.55%), and as a percentage of all the country's traffic (73%), followed by The Netherlands (35%). In Q4 2023, China maintained the first position both in absolute numbers (45%) followed by Brazil (3.1%) and the Palestinian territories (1.1%), and as a percentage of all the country's traffic (85.8%), followed by the Palestinian territories (68.4%) and Brazil (61.1%). Q1 2024 saw a monopolisation of the first positions by China (39%) and related countries (Hong Kong 28%, Taiwan 8%). Hong Kong (78.6%) and China (75.4%) took the lead also with relative numbers.

Industrial Sector Spread

When analysing the spread of DDoS across industrial sectors, it is difficult to find a perfect match between different organisations. However, some common facts and trends emerge.

Gcore analysed the most targeted industries in H2 2023 finding gaming (42%) in the first spot, followed by the more traditional financial sector (22%) and telecom (18%)⁵³⁰. Potential attacks on the gaming and gambling sector are more frequent⁵³¹ but low in power and duration; attacks on the financial and telecom sectors are high in volume with variable length. According to Akamai, DDoS attacks on financial services accounted for 25% of all attacks (66% in EMEA)⁵³².

Considering application-layer DDoS attacks, in Q3 2023⁵³³, CloudFlare observed that the gaming domain took the lead (5.41%) as the domain with the highest application-layer attack traffic, followed by Internet technology and Internet (4.38%) and cryptocurrency (3.43%). The first three domains also remained at the three first spots in the ranking in Q4 2023⁵³⁴, with cryptocurrency taking the lead. In Q1 2024⁵³⁵, gaming (7.45%) and Internet technology and Internet (4.52%) were in the first two positions, with Marketing and Advertising (2.68%) jumping into third position. Observations of the HTTP/2 Rapid Reset Attack at CloudFlare confirmed the relevance of the gaming domain (18%) which was the target of the largest HTTP DDoS attack traffic⁵³⁶. CloudFlare infrastructure (19%) and the VoIP (10%) were the other two domains in the first three spots.

Considering L3/4 DDoS attacks^{537 538}, Information technology and Internet is by far the most impacted domain in absolute numbers (34.86% in Q3 2023 and 45% in Q4 2023) with telecommunications reaching the second position with 3.01% in Q3 and Banking, Financial Services and Insurance (BFSI) reaching the second position with 4.3% in Q4. Similar trends were confirmed in Q1 2024 with Information technology and Internet reaching 75%⁵³⁹ and the Telecommunications industry, BFSI, Gaming and Gambling industry, and Computer Software cumulatively reaching 3%. When considering the rate of attack traffic on the total traffic for the domain, though high oscillations in values can be observed, we can note that computer and network security, and information technology and internet in Q3 and Information Technology and Internet and BFSI in Q4 are among the most impacted domains. In Q1 2024, Information technology and internet was the most impacted domain with 29%, with BFSI following in 4th position with around 4.0%.

StormWall put the focus on finance, government and services, and retail as the domains most impacted by DDoS attacks with an increase of 108% in the government sector⁵⁴⁰. Similarly, Akamai analysed the financial domain, identified as the largest in terms of the number of

⁵³⁰ Gcore Radar: DDoS Attack Trends, Q3-Q4 2023.

⁵³¹ <https://www.netscout.com/threatreport/>.

⁵³² https://www.fsisac.com/hubfs/Knowledge/DDoS/FSISAC_DDoS-HereToStay.pdf.

⁵³³ <https://blog.cloudflare.com/ddos-threat-report-2023-q3>.

⁵³⁴ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁵³⁵ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵³⁶ <https://blog.cloudflare.com/ddos-threat-report-2023-q3>.

⁵³⁷ <https://blog.cloudflare.com/ddos-threat-report-2023-q3>.

⁵³⁸ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁵³⁹ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵⁴⁰ <https://stormwall.network/ddos-attack-report-2023>.



attacks, seeing the rise in geopolitical hacktivism and the availability of VM botnets (see Section 1.8) as the most impactful aspects^{541 542}. In this context, pro-Russian hacker groups (e.g. Killnet, REvil, and Anonymous Sudan) targeted European and US financial organisations causing EMEA to almost double the figures for North America.

Targeted attacks have been launched in connection with the approach of relevant events. For instance, in Q4 2023, a wave of network-layer DDoS attacks targeted retail, shipping and public relations websites during and around Black Friday and the holiday season^{543 544 545}. Another impressive growth of 61.839% year-on-year in DDoS attack traffic targeted Environmental Services, especially coinciding with the 28th United Nations Climate Change Conference (COP 28)⁵⁴⁶. The same pattern emerged in February and March 2023, around events such as the UN's resolution on climate justice and the launch of the United Nations Environment Programme's Freshwater Challenge, showing a growing relationship between environmental issues and cybersecurity. Similarly to what happened to Finland in 2023, Sweden observed a surge of 466% in DDoS attacks after it was accepted into NATO⁵⁴⁷. A 30% increase in attacks in December 2023 was observed in Perú in conjunction with a series of protests against the release of former Peruvian President Fujimori from prison on 6 December. A 50% increase was observed in Poland when the Law and Justice party lost power in government⁵⁴⁸. Finally, European Governments were hit by DDoS during election periods^{549 550}. For instance, the Dutch government was the target of two DDoS attacks on 5 and 6 June 2023.

8.10 ATTACK VECTORS

Attacks are increasingly becoming multi-vector and targeting DNS protocol^{551 552 553}. DDoS attacks at the network layer increasingly aim to disrupt the DNSs. These increased by 28% in 2023 and 80% year-on-year in Q1 2024⁵⁵⁴. This type of attack impedes DNS translations thus making the target of a request unavailable to average users even if the target is online.

According to CloudFlare⁵⁵⁵, DNS-based attacks were the most common at 47% of all attacks in Q3 2023 and 50.4% in Q4 2023, rising to 60% in 2023 according to Akamai⁵⁵⁶. SYN floods (22% in Q3, 19% in Q4) were in second place, followed by RST floods, UDP floods and Mirai attacks. The mantra *reduce, reuse and recycle* is also used to use fewer known attack vectors built on older attack vectors, usually UDP-based protocols used to launch amplification and reflection attacks. For instance, mDNS flood saw an increase of 456.4% quarter-on-quarter, CoAP flood of 387.1% and ESP flood of 302.6% in Q3, while ACK-RST Floods increased by 1,161%, CLDAP floods by 515% and SPSS floods by 243% in Q4.

In general, network attacks increased at the end of 2023 by 117% year-on-year⁵⁵⁷. The top three, according to NexusGuard, included NTP amplification attacks, HTTPS Flood and DNS amplification attacks⁵⁵⁸.

⁵⁴¹ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁵⁴² <https://www.akamai.com/lp/soti/high-stakes-of-innovation>.

⁵⁴³ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁵⁴⁴ <https://stormwall.network/ddos-report-stormwall-q4-2023>.

⁵⁴⁵ <https://azure.microsoft.com/es-es/blog/unwrapping-the-2023-holiday-season-a-deep-dive-into-azures-ddos-attack-landscape/>.

⁵⁴⁶ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁵⁴⁷ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵⁴⁸ <https://www.netscout.com/threatreport/>.

⁵⁴⁹ <https://www.bleepingcomputer.com/news/security/ddos-attacks-target-eu-political-parties-as-elections-begin/>.

⁵⁵⁰ <https://blog.cloudflare.com/exploring-the-2024-eu-election-internet-traffic-trends-and-cybersecurity-insights>.

⁵⁵¹ <https://stormwall.network/ddos-attack-report-2023>.

⁵⁵² <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁵⁵³ <https://www.netscout.com/threatreport/>.

⁵⁵⁴ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵⁵⁵ <https://blog.cloudflare.com/ddos-threat-report-2023-q3>.

⁵⁵⁶ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁵⁵⁷ <https://blog.cloudflare.com/ddos-threat-report-2023-q4>.

⁵⁵⁸ <https://www.nexusguard.com/file/nexusguard-ddos-trend-report-2024>.



Similar figures emerged in Q1 2024 with DNS-based attacks reaching 54% of all L3/4 attacks (37% in total), a total of 1.7 million attacks representing 37% of all DDoS attacks⁵⁵⁹. SYN flood, on a decreasing trend (15.3%), was in second place, followed by RST floods, UDP floods, and Mirai attacks. Regarding emerging vectors, Jenkins Flood saw an increase of 826.7%, SNMP flood of 274.4%, and ESP Flood of 169.1%.

HTTP/2 protocol implementation was misused to send hyper-volumetric DDoS attacks built on HTTP/2 Rapid Reset (2023) and HTTP/2 continuation flood (2024) vulnerabilities⁵⁶⁰. In general, CloudFlare observed that about one-third of attacks (37%, 1.7 million) had been built on HTTP crossing 2023-2024⁵⁶¹.

As discussed in Section 1.5, DDoS continues to be an attack vector itself for other attacks.

8.11 ADDITIONAL FACTS AND NUMBERS

- According to CrowdStrike⁵⁶², from June 2023 onwards, the CrowdStrike eCrime Index grew significantly, with major spikes between June and August. A sudden increase in observed DDoS attacks was among the major reasons.
- According to Microsoft⁵⁶³, DDoS attacks on the healthcare sector rose; the overall attack throughput was around 100k packets per second in 99% of the incidents with a peak of 14 million packets per second.
- According to Akamai⁵⁶⁴, 30% of the DDoS attacks were horizontal and multi-destination attacks, an increase of nearly 50%.
- According to Akamai⁵⁶⁵, the Europe, the Middle East and Africa (EMEA) region was the most targeted by DDoS.
- According to NexusGuard⁵⁶⁶, 87% of DDoS attacks targeted Windows OS devices with computers and servers becoming the primary target of DDoS (92%).
- Horizontal DDoS attacks (aka carpet-bombing attacks), which attack multiple IP destinations, grew of 52% in 2023 and accounted for almost 50% of all attacks^{567 568}.
- DDoS attacks based on Mirai, a botnet introduced almost 8 years ago, are still very common⁵⁶⁹.
- In September 2023, Akamai observed the largest ever DDoS attack targeting a US financial institution⁵⁷⁰. The attack lasted less than two minutes and was a combination of ACK, PUSH, RESET and SYN flood attack vectors, reaching 633.7 gigabits per second (Gbps) and 55.1 million packets per second (Mbps).

⁵⁵⁹ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵⁶⁰ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵⁶¹ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵⁶² CrowdStrike 2024 Global Threat Report.

⁵⁶³ Microsoft Digital Defense Report 2023.

⁵⁶⁴ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁵⁶⁵ <https://www.akamai.com/newsroom/press-release/akamai-report-finds-ddos-attacks-against-financial-services-gambling-and-manufacturing-sectors-in-emea-exceeded-the-numbers-in-all-other-regions-combined>.

⁵⁶⁶ <https://www.nexusguard.com/press/87-of-ddos-attacks-targeted-windows-os-devices-in-2023>.

⁵⁶⁷ <https://vercara.com/resources/2023-ddos-statistics-and-trends>.

⁵⁶⁸ <https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023>.

⁵⁶⁹ <https://blog.cloudflare.com/ddos-threat-report-for-2024-q1>.

⁵⁷⁰ <https://www.akamai.com/blog/security/akamai-prevents-the-largest-ddos-attack-on-a-us-financial-company>.





9. INFORMATION MANIPULATION AND INTERFERENCE

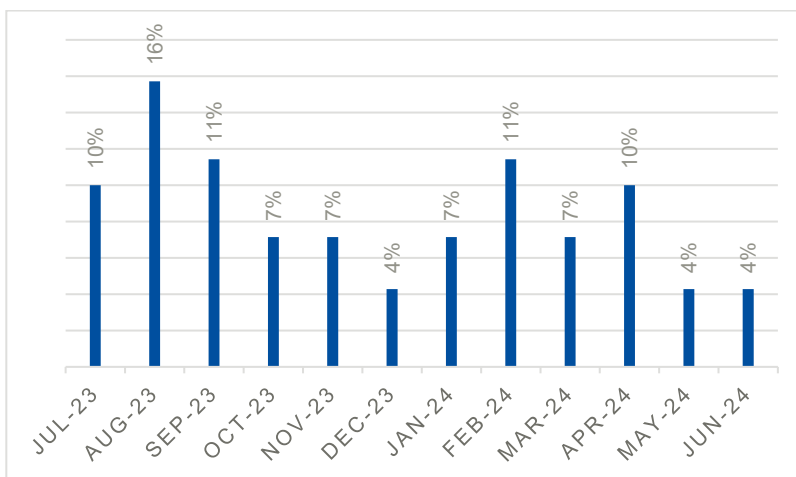
Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Those who carry out such activities can be state or non-state actors, including their proxies inside and outside their own territory⁵⁷¹. The current chapter focuses on **information manipulation and interference** regardless of its origin.

As in the 2023 ENISA Threat Landscape (ETL 2023), in this edition we continue to use the term ‘information manipulation’, as opposed to ‘disinformation/misinformation’; this reflects a broader set of potential threats and, more importantly, it puts emphasis on manipulative behaviour, instead of the truthfulness of the content being delivered.

We argue that information manipulation and relevant operations should be considered a cybersecurity threat, since such operations directly affect at least one of the three components of the information security model and in particular that of integrity of information, as well as other cybersecurity principles (such as authenticity and accountability) and leverage on other types of cybersecurity tactics, techniques and procedures⁵⁷².

The figure below shows the timeline of information manipulation events that we have observed throughout the period of reference. The following sections give an overview of identified trends.

Figure 39: Distribution of information manipulation incidents during the period of reference



⁵⁷¹ https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

⁵⁷² In the MITRE ATT&CK Framework, the definition of the cybersecurity tactic of data manipulation is ‘Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data’. The notion of information manipulation is thus directly related to the aforementioned cybersecurity adversary tactic. For a more elaborated explanation on the relationship between information manipulation and cybersecurity, please refer to the ENISA Threat Landscape 2023.



Methodological note for this chapter:

Data: Most of the events analysed have been shared by the European External Action Service (EEAS) Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI) Division. The division focuses on Foreign Information Manipulation and Interference (FIMI) and on activities traceable to specific foreign actors or regions. The incidents of this report have been selected with keywords related to cybersecurity (e.g. phishing, defacement). The majority refers to activities suspected to be linked to Russian actors to different degrees. Data on cyber-related FIMI activities by other actors are not systemically collected. Whereas attribution remains challenging, the narratives and the motivations exhibited by adversaries point to likely foreign threat actors. This is by no means a formal attribution, just a likely provenance. This focus might be due to data collection (focusing on strategic issues), and/or to the geopolitical context, possibly leading to a surge in information manipulation activities and/or in Tactics Techniques and Procedures (TTPs) combining cybersecurity and the manipulation of information. In some cases, observation on other actors from other sources have been inserted, in particular if said actors interacted with the observed infosphere and/or adopted similar behaviours. A brief, more general, analysis from the perspective of Artificial Intelligence has also been included.

Important: This does not necessarily imply that a given incident or source of information is linked to the Russian government or editorially in favour of the Russian government, nor that it has intentionally sought to disinform.

Analysis: This chapter analyses incidents both with the DISARM (DISinformation Analysis & Risk Management) Red framework⁵⁷³, describing behaviours for manipulating information, and MITRE ATT&CK Framework. This combined approach was proposed for the first time in the 2022 ENISA-EEAS joint report⁵⁷⁴ and used for the first time in the ETL for the 2023 edition. It should be noted that the application of these frameworks, and especially of DISARM, has been further fine-tuned in this year's edition. For example, the DISARM framework has also been used more extensively to describe the infrastructure underlying the events observed (see in particular section 9.2.4). Also, the quality of the data has improved, for example with more information about related events. For this reason, the comparison with the data of the ETL 2023 should be interpreted as indicating trends, rather than exact increases or decreases in the percentages of tactics or techniques.

⁵⁷³ <https://www.disarm.foundation/framework>. The report uses a version of the DISARM framework prior to the latest update, which took place at the beginning of August, after the analysis was already concluded (<https://medium.com/disarming-disinformation/disarm-v1-5-personas-update-bf0323614e3b>).

⁵⁷⁴ <https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape>.



9.1 TRENDS

By analysing incidents of information manipulation, we have identified several trends:

- Information manipulation continues to be a key element of Russia’s war of aggression against Ukraine, although an effort to further localise content and, at the same time, to globalise its presence is observed.
- Manipulating information in response of specific news seems to have increased, probably because 2024 has been marked by many major events, elections in particular. Elections have also been the target of self-proclaimed hacktivists, whose presence was also reported in the ETL 2023.
- Information manipulation continues to be supported by a widespread digital presence, showing many cases of inauthentic accounts and websites.
- AI-enabled information manipulation has been observed, but still on a limited scale.

9.2 OVERVIEW OF TACTICS

In terms of information manipulation, the most recurrent tactic is content development, followed by the establishment of assets and microtargeting⁵⁷⁵.

Table 1: Definitions of the top-3 DISARM tactics (in order of recurrence)⁵⁷⁶

DISARM Tactic	Definition
TA06 - Develop Content	Create or acquire text, images and other content
TA15- Establish Social Assets	Establishing information assets generates messaging tools, including social media accounts, operational personnel and organisations, including directly and indirectly managed assets
TA14 – Microtarget	Target very specific populations of people

The figure below shows the distribution of the most recurrent tactics according to the DISARM framework. The analysis has been carried out by associating several tactics to each incident. With respect to the ETL 2023, there is an increase in the establishment of social assets and microtargeting⁵⁷⁷.

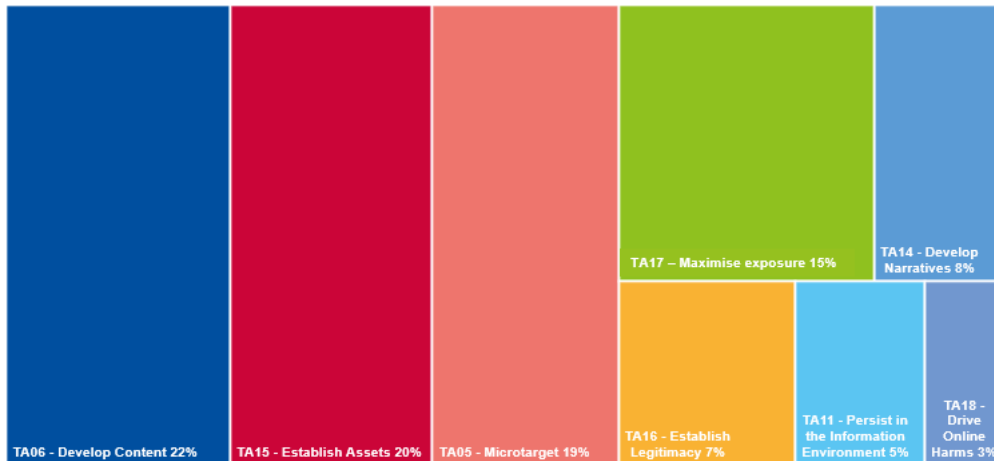
Figure 40: Distribution of information manipulation tactics according to the DISARM framework

⁵⁷⁵ In this instance the increase has it has been estimated that the increase is partially due to the changes in methodology highlighted in the introduction.

⁵⁷⁶ For the full definitions, refer to <https://www.disarm.foundation/framework>.

⁵⁷⁷ In this instance it has been estimated that the increase is partially due to the changes in methodology highlighted in the introduction.





According to the MITRE ATT&CK framework, that is from a cybersecurity perspective, information manipulation has been supported mainly by tactics for the development of resources, which amount to more of than half of the tactics used, followed by tactics related to the evasion of defences and impact.

Table 2: Definitions of the top-3 MITRE ATT&CK tactics (in order of occurrence)⁵⁷⁸

MITRE ATT&CK Tactic	Definition
Resource Development	Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising or stealing resources that can be used to support targeting.
Defence evasion	The adversary is trying to avoid being detected.
Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Figure 41: Distribution of information manipulation tactics according to the MITRE ATT&CK framework

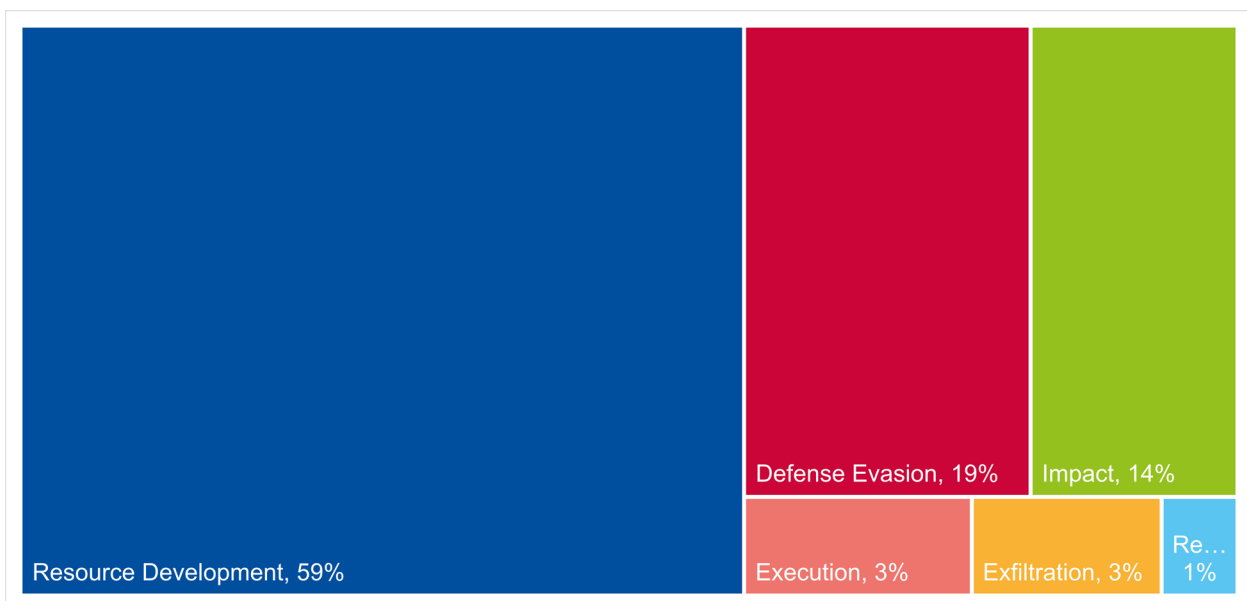


Figure 41 shows the distribution of the most recurrent tactics. The analysis has been carried out by associating several tactics to each incident. With respect to the ETL 2023, the top tactics

⁵⁷⁸ For the full definitions, refer to: <https://attack.mitre.org/>.



have not changed, only their proportion: resource development represented 59% of tactics (52% in the ETL 2023), defence evasion 19% (12% in the ETL 2023) and impact 14% (27% in the ETL 2023). This seems to indicate that malicious actors focus on the establishment of inauthentic accounts (resource development) and the concealment of infrastructure or assets (defence evasion). The decrease in impact tactics (associated with data manipulation) might be explained by the focus on impersonating legitimate entities and creating content from scratch, as opposed to the reframing of existing legitimate content.

In the following sections the most recurrent tactics, for both the DISARM and MITRE ATT&CK frameworks, are broken down into techniques and contextualised into specific trends. Additional trends emerging from the data analysis are also discussed.

9.3 SEIZING THE OPPORTUNITY OF LEVERAGING ON MAJOR EVENTS

The period of reference of this report has been marked by major events that have been promptly exploited for FIMI purposes. In approximately 40% of the events analysed, the DISARM technique of responding to breaking news events marked a significant increase with respect to the ETL 2023, where this technique was used in 27% of events. Breaking news events are events where media attention on a story is heightened. It is noticeable that the timeline of events (Figure 39) does not reflect this trend. Possible explanations are that the information has been manipulated in reaction to more events than in the past either because the capacity of threat actors to react quickly and more specifically has improved and/or because there have been more note-worthy events over the period of observation. We have identified several thematic clusters of such events, in particular revolving around the geopolitical situation and elections.

Geopolitical situation

Russia's war of aggression against Ukraine remains a catalyst for the FIMI activities observed. As explained in the ETL 2023, while this could be due to a bias induced by the data collection⁵⁷⁹, information manipulation has been an essential and well-established component of Russian security strategies^{580 581}. Throughout the period of reference, a shift in the narrative was observed. While in the first year of the war influence operations would be generally intertwined with Russia's political and military efforts, the focus seems to have moved more distinctly to Ukraine's allies, sowing distrust between Ukrainian populations and European partners and undermining the support of European citizens for Western military assistance to Ukraine⁵⁸². Besides the war, it seems that pro-Kremlin actors are leveraging on the geopolitical situations beyond EU's borders and affecting Ukraine's allies.

Elections

2024 has been widely labelled as the 'election year' as more than 80 countries, representing more than half of the world's population, are voting⁵⁸³. The manipulation of information can affect the electoral processes in various way, such as setting the agenda on certain key topics, encouraging abstention or undermining political adversaries⁵⁸⁴. Cybersecurity attacks can also facilitate the creation and spread of manipulated information among the electorate, for example by exfiltrating (or claiming to have exfiltrated) data in order to harm the reputation of an electoral candidate, as well as by carrying out (or claiming to have carried out) attacks affecting the electoral infrastructure to undermine the public's trust on the integrity of the electoral process⁵⁸⁵. This indeed happened in the period of reference on several occasions. The European Parliament elections, held between 6 and 9 June, have been looked at with particular concern

⁵⁷⁹ See the methodological note in the box at the beginning of the chapter.

⁵⁸⁰ No Water's Edge: Russia's Information War and Regime Security (2023, Carnegie Endowment for International Peace).

⁵⁸¹ <https://raport.valisluureamet.ee/2023/en/russian-armed-forces/1-3-russia-continues-to-look-for-a-weak-link-in-ukrainian-cyberspace/>.

⁵⁸² A Year of Russian Hybrid Warfare in Ukraine (2023, Microsoft) - https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf; Microsoft Digital Defense Report (2023): <https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023>.

⁵⁸³ <https://www.theguardian.com/world/2024/feb/23/2024-global-elections-tracker-voting-dates-us-india-indonesia-belarus-haiti-pakistan-full-list> (Accessed 30/07/2024).

⁵⁸⁴ EEAS, https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

⁵⁸⁵ <https://digital-strategy.ec.europa.eu/en/news/new-cybersecurity-compendium-how-protect-integrity-elections-published>.



given the complexity of the exercise, encompassing, in practice, the organisation of elections in each of the 27 Member States over a very short time-frame⁵⁸⁶. While no major disruption in terms of information manipulation was registered⁵⁸⁷, some threat actors, including NoName057, have claimed cyber-attacks (DDoS) targeting the internet infrastructure in the EU during the electoral period⁵⁸⁸. This suggests that the trend identified in the ETL 2023, linking self-proclaimed hacktivists with pollution of the information environment, has not disappeared. As to national elections, the EEAS reports that a few days before the Polish 2023 parliamentary elections photos and videos targeting a candidate, seemingly obtained through a previous Ghostwriter hacking operation⁵⁸⁹, were published online by a website previously blocked for releasing leaked emails from Polish politicians, and which was attributed by independent researchers and Polish services to the Russian and Belarusian security services⁵⁹⁰.

Paris 2024 Olympics

Although the Olympics are outside the period of reference of this report, they have already been a recurrent theme in information manipulation campaigns since 2023⁵⁹¹. Microsoft reports the detection of several information manipulation operations especially since, in 2023, the International Olympic Committee's (IOC) decided that Russian citizens would be allowed to compete in Paris but only as neutral athletes. The objectives of these operations are two-fold: on one hand to denigrate the reputation of the IOC and, on the other, to create the expectation of violence breaking out in Paris during the games⁵⁹². VIGINUM, the French governmental agency tasked with the protection against and monitoring of foreign digital interferences, has pointed out similar narratives used in the operation 'Matryoshka', whereby fake content impersonating legitimate entities (e.g. media outlets) is shared in a coordinated manner on social media⁵⁹³.

9.4 LOCALISED TARGETING AND ON A GLOBAL SCALE

As explained above, microtargeting is the third most recurrent DISARM tactic, with an increase over the ETL 2023. The most recurrent microtargeting technique is the creation of localised content, followed by the purchasing of targeted advertisements (the latter is treated in the next section).

The creation of content appealing to a specific community of individuals can have different forms, such as the development of narratives with a local spin (for example in reaction to events with local relevance, as explained in the previous section), as well as the use of local languages. It has been observed that threat actors seem to have adapted the manipulation of information to specific situations more and more, thus widening their potential for a global outreach.

Since Russia's full-scale invasion of Ukraine, pro-Russian information manipulation has consistently been conducted in several languages⁵⁹⁴ to maximise its exposure. Between September and December 2023, for example, a network of almost 200 'information portals' with similar characteristics and targeting western countries in their local languages has been detected. Moreover, the network appeared to use search engine optimisation to be prompted by more precise and occasional queries referring to current events⁵⁹⁵.

⁵⁸⁶ <https://www.europarl.europa.eu/news/en/press-room/20230524IPR91908/foreign-interference-meps-call-for-urgent-protection-of-2024-european-elections>.

⁵⁸⁷ <https://edmo.eu/blog/eu-elections-2024-the-battle-against-disinformation-was-won-but-the-attribution-war-is-far-from-over/>.

⁵⁸⁸ <https://www.radware.com/blog/security/2024/06/uncovering-the-hackivist-cyberattacks-targeting-the-eu-election/>.

⁵⁸⁹ <https://vsquare.org/behind-the-hack-and-leak-scandal-in-poland/>.

⁵⁹⁰ EEAS, https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

⁵⁹¹ https://www.lemonde.fr/en/france/article/2024/03/01/bedbug-panic-was-stoked-by-russia-says-france_6575870_7.html (Accessed 30/07/2024).

⁵⁹² <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/how-russia-is-trying-to-disrupt-the-2024-paris-olympic-games> (Accessed 30/07/2024).

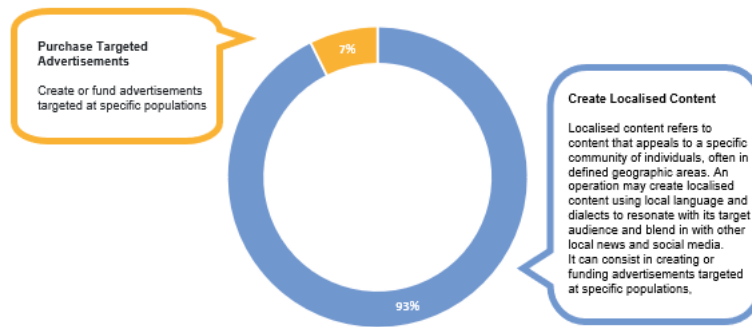
⁵⁹³ VIGINUM (2024) – https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf.

⁵⁹⁴ <https://www.nature.com/articles/s41598-024-60653-y> (Accessed 31/07/2024).

⁵⁹⁵ VIGINUM (2024), https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf.



Figure 42: Distribution of information manipulation techniques within the DISARM tactic ‘Microtarget’



These efforts also seem to have gradually expanded globally, and to be relying more on social media, probably because the shift in narrative is targeting Ukraine’s supporters (rather than Ukrainians themselves), as well as Western sanctions disrupting the communications of state-sponsored media, in particular RT and Sputnik. RT and Sputnik are still influential in parts of Latin America, Middle East and Africa, where Russia also uses using its diplomatic network for the amplification of its narratives⁵⁹⁶ and local information outlets have been established as well⁵⁹⁷.

China is also expanding its FIMI activities, with operations being tracked all over the world, employing, among others, bots, trolls and coordinated campaigns with inauthentic social media accounts⁵⁹⁸. According to Microsoft, Chinese-affiliated covert propaganda operates *at a scale unmatched by other malign influence actors* deploying *thousands of accounts across dozens of websites spreading memes, videos, and articles in multiple languages*⁵⁹⁹. China is also experimenting with Artificial Intelligence, with deepfake news anchors⁶⁰⁰ and large language models (LLMs) to generate texts in languages such as Japanese and Korean that are posted across social media platforms⁶⁰¹.

9.5 INAUTHENTIC CHANNELS AND BEHAVIOUR NURTURING EXPOSURE AND CONFUSION

The ETL 2023 pointed to a very widespread digital presence to maximise the exposure of adversarial operations. This trend has continued and likely strengthened over the last year.

Resource development, that is the creation or acquisition of resources that are used by adversaries to support targeting, is the most recurrent MITRE ATT&CK tactic. Coherently, the second most recurrent DISARM tactic, after the development of content, is the establishment of social assets, intended as information assets. The DISARM framework allows a closer look on the type of resources or assets that have been developed or established. The break-down of

⁵⁹⁶ Digital Forensic Research Lab (2024), <https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/> (Accessed 31/07/2024).

⁵⁹⁷ The U.S. Government’s dedicated center for countering foreign disinformation and propaganda, the Global Engagement Center (GEC) reports of activities, among others, in France, the UK, Honduras, Israel, Pakistan, East Africa and globally (through ByteDance). https://www.state.gov/wp-content/uploads/2023/10/HOW-THE-PEOPLES-REPUBLIC-OF-CHINA-SEEKS-TO-RESHAPE-THE-GLOBAL-INFORMATION-ENVIRONMENT_508.pdf

⁵⁹⁸ https://www.state.gov/wp-content/uploads/2023/10/HOW-THE-PEOPLES-REPUBLIC-OF-CHINA-SEEKS-TO-RESHAPE-THE-GLOBAL-INFORMATION-ENVIRONMENT_508.pdf

⁵⁹⁹ Microsoft Digital Defense Report (2023): <https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023>.

⁶⁰⁰ <https://www.theguardian.com/technology/article/2024/may/18/how-china-is-using-ai-news-anchors-to-deliver-its-propaganda#:~:text=China%20is%20at%20the%20forefront,fictitious%20broadcaster%20called%20Wolf%20News.> (Accessed 31/07/2024).

⁶⁰¹ <https://openai.com/index/disrupting-deceptive-uses-of-ai-by-covert-influence-operations/> (Accessed 31/07/2024).



the DISARM techniques within the DISARM tactic 'Establish social assets', shows that assets included mostly inauthentic accounts, sometimes grouped in networks of fake profiles, and websites.

Figure 43: Distribution of information manipulation techniques within the DISARM tactic 'Establish social assets'



Inauthenticity supports information manipulation both by giving threat actors the possibility to impersonate legitimate entities and rendering the detection of FIMI activities more difficult.

Impersonation of legitimate entities was a common trend in the events analysed, commonly implemented through typo-squatting websites to mimic legitimate media outlets or entities (e.g. by slightly altering the URL of a known news website) or by forging content that appears as originating from specific organisations (e.g. by using the logo of a known news outlet on a forged video). Threat actors continue to adopt work-arounds to reach European audiences. As seen in section 1.2, the MITRE ATT&CK tactic 'Defence evasion' is the second most recurrent MITRE tactic (19% of tactics, increasing from the ETL 2023's 12%) and, within that tactic, masquerading is the most common technique. Masquerading is defined by MITRE ATT&CK as *the manipulation of an artifact's feature to make it appear legitimate, (and) is used as the main technique to evade defences and avoid being detected*⁶⁰². The sustained introduction of sanctions targeting FIMI activities by the EU in the last two years⁶⁰³ and possibly the entry into application at the beginning of 2024 of the Digital Services Act⁶⁰⁴ might contribute to explaining this increase. It is noteworthy that some of the observed typo-squatting cases seem to belong to the infrastructure revealed by VIGINUM already in 2023 as serving the so-called DoppelGänger or Recent Reliable News (RRN) campaign. As reported in the ETL 2023, in 2022 and 2023 VIGINUM had observed the registration of 355 domain names impersonating the identity of media outlets in France and in nine states in Europe, the Americas and the Middle East. This

⁶⁰² In continuation with 2023, this definition is stretched to also include attempts to conceal identity and undermine accountability.

⁶⁰³ Some examples: since 2022 several state-owned media have been prohibited from broadcasting in the EU, in 2024 the prohibition on accepting financing from the Russian state and its proxies by political parties, NGOs and media service providers in the EU has been introduced. More information about EU sanctions: https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en.

⁶⁰⁴ The Digital Services Act is mandating, among others, very large online platforms (VLOPs) or very large online search engines (VLOSEs) to identify and mitigate systemic risk (e.g. related to illegal content, public security and electoral processes) linked to their services. Regulation (EU) 2022/2065 on a Single Market For Digital Services - <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.



campaign was assessed in April 2024 as still on-going and its infrastructure as still active⁶⁰⁵. Another observed way to avoid detection when exploiting inauthenticity is through a combination of targeted advertising and URL redirection. The EEAS has observed that malicious actors, in order to circumvent the efforts of platforms to limit access to sanctioned websites, use targeted advertising on platforms to disseminate the URLs of webpages, whose source code has been manipulated so it redirects visitors to blocked domains automatically⁶⁰⁶.

The cases observed show that there is coordination among inauthentic accounts and websites, with cross-posting and flooding the information space being the most used technique to maximise the exposure of manipulated information. Interactions among accounts and websites create the illusion of an authentic discussion and, the same time, obfuscate the origins of FIMI content⁶⁰⁷. For example, the Matryoshka campaign mentioned above uses artificial or the automated dissemination of content, involving a first group of accounts posting fake content on a platform and a second one spreading it by 'quoting' it in response to posts by media outlets, public figures and fact-checkers.

9.6 AI IMPACT ON INFORMATION MANIPULATION REMAINS LIMITED (FOR NOW)

In the last three editions of the ETL, AI-enabled information manipulation has been looked at with concern. In particular, the ETL 2023, drafted in the wake of the release of multiple publicly available and widely used AI chatbots, summarised the potential impact of AI on the 'ABC' of information manipulation campaigns⁶⁰⁸, namely the actors waging the campaigns, their behaviours and the content. It has been observed that AI has impacted these dimensions on a non-negligible, probably evolving, but still relatively limited, scale:

- **Actors:** As noted in section 2.2.9 some threat actors are experimenting with AI for information manipulation. The effectiveness of AI-supported campaigns has been disputed, however, and it seems that this is rather an exploration phase to assess how AI can be exploited in this context, and evolution is expected⁶⁰⁹.
- **Behaviour:** The extent to which AI is used to disseminate content is not fully clear, although it is happening. For example, NewsGuard has identified over 1,000 AI-generated news and information sites operating with little to no human oversight⁶¹⁰. OpenAI has also reported on malicious actors using their models to debug code, seek advice on social media analysis, and fake engagement⁶¹¹.
- **Content:** Unsurprisingly, it seems that AI has been used more extensively for content generation. In the cases analysed, AI-generated text, audio, images and videos have all been observed. The DFR Lab has collected a list of AI-generated content since the Russia's invasion of Ukraine, also including, in November 2023 deep-fake videos of the then-Ukrainian Commander-in-chief⁶¹².

All the above, seems to mark a progression in the use of AI for FIMI activities, but the full range of predicted consequences has not yet materialised.

⁶⁰⁵ <https://blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign/> (Accessed 31/07/2024).

⁶⁰⁶ <https://euvsdisinfo.eu/something-dark-hiding-behind-the-ads/>.

⁶⁰⁷ EEAS, https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

⁶⁰⁸ Transatlantic Working Group (2019) - , https://www.ivir.nl/publicaties/download/ABC_Framework_2019_Sept_2019.pdf ;

OpenAI (2023) <https://cdn.openai.com/papers/forecasting-misuse.pdf>

⁶⁰⁹ <https://www.wired.com/story/openai-threat-report-china-russia-ai-propaganda/>.

⁶¹⁰ <https://www.newsguardtech.com/special-reports/ai-tracking-center/>.


⁶¹¹ OpenAI (2024) – AI and Covert Operations. Also <https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/>.

⁶¹² <https://dfriab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine/> (Accessed on 31/07/2024).





A ANNEX: MAPPING TO MITRE ATT&CK FRAMEWORK

RANSOMWARE 		
<p>The current table highlights the techniques in the MITRE ATT&CK® Framework associated with ransomware software, ransomware groups or both, according to Ransomware techniques in ATT&CK⁶¹³. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques, starting from initial access.</p>		
Tactic	Technique	Mitigation
TA0001 : Initial Access	T1190 : Exploit Public-Facing Application T1133 : External Remote Services T1566 : Phishing T1199 : Trusted Relationship	M1048 : Application Isolation and Sandboxing M1050 : Exploit Protection M1030 : Network Segmentation M1026 : Privileged Account Management M1051 : Update Software M1016 : Vulnerability Scanning M1042 : Disable or Remove Feature or Program M1035 : Limit Access to Resource Over Network M1032 : Multi-factor Authentication M1049 : Antivirus/Antimalware M1031 : Network Intrusion Prevention M1021 : Restrict Web-Based Content M1054 : Software Configuration M1017 : User Training M1018 : User Account Management
TA0002 : Execution	T1106 : Native API T1047 : Windows Management Instrumentation	M1040 : Behaviour Prevention on Endpoint M1038 : Execution Prevention M1026 : Privileged Account Management M1018 : User Account Management
TA0003 : Persistence	T1197 : BITS Jobs T1554 : Compromise Client Software Binary T1136 : Create Account T1133 : External Remote Services	M1037 : Filter Network Traffic M1028 : Operating System Configuration M1018 : User Account Management M1045 : Code Signing M1030 : Network Segmentation M1032 : Multi-factor Authentication M1026 : Privileged Account Management M1042 : Disable or Remove Feature or Program M1035 : Limit Access to Resource Over Network
TA0004 : Privilege Escalation	T1134 : Access Token Manipulation T1068 : Exploitation for Privilege Escalation T1055 : Process Injection	M1018 : User Account Management M1026 : Privileged Account Management M1048 : Application Isolation and Sandboxing

⁶¹³ Ransomware techniques in ATT&CK, <https://healthcyber.mitre.org/blog/resources/attack-navigator/>



		M1050 : Exploit Protection M1051 : Update Software M1038 : Execution Prevention M1019 : Threat Intelligence Program M1040 : Behaviour Prevention on Endpoint
TA0005 : Defence Evasion	T1134 : Access Token Manipulation T1197 : BITS Jobs T1140 : Deobfuscate/Decode Files or Information T1480 : Execution Guardrails T1036 : Masquerading T1112 : Modify Registry T1027 : Obfuscated Files or Information T1055 : Process Injection T1620 : Reflective Code Loading T1497 : Virtualisation/Sandbox Evasion	M1018 : User Account Management M1026 : Privileged Account Management M1037 : Filter Network Traffic M1028 : Operating System Configuration M1055 : Do Not Mitigate M1049 : Antivirus/Antimalware M1040 : Behaviour Prevention on Endpoint M1045 : Code Signing M1038 : Execution Prevention M1022 : Restrict File and Directory Permissions M1024 : Restrict Registry Permissions M1047 : Audit
TA0006 : Credential Access	T1555 : Credentials from Password Stores T1539 : Steal Web Session Cookie	M1027 : Password Policies M1032 : Multi-factor Authentication M1054 : Software Configuration M1017 : User Training
TA0007 : Discovery	T1087 : Account Discovery T1217 : Browser Bookmark Discovery T1135 : Network Share Discovery T1069 : Permission Groups Discovery T1057 : Process Discovery T1012 : Query Registry T1518 : Software Discovery T1614 : System Location Discovery T1033 : System Owner/User Discovery T1124 : System Time Discovery T1497 : Virtualisation/Sandbox Evasion	M1028 : Operating System Configuration
TA0008 : Lateral Movement	T1210 : Exploitation of Remote Services T1080 : Taint Shared Content	M1050 : Exploit Protection M1030 : Network Segmentation M1026 : Privileged Account Management M1016 : Vulnerability Scanning M1042 : Disable or Remove Feature or Program M1048 : Application Isolation and Sandboxing M1051 : Update Software M1019 : Threat Intelligence Program M1038 : Execution Prevention M1022 : Restrict File and Directory Permissions
TA0009 : Collection	T1560 : Archive Collected Data T1530 : Data from Cloud Storage Object T1213 : Data from Information Repositories T1039 : Data from Network Shared Drive T1113 : Screen Capture	M1047 : Audit M1018 : User Account Management M1037 : Filter Network Traffic M1022 : Restrict File and Directory Permissions M1032 : Multi-factor Authentication M1041 : Encrypt Sensitive Information M1017 : User Training



TA0011 : Command and Control	T1568 : Dynamic Resolution T1095 : Non-Application Layer Protocol T1071 : Non-Standard Port T1072 : Protocol Tunnelling T1090 : Proxy T1102 : Web Service	M1031 : Network Intrusion Prevention M1021 : Restrict Web-Based Content M1030 : Network Segmentation M1037 : Filter Network Traffic M1015 : Active Directory Configuration M1032 : Multi-factor Authentication M1027 : Password Policies M1026 : Privileged Account Management M1029 : Remote Data Storage M1051 : Update Software M1018 : User Account Management M1017 : User Training M1020 : SSL/TLS Inspection
TA0010 : Exfiltration	T1041 : Exfiltration Over C2 Channel	M1031 : Network Intrusion Prevention M1057 : Data Loss Prevention
TA0040 : Impact	T1485 : Data Destruction T1499 : Endpoint Denial of Service T1489 : Service Stop	M1053 : Data Backup M1037 : Filter Network Traffic M1030 : Network Segmentation M1022 : Restrict File and Directory Permissions M1024 : Restrict Registry Permissions M1018 : User Account Management

MALWARE (PEGASUS FOR ANDROID)



The current table highlights the techniques in the MITRE ATT&CK® Framework (Mobile) associated with the Pegasus spyware. The Pegasus⁶¹⁴ for Android is the Android version of malware that has reportedly been linked to the NSO Group (Update August 2022).

Tactic	Technique	Mitigation
TA0035 : Collection	T1429 : Audio Capture	M1006 : Use Recent OS Version M1011 : User Guidance
TA0028 : Persistence	T1645 : Compromise Client Software Binary	M1002 : Attestation M1003 : Lock Bootloader M1001 : Security Updates M1004 : System Partition Integrity
TA0028 : Persistence	T1624.001 : Event Triggered Execution: Broadcast Receivers	M1006 : Use Recent OS Version
TA0029 : Privilege Escalation	T1404 : Exploitation for Privilege Escalation	M1002 : Attestation M1010 : Deploy Compromised Device Detection Method M1001 : Security Updates
TA0037 : Command and Control	T1644 : Out of Band Data	M1011 : User Guidance
TA0035 : Collection	T1636.001 : Protected User Data: Calendar Entries	M1011 : User Guidance

⁶¹⁴ <https://attack.mitre.org/techniques/T1587/001/>



TA0035 : Collection	T1636.002 : Protected User Data: Call Log	M1011 : User Guidance
TA0035 : Collection	T1636.003 : Protected User Data: Contact List	M1011 : User Guidance
TA0032 : Discovery	T1418 : Software Discovery	M1006 : Use Recent OS Version M1011 : User Guidance
TA0035 : Collection	T1409 : Stored Application Data	M1006 : Use Recent OS Version
TA0032 : Discovery	T1422 : System Network Configuration Discovery	M1006 : Use Recent OS Version
TA0035 : Collection	T1512 : Video Capture	M1006 : Use Recent OS Version

SOCIAL ENGINEERING



The current table highlights the techniques in the MITRE ATT&CK® Framework associated with social engineering. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques relevant to social engineering. We do not include the techniques commonly used for follow-up activity (including for example the methods showing how malicious documents can be executed).

Tactic	Technique	Mitigation
TA0043 : Reconnaissance	T1595 : Active Scanning T1592 : Gather Victim Host Information T1589 : Gather Victim Identity Information T1590 : Gather Victim Network Information T1591 : Gather Victim Org Information T1598 : Phishing for Information T1597 : Search Closed Sources T1596 : Search Open Technical Databases T1593 : Search Open Websites/Domains T1594 : Search Victim-Owned Websites	M1056 : Pre-compromise M1054 : Software Configuration M1017 : User Training M1013 : Application Developer Guidance M1047 : Audit
TA0042 : Resource Development	T1583 : Acquire Infrastructure T1586 : Compromise Accounts T1584 : Compromise Infrastructure T1587 : Develop Capabilities T1585 : Establish Accounts T1588 : Obtain Capabilities T1608 : Stage Capabilities	M1056 : Pre-compromise
TA0001 : Initial Access	T1133 : External Remote Services T1566 : Phishing T1199 : Trusted Relationship T1078 : Valid Accounts	M1035 : Limit Access to Resource Over Network M1032 : Multi-factor Authentication M1030 : Network Segmentation M1042 : Disable or Remove Feature or Program M1031 : Network Intrusion Prevention M1021 : Restrict Web-Based Content M1054 : Software Configuration M1049 : Antivirus/Antimalware M1017 : User Training M1018 : User Account Management M1036 : Account Use Policies



		M1015 : Active Directory Configuration M1013 : Application Developer Guidance M1027 : Password Policies M1026 : Privileged Account Management
TA0002 : Execution	T1204 : User Execution	M1040 : Behaviour Prevention on Endpoint M1038 : Execution Prevention M1031 : Network Intrusion Prevention M1021 : Restrict Web-Based Content M1017 : User Training

THREATS AGAINST DATA



The anatomy of data exfiltration is depicted in the following table, which includes the techniques that may be used in each kill chain phase and lead to data exfiltration or data breach or identity theft. The construction of the table is based on the MITRE ATT&CK⁶¹⁵ knowledge base. MITRE ATT&CK[®] provides information regarding the behaviour of cyber adversaries and a taxonomy of adversarial actions. The techniques leading to data exfiltration were selected using the MITRE ATT&CK[®] part for Enterprise, which covers behaviours against enterprise IT networks and the cloud.

DATA EXFILTRATION

Tactic	Technique	Mitigation
TA0003 : Persistence	T1197 : BITS Jobs	M1018 : User Account Management M1028 : Operating System Configuration M1037 : Filter Network Traffic
TA0005 : Defence Evasion	T1197 : BITS Jobs T1599 : Network Boundary Bridging	M1018 : User Account Management M1028 : Operating System Configuration M1037 : Filter Network Traffic M1026 : Privileged Account Management M1032 : Multi-factor Authentication M1027 : Password Policies M1037 : Filter Network Traffic M1043 : Credential Access Protection
TA0009 : Collection	T1560 : Archive Collected Data T1005 : Data from Local System T1039 : Data from Network Shared Drive T1025 : Data from Removable Media T1074 : Data Staged	M1047 : Audit M1057 : Data Loss Prevention
TA0010 : Exfiltration	T1020 : Automated Exfiltration T1048 : Exfiltration Over Alternative Protocol T1041 : Exfiltration Over C2 Channel T1011 : Exfiltration Over Other Network Medium T1052 : Exfiltration Over Physical Medium T1567 : Exfiltration Over Web Service T1029 : Scheduled Transfer T1537 : Transfer Data to Cloud Account	M1030 : Network Segmentation M1018 : User Account Management M1031 : Network Intrusion Prevention M1037 : Filter Network Traffic M1057 : Data Loss Prevention M1022 : Restrict File and Directory Permissions M1028 : Operating System Configuration M1042 : Disable or Remove Feature or Program M1034 : Limit Hardware Installation M1021 : Restrict Web-Based Content M1027 : Password Policies

⁶¹⁵ MITRE ATT&CK[®], <https://attack.mitre.org/>



THREATS AGAINST AVAILABILITY (DDOS)		
<p>The anatomy of Denial of Services attacks and web attacks are depicted in the following figures, which includes the techniques that may be used in each kill chain phase. The table is constructed based on the MITRE ATT&CK⁶¹⁶ knowledge base. MITRE ATT&CK[®] provides information regarding the behaviour of cyber adversaries and a taxonomy of adversarial actions. The techniques are selected using the MITRE ATT&CK[®] part for Enterprise, which covers behaviours against enterprise IT networks and the cloud.</p>		
Tactic	Technique	Mitigation
TA0042 : Resource Development	T1583 : Acquire Infrastructure T1584 : Compromise Infrastructure	M1056 : Pre-compromise
TA0005 : Defence Evasion	T1553 : Subvert Trust Controls	M1038 : Execution Prevention M1028 : Operating System Configuration M1024 : Restrict Registry Permissions M1054 : Software Configuration
TA0040 : Impact	T1485 : Data Destruction T1489 : Service Stop T1499 : Endpoint Denial of Service T1498 : Network Denial of Service	M1053 : Data Backup M1030 : Network Segmentation M1022 : Restrict File and Directory Permissions M1024 : Restrict Registry Permissions M1018 : User Account Management M1037 : Filter Network Traffic





THREATS AGAINST AVAILABILITY- INTERNET THREATS		
<p>The current table highlights the techniques in the MITRE ATT&CK[®] Framework associated with ransomware software, ransomware groups or both according to the legend⁶¹⁷. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques.</p>		
Tactic	Technique	Mitigation
TA0001 : Initial Access	T1189 : Drive-by Compromise	M1048 : Application Isolation and Sandboxing M1050 : Exploit Protection M1021 : Restrict Web-Based Content M1051 : Update Software
TA0007 : Discovery	T1046 : Network Service Scanning	M1042 : Disable or Remove Feature or Program M1031 : Network Intrusion Prevention M1030 : Network Segmentation
TA0009 : Collection	T1557 : Adversary-in-the-Middle	M1042 : Disable or Remove Feature or Program M1041 : Encrypt Sensitive Information M1037 : Filter Network Traffic M1035 : Limit Access to Resource Over Network M1031 : Network Intrusion Prevention M1030 : Network Segmentation M1017 : User Training



⁶¹⁶ MITRE ATT&CK[®], <https://attack.mitre.org/>

⁶¹⁷ Ransomware techniques in ATT&CK, <https://healthcyber.mitre.org/blog/resources/attack-navigator/>



TA0040 : Impact	T1498 : Network Denial of Service	M1037 : Filter Network Traffic
<h2>INFORMATION MANIPULATION AND INTERFERENCE</h2> 		
<p>It is important to note that disinformation and misinformation attacks are among the preparatory activities at the basis of other attacks (e.g. phishing, social engineering, malware infection). The MITRE ATT&CK® graph below can give an idea of the link between disinformation/misinformation and connected attacks.</p>		
Tactic	Technique	Mitigation
TA0043 : Reconnaissance	T1592 : Gather Victim Host Information T1589 : Gather Victim Identity Information T1590 : Gather Victim Network Information T1591 : Gather Victim Org Information T1598 : Phishing for Information T1597 : Search Closed Sources T1596 : Search Open Technical Databases T1593 : Search Open Websites/Domains T1594 : Search Victim-Owned Websites	M1056 : Pre-compromise M1054 : Software Configuration M1017 : User Training M1013 : Application Developer Guidance M1047 : Audit
TA0042 : Resource Development	T1586 : Compromise Accounts T1585 : Establish Accounts	M1056 : Pre-compromise
TA0001 : Initial Access	T1566 : Phishing	M1049 : Antivirus/Antimalware M1031 : Network Intrusion Prevention M1021 : Restrict Web-Based Content M1054 : Software Configuration M1017 : User Training
TA0002 : Execution	T1203 : Exploitation for Client Execution T1204 : User Execution	M1048 : Application Isolation and Sandboxing M1050 : Exploit Protection M1040 : Behaviour Prevention on Endpoint M1038 : Execution Prevention M1031 : Network Intrusion Prevention M1021 : Restrict Web-Based Content M1017 : User Training
TA0005 : Defense Evasion	T1036 : Masquerading	M1049 : Antivirus/Antimalware M1040 : Behaviour Prevention on Endpoint M1045 : Code Signing M1038 : Execution Prevention M1022 : Restrict File and Directory Permissions
TA0040 : Impact	T1565 : Data Manipulation T1491 : Defacement	M1041 : Encrypt Sensitive Information M1030 : Network Segmentation M1029 : Remote Data Storage M1022 : Restrict File and Directory Permissions M1053 : Data Backup
<h2>SUPPLY CHAIN ATTACKS</h2> 		
<p>The current table highlights the techniques in the MITRE ATT&CK® Framework associated with supply chain attacks. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new</p>		



techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques. In addition, we only list those techniques relevant for supply chain attacks, and do not include the techniques commonly used for follow-up activity.

In addition to the MITRE ATT&CK Framework, it is useful to note that MITRE revealed its 'System of Trust Framework' ⁶¹⁸ in June 2022. This framework builds a basis for trust by identifying the three main trust aspects of supply chain security, suppliers, supplies and services, and then identifying and addressing 14 top-level risk areas that require evaluation. The framework offers a comprehensive, consistent and repeatable methodology for evaluating suppliers, supplies and service providers.

Tactic	Technique	Mitigation
TA0043 : Reconnaissance	T1595 : Active Scanning T1592 : Gather Victim Host Information T1589 : Gather Victim Identity Information T1590 : Gather Victim Network Information T1591 : Gather Victim Org Information T1598 : Phishing for Information T1597 : Search Closed Sources T1596 : Search Open Technical Databases T1593 : Search Open Websites/Domains T1594 : Search Victim-Owned Websites	M1056 : Pre-compromise M1054 : Software Configuration M1017 : User Training M1013 : Application Developer Guidance M1047 : Audit
TA0042 : Resource Development	T1583 : Acquire Infrastructure T1586 : Compromise Accounts T1584 : Compromise Infrastructure T1587 : Develop Capabilities T1585 : Establish Accounts T1588 : Obtain Capabilities T1608 : Stage Capabilities	M1056 : Pre-compromise
TA0001 : Initial Access	T1195 : Supply Chain Compromise T1200 : Hardware Additions T1199 : Trusted Relationship	M1051 : Update Software M1016 : Vulnerability Scanning M1035 : Limit Access to Resource Over Network M1034 : Limit Hardware Installation M1030 : Network Segmentation M1018 : User Account Management M1032 : Multi-factor Authentication


⁶¹⁸ MITRE SoT: <https://sot.mitre.org/>





B ANNEX: RECOMMENDATIONS

Our recommendations are mapped⁶¹⁹ to the security measures that are part of international standards i.e. ISO/IEC 27001:2022⁶²⁰, NIST Cybersecurity Framework (CSF) v2.0⁶²¹, used by organisations in the various business sectors.

RANSOMWARE		
Implement a secure and redundant backup strategy. Ensure you maintain offline, encrypted data backups that are regularly tested, following your backup procedures.		
ISO/IEC 27001:2022 A5.30 ICT readiness for business continuity A8.13 Information backup A8.14 Redundancy of information processing facilities	NIST Cybersecurity Framework (CSF) PR.DS-11 Backups of data are created, protected, maintained, and tested RC.RP-03 The integrity of backups and other restoration assets is verified before using them for restoration PR.IR-04: Adequate resource capacity to ensure availability is maintained PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	
Create, maintain, and exercise an incident response plan that is regularly tested. Document the communication flows, including response and notification procedures during an incident. The ransomware Response Checklist from CISA can help you prepare.		
ISO/IEC 27001:2022 A5.24 Information security incident management planning and preparation A5.25 Assessment and decision on information security events A5.26 Response to information security incidents A5.27 Learning from information security incidents A5.29 Information security during disruption A5.30 ICT readiness for business continuity	NIST Cybersecurity Framework (CSF) ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	
Ensure your internet-facing infrastructure is secure. Perform regular vulnerability scanning to identify and address vulnerabilities. Install (security) updates and patches regularly, per your patch policy.		
ISO/IEC 27001:2022 A5.7 Threat intelligence A.8.8 Management of technical vulnerabilities	NIST Cybersecurity Framework (CSF) ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded PR.PS-02: Software is maintained, replaced, and removed commensurate with risk PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	

⁶¹⁹ Note that when a measure is applied to a given recommendation, we include all measures as documented by ENISA. For example, for the first recommendation, all measures for an 'Information system security incident response' were taken into consideration.

⁶²⁰ <https://www.iso.org/standard/27001>


⁶²¹ <https://www.nist.gov/cyberframework>



	DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis
Ensure remote access technology or other exposed services are configured security, and MFA and strong password policies are actively managed, audited, and enforced on the user accounts. Apply the principles of least privilege and separation of duties.	
ISO/IEC 27001:2022 A5.3 Segregation of duties A5.14 Information transfer A5.15 Access control A5.16 Identity management A5.17 Authentication information A5.18 Access rights A5.19 Information security in supplier relationships A5.20 Addressing information security within supplier agreements A5.21 Managing information security in the ICT supply chain A5.22 Monitoring, review and change management of supplier services A5.23 Information security for use of cloud services A6.7 Remote working A7.9 Security of assets off-premises A7.13 Equipment maintenance A8.1 User endpoint devices A8.3 Information access restriction A8.4 Access to source code A8.5 Secure authentication A8.20 Network security	NIST Cybersecurity Framework (CSF) DE.CM-06: External service provider activities and services are monitored to find potentially adverse events ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected PR.PS-02: Software is maintained, replaced, and removed commensurate with risk
Periodic security awareness and training are critical, as ransomware often relies on social engineering to lure users into clicking a link.	
ISO/IEC 27001:2022 A6.3 Information Security Awareness, Education and Training	NIST Cybersecurity Framework (CSF) Awareness and Training (PR.AT): The organization’s personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks
Collaborate with peers and national CERTs. Use the tools available for sharing malware information and -mitigation (e.g., MISP).	
ISO/IEC 27001:2022 A5.5 Contact with authorities A5.6 Contact with special interest groups A5.7 Threat intelligence A6.8 Information security event reporting	NIST Cybersecurity Framework (CSF) Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies DE.AE-06: Information on adverse events is provided to authorized staff and tools DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis
Monitor and centralise logs using a security incident and event management (SIEM) solution. Develop relevant use-cases to improve the effectiveness of detections and reduce log alert fatigue and achievable continuous monitoring.	
ISO/IEC 27001:2022 A5.28 Collection of evidence A5.33 Protection of records A8.15 Logging A8.26 Monitoring activities	NIST Cybersecurity Framework (CSF) Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events PR.PS-04: Log records are generated and made available for continuous monitoring
Ensure your assets are inventoried, managed, and under control.	



<p>ISO/IEC 27001:2022</p> <p>A5.9 Inventory of information and other associated assets A7.9 Security of assets off-premises A5.14 Information transfer</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational object's risk strategy</p> <p>DE.CM-06: External service provider activities and services are monitored to find potentially adverse events</p>
<p>Deploy EDR/XDR and ensure the signatures are up to date.</p> <p>Use application directory allow-listing, blocking any unauthorized software execution.</p> <p>Monitor process execution to detect anomalies</p> <p>Employ e-mail filtering for malicious e-mails and remove executable attachments.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.14 Information transfer A5.15 Access control A5.16 Identity management A5.17 Authentication information A5.18 Access rights A5.22 Monitoring, review and change management of supplier services A5.28 Collection of evidence A5.33 Protection of records A8.20 Network security A8.3 Information access restriction A8.5 Secure authentication A8.15 Logging A8.26 Monitoring activities</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents</p> <p>Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events</p> <p>PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p> <p>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected</p> <p>PR.PS-04: Log records are generated and made available for continuous monitoring</p>


<p>MALWARE</p> 	
<p>Create, maintain, and exercise an incident response plan that is regularly tested. Document the communication flows, including response and notification procedures during an incident.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.24 Information security incident management planning and preparation A5.25 Assessment and decision on information security events A5.26 Response to information security incidents A5.27 Learning from information security incidents A5.29 Information security during disruption A5.30 ICT readiness for business continuity</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties</p> <p>ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved</p> <p>RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared</p> <p>Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies</p>
<p>Ensure your internet-facing infrastructure is secure. Perform regular vulnerability scanning to identify and address vulnerabilities. Install (security) updates and patches regularly, per your patch policy.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.7 Threat intelligence A.8.8 Management of technical vulnerabilities</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded</p>



	<p>PR.PS-02: Software is maintained, replaced, and removed commensurate with risk</p> <p>PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle</p> <p>DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis</p> <p>ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated</p>
<p>Ensure remote access technology or other exposed services are configured security, and MFA and strong password policies are actively managed, audited, and enforced on the user accounts.</p> <p>Apply the principles of least privilege and separation of duties.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.14 Information transfer</p> <p>A5.15 Access control</p> <p>A5.16 Identity management</p> <p>A5.17 Authentication information</p> <p>A5.18 Access rights</p> <p>A5.19 Information security in supplier relationships</p> <p>A5.22 Monitoring, review and change management of supplier services</p> <p>A5.3 Segregation of Duties</p> <p>A6.7 Remote working</p> <p>A7.13 Equipment maintenance</p> <p>A7.9 Security of assets off-premises</p> <p>A8.1 User endpoint devices</p> <p>A8.18 Use of privileged utility programs</p> <p>A8.20 Network security</p> <p>A8.3 Information access restriction</p> <p>A8.4 Access to source code</p> <p>A8.5 Secure authentication</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>DE.CM-06: External service provider activities and services are monitored to find potentially adverse events</p> <p>ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles</p> <p>Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access</p> <p>Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access</p> <p>PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p> <p>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected</p> <p>PR.PS-02: Software is maintained, replaced, and removed commensurate with risk</p>
<p>Periodic security awareness and training are critical, as ransomware often relies on social engineering to lure users into clicking a link.</p>	
<p>ISO/IEC 27001:2022</p> <p>A6.3 Information Security Awareness, Education and Training</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks</p>
<p>Collaborate with peers and national CERTs. Use the tools available for sharing malware information and -mitigation (e.g., MISP).</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.5 Contact with authorities</p> <p>A5.6 Contact with special interest groups</p> <p>A5.7 Threat intelligence</p> <p>A6.8 Information security event reporting</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies</p> <p>DE.AE-06: Information on adverse events is provided to authorized staff and tools</p>
<p>Monitor and centralise logs using a security incident and event management (SIEM) solution. Develop relevant use-cases to improve the effectiveness of detections and reduce log alert fatigue and achievable continuous monitoring.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.28 Collection of evidence</p> <p>A5.33 Protection of records</p> <p>A8.15 Logging</p> <p>A8.26 Monitoring activities</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents</p> <p>Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events</p>



<p>Ensure your assets are inventoried, managed, and under control.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.9 Inventory of information and other associated assets A7.9 Security of assets off-premises A5.14 Information transfer</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational object's risk strategy</p> <p>DE.CM-06: External service provider activities and services are monitored to find potentially adverse events</p>
<p>Deploy EDR/XDR and ensure the signatures are up to date.</p> <p>Use application directory allow-listing, blocking any unauthorised software execution.</p> <p>Monitor process execution to detect anomalies.</p> <p>Employ E-mail filtering for malicious e-mails and remove executable attachments.</p> <p>Implement malware detection for all inbound/outbound channels, including e-mail, network, web, and application systems on all applicable platforms (i.e., servers, network infrastructure, personal computers, and mobile devices).</p> <p>Inspect the SSL/TLS traffic allowing the firewall to decrypt what is being transmitted to and from websites, e-mail communications, and mobile applications.</p>	
<p>ISO/IEC 27001:2022</p> <p>A8.15 Logging A5.22 Monitoring, review and change management of supplier services A5.28 Collection of evidence A8.30 Outsourced Development</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents</p> <p>Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events</p> <p>PR.PS-04: Log records are generated and made available for continuous monitoring</p>

<p>SOCIAL ENGINEERING</p> 	
<p>Review and update the incident response plans to adapt to the latest trends identified for social engineering attacks.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.7 Threat intelligence A5.24 Information security incident management planning and preparation A5.25 Assessment and decision on information security events A5.26 Response to information security incidents A5.27 Learning from information security incidents A5.29 Information security during disruption A5.30 ICT readiness for business continuity</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization</p> <p>ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties</p> <p>ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved</p> <p>RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared</p> <p>RS.MA-03: Incidents are categorized and prioritized</p> <p>ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established</p>



	RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process
<p>Maintain an overview of the digital footprint of your organisation and update this information on a frequent basis. Ideally this updating is done automatically and changes in the digital footprint trigger an alert for follow-up investigations.</p> <p>Appoint a role within your organisation to do regular OSINT research on your organisation (taking on the role of an "outsider").</p> <p>Preventively register domains that resemble your organisation's name, including alternative TLDs. Regularly review the organisations 'domain settings to support anti-spoofing and authentication mechanisms to filter e-mail.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.7 Threat intelligence</p> <p>A5.9 Inventory of information and other associated assets</p> <p>A8.8 Management of technical vulnerabilities</p> <p>A5.35 Independent review of information security</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy</p> <p>GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated</p> <p>ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded</p> <p>PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle</p> <p>ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded</p> <p>ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated</p> <p>DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis</p> <p>ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established</p> <p>PR.PS-02: Software is maintained, replaced, and removed commensurate with risk</p> <p>Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization</p> <p>Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions</p>
<p>Adjust the awareness trainings to take into account the new social engineering trends. Consider tailored trainings that focus on the HR, sales and finance departments. Also consider specific trainings for IT and security staff.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.2 Information security roles and responsibilities</p> <p>A5.3 Segregation of duties</p> <p>A6.3 Information security awareness, education and training</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks</p> <p>DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability</p> <p>GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced</p> <p>GV.RR-04: Cybersecurity is included in human resources practices</p> <p>GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established,</p>
<p>Ensure that the infrastructure of your organisation where social engineering attacks can be detected is "forensic ready", meaning the relevant logs are collected with sufficient details to support incident response investigations. Logs should be complete, reliable, accurate and consistent.</p> <p>Expand the monitoring use cases to go beyond your perimeter and to include domain and certificate monitoring that resemble the organisations 'assets. Additionally, include in these monitoring use cases detections for signs of data breaches relevant for your organisation.</p>	




<p>Employ threat intelligence relevant to detect social engineering operations and automatically apply this information for network intrusion prevention, web access and e-mail filtering.</p> <p>Subscribe to a feed of issued certificates (certificate transparency feed) and alert on names resembling your organisation's name or assets. Monitor newly issued domains for names resembling your organisation's name or assets. Subscribe to alerts from data breach monitoring sites. Subscribe to alerts of the organisation assets being published on criminal forums. Consider the use of the AIL framework⁶²².</p> <p>Deploy detection rules that alert on the presence (or opening) of disk image files on systems where these file types are not commonly present.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.22 Monitoring, review and change management of supplier services</p> <p>A5.28 Collection of evidence</p> <p>A5.33 Protection of records</p> <p>A8.8 Management of technical vulnerabilities</p> <p>A8.15 Logging</p> <p>A8.16 Monitoring activities</p> <p>A8.26 Application security requirements</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents</p> <p>Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events</p> <p>DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis</p> <p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p> <p>GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties</p> <p>ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles</p> <p>ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated</p> <p>PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p> <p>PR.PS-04: Log records are generated and made available for continuous monitoring</p> <p>RS.MA-02: Incident reports are triaged and validated</p>
<p>Block the use of disk images exchanged via e-mail.</p>	
<p>ISO/IEC 27001:2022</p> <p>A8.21 Security of network services</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>PR.IR-01: Networks and environments are protected from unauthorized logical access and usage</p>
<p>Enforce user-consent settings so users cannot consent to allow third-party application access. Only allow applications from verified publishers or for specific low-risk permissions.</p> <p>Routinely review mail server configurations, employee mail settings and connection logs. Focus efforts on identifying employee mail-forwarding rules and identifying abnormal connections to mail servers.</p> <p>Utilise e-mail security features that notify a user when an e-mail is being sent from a user they have not interacted with before.</p>	
<p>ISO/IEC 27001:2022</p> <p>A7.10 Storage media</p> <p>A8.1 User endpoint devices</p> <p>A8.19 Installation of software on operational systems</p> <p>A8.21 Security of network services</p> <p>A8.25 Secure development life cycle</p> <p>A8.26 Application security requirements</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>PR.PS-01: Configuration management practices are established and applied</p> <p>ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained</p> <p>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>PR.IR-01: Networks and environments are protected from unauthorized logical access and usage</p>

⁶²² AIL Framework <https://github.com/CIRCL/AIL-framework>



Review consented permissions for external applications on a regular basis.	
ISO/IEC 27001:2022 A5.1 Policies for information security	NIST Cybersecurity Framework (CSF) GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced

<h2 style="color: #0056b3;">THREATS AGAINST DATA</h2> 	
<p>Build a team of specialists: Having a team of specialists with skill and knowledge to respond to data breaches is critically important to maintain data availability, confidentiality, and integrity.</p> <p>Asset discovery, risk assessment, mitigation plan: A proper mitigation strategy starts from the knowledge of the assets that can be target of an attack, as well as a proper risk assessment are at the basis of a proper data security posture.</p>	
ISO/IEC 27001:2022 A5.2 Information security roles and responsibilities A5.3 Segregation of duties A5.9 Inventory of information and other associated assets A6 People controls A7.9 Security of assets off-premises A5.14 Information transfer A5.26 Response to information security incidents A5.27 Learning from information security incidents	NIST Cybersecurity Framework (CSF) Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced GV.RR-04: Cybersecurity is included in human resources practices GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared
<p>Proper security budgeting and spending: Proper planning and budgeting for data management risks is key and requires alignment in understanding security impacts between management and practitioners.623</p>	
ISO/IEC 27001:2022 A5.1 Policies for information security A5.4 Management responsibilities	NIST Cybersecurity Framework (CSF) Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy

⁶²³ 2022 Thales Data Threat Report



	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles
Support for compliance and certification:624	
<p>ISO/IEC 27001:2022</p> <p>A5.1 Policies for information security A5.28 Collection of evidence A5.31 Legislation, regulations and statutory and contractual requirements 5.32 Intellectual property rights A5.33 Protection of records A5.34 Privacy and protection of PII A5.36 Conformance with policies, rules and standards for information security A5.37 Documented operating procedures A8.34 Protection of information systems during audit testing</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.</p> <p>Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions</p>
<p>Authorisation Management: Human errors and misconfigurations are at the basis of many data breaches. A proper authorisation management that reviews access privileges according to changing rights of the users, users leaving an organisation is key to reduce possible insider threat attacks. 625</p> <p>Zero trust architectures: Zero trust architectures can increase the security posture of a system by implementing “never trust, always verify” paradigm. 626 This paradigm could be particularly important when accessing sensitive information.</p> <p>Unique and strong passwords: A proper password management approach is important to reduce the risk of an attack to a system. 627 Unique passwords avoid multiple system compromise with a single password breach. Strong passwords can increase the robustness of the system against attacks. A password manager can simplify users’ activities.</p> <p>Enforcing password hygiene: Having unique and strong passwords contributes to the protection of sensitive data. Unfortunately, the current norm tells of users adopting weak password that are easily guessable and can be broken with brute force attacks. Multi-factor authentication (T1) can be used to strengthen the authentication process using token or fingerprints. Enforcement of longer passwords or enterprise password management systems come with additional burden on users and organisations. 628</p> <p>User awareness training and education: Insufficient level of cybersecurity expertise and inadequate education of employees can lead to database breaches. Non-technical employees can put the entire system and its data at risk. Both IT security personnel and end users should be professionally trained and know the most recent cybersecurity trends. The first should increase their knowledge to implement security controls and professionally manage data; the latter should undergo basic training in database security. 629 The need of a security awareness programme stands out when social attacks are executed and result in malware installation and stolen credentials. 630</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.15 Access control A5.16 Identity management A5.17 Authentication information A5.18 Access rights A5.3 Segregation of Duties A6.3 Information security awareness, education and training A8.15 Logging A8.3 Information access restriction A8.4 Access to source code A8.5 Secure authentication</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Awareness and Training (PR.AT): The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p> <p>GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered</p> <p>GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed</p> <p>GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced</p> <p>GV.RR-04: Cybersecurity is included in human resources practices</p>

⁶²⁴ <https://artificialintelligenceact.eu/>

⁶²⁵ EU H2020 CONCORDIA, D4.3

⁶²⁶ https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf

⁶²⁷ <https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference/>

⁶²⁸ EU H2020 CONCORDIA, D4.3

⁶²⁹ EU H2020 CONCORDIA, D4.3

⁶³⁰ <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>



	<p>Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access</p> <p>PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind</p> <p>PR.PS-01: Configuration management practices are established and applied</p> <p>PR.PS-04: Log records are generated and made available for continuous monitoring</p>
<p>Data security auditing: The support of security auditing is key to identify organisational gaps and vulnerabilities, as well as data misuse. 631 Security audits can be performed either by security experts or by a third party (e.g. penetration testing model), evaluating the risk of data breaches. 632</p>	
<p>ISO/IEC 27001:2022</p> <p>A8.34 Protection of information systems during audit testing</p> <p>A5.35 Independent review of information security</p> <p>A5.36 Conformance with policies, rules and standards for information security</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>PR.PS-04: Log records are generated and made available for continuous monitoring</p> <p>ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded</p> <p>PR.PS-01: Configuration management practices are established and applied</p> <p>DE.AE-03: Information is correlated from multiple sources</p>
<p>Data sanitisation: Data sanitisation enables end-users to protect their data by decreasing the quality of data according to different techniques including anonymisation, generalisation, encryption, masking, filtering. Manipulated data can then be used for testing, training, processing. 633 634</p> <p>Countermeasures against data poisoning: Countermeasures against data poisoning are important to increase the robustness of the model by using datasets of higher quality. The dataset is evaluated to filter out poisoned data points, including poisoned data points removal, 635 replacement and healing. 636 Countermeasures should also aim to increase the strength of the model itself, for instance, by using an ensemble of models to reduce the impact of a poisoning attack. 637 638</p> <p>Adversarial training: Adversarial training is important to protect a ML model against inference-time attacks. It builds on training set augmentation (adversarial training), 639 where adversarial data points are added to the training set to increase the resilience of the model against malicious data points.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.37 Documented operating procedures</p> <p>A7.10 Storage media</p> <p>A8.1 User endpoint devices</p> <p>A8.19 Installation of software on operational systems</p> <p>A8.21 Security of network services</p> <p>A8.24 Use of cryptography</p> <p>A8.25 Secure development life cycle</p> <p>A8.26 Application security requirements</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events</p> <p>GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed</p> <p>ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained</p> <p>ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked</p>

⁶³¹ EU H2020 CONCORDIA, D4.3

⁶³² EU H2020 CONCORDIA, D4.3

⁶³³ EU H2020 CONCORDIA, D4.3

⁶³⁴ Marco Anisetti, Claudio A. Ardagna, Chiara Braghin, Ernesto Damiani, Antongiaco Polimeno, and Alessandro Balestrucci. 2021. Dynamic and Scalable Enforcement of Access Control Policies for Big Data. Proceedings of the 13th International Conference on Management of Digital EcoSystems.

⁶³⁵ N. Peri, N. Gupta, W. R. Huang, L. Fowl, C. Zhu, S. Feizi, T. Goldstein, and J. P. Dickerson, 'Deep k-NN Defence Against Clean-Label Data Poisoning Attacks,' in Proc. of ECCV 2020, August 2020.

⁶³⁶ E. Rosenfeld, E. Winston, P. Ravikumar, and Z. Kolter, 'Certified Robustness to Label-Flipping Attacks via Randomised Smoothing,' in Proc. of ICML 2020, Virtual, June 2020.

⁶³⁷ J. Jia, X. Cao, and N. Z. Gong, 'Intrinsic Certified Robustness of Bagging against Data Poisoning Attacks,' in Proc. of AAAI 2021, Virtual, February 2021.

⁶³⁸ W. Wang, A. Levine, and S. Feizi, 'Improved Certified Defences against Data Poisoning with (Deterministic) Finite Aggregation,' arXiv preprint arXiv:2202.02628, 2022.

⁶³⁹ A. Kurakin, D. Boneh, F. Tramèr, I. Goodfellow, N. Papernot, and P. McDaniel, 'Ensemble Adversarial Training: Attacks and Defences,' in Proc. of ICLR 2018, Vancouver, BC, Canada, April, May 2018.



<p>A8.27 Secure system architecture and engineering principles</p> <p>8.28 Secure coding</p> <p>A8.31 Separation of development, test and production environments</p> <p>A8.32 Change management</p>	<p>ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use</p> <p>PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk</p> <p>PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p> <p>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected</p> <p>PR.IR-01: Networks and environments are protected from unauthorized logical access and usage</p> <p>PR.PS-01: Configuration management practices are established and applied</p>
--	--

Data Loss Prevention solutions: Inspecting and controlling file management and transfer is key to avoid sensitive and personal data or intellectual property does not exit the corporate network or to a user without access.

<p>ISO/IEC 27001:2022</p> <p>A5.14 Information transfer</p> <p>A5.32 Intellectual property rights</p> <p>A5.33 Protection of records</p> <p>A5.34 Privacy and protection of PII</p> <p>A8.10 Information deletion</p> <p>A8.11 Data masking</p> <p>A8.12 Data leakage prevention</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>ID.AM-03: Representations of the organization’s authorized network communication and internal and external network data flows are maintained</p> <p>PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p> <p>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected</p>
---	--

Data backups: Data backups are fundamental to support prompt recovery from attacks. 640 Backup sites must be geographically distributed and separated to avoid being tampered by the same attack. Geographical redundancy can also help in preventing damages originating from natural disasters and sudden power outages.

<p>ISO/IEC 27001:2022</p> <p>A5.30 ICT readiness for business continuity</p> <p>A8.13 Information backup</p> <p>A8.14 Redundancy of information processing facilities</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>PR.DS-11 Backups of data are created, protected, maintained, and tested</p> <p>RC.RP-03 The integrity of backups and other restoration assets is verified before using them for restoration</p> <p>PR.IR-04: Adequate resource capacity to ensure availability is maintained</p> <p>PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p> <p>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected</p>
--	--

THREATS AGAINST AVAILABILITY



Build a team of specialists: having a team of specialists with the skills and knowledge to respond to DDoS attacks is critically important to maintain system availability and operation.

<p>ISO/IEC 27001:2022</p> <p>A5.2 Information security roles and responsibilities</p> <p>A5.3 Segregation of duties</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability</p>
--	---

⁶⁴⁰ EU H2020 CONCORDIA, D4.3



<p>A5.9 Inventory of information and other associated assets A6 People controls</p>	<p>GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced GV.RR-04: Cybersecurity is included in human resources practices GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established,</p>
<p>Knowledge on third-party agreements: a response to a DDoS attack with third parties. Validating third-party agreements and contact information is key.</p>	
<p>ISO/IEC 27001:2022 A5.19 Information security in supplier relationships A5.20 Addressing information security within supplier agreements A5.21 Managing information security in the ICT supply chain A5.22 Monitoring, review and change management of supplier services A5.23 Information security for use of cloud services</p>	<p>NIST Cybersecurity Framework (CSF) Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders</p>
<p>Service restore: a plan B should exist in order to quickly restore business-critical services and reduce the mean time to recovery.</p>	
<p>ISO/IEC 27001:2022 A5.29 Information security during disruption A5.30 ICT readiness for business continuity A7.13 Equipment maintenance A8.13 Information backup A8.14 Redundancy of information processing facilities</p>	<p>NIST Cybersecurity Framework (CSF) ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations PR.IR-04: Adequate resource capacity to ensure availability is maintained RS.MI-02: Incidents are eradicated</p>
<p>Asset discovery, risk assessment and mitigation plan: a proper mitigation strategy starts from knowledge of the assets that can be the target of an attack as well as a proper assessment of risk⁶⁴¹. All critical elements (e.g. servers, services and applications) should be protected and included in recurrent tests of a DDoS mitigation plan⁶⁴².</p>	
<p>ISO/IEC 27001:2022 A5.9 Inventory of information and other associated assets A5.8 Information security in project management A5.14 Information transfer A5.22 Monitoring, review and change management of supplier services A5.35 Independent review of information security A7.9 Security of assets off-premises A7.13 Equipment maintenance A8.8 Management of technical vulnerabilities A8.25 Secure development life cycle A8.32 Change management</p>	<p>NIST Cybersecurity Framework (CSF) Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and</p>

⁶⁴¹ Neustar, Pay Or Else: DDoS Ransom Attacks

⁶⁴² <https://www.netscout.com/blog/asert/ddos-attack-campaign-targeting-multiple-organizations-ukraine>



	assumptions are established, communicated, and used to support operational risk decisions
<p>Guarantee Best Current Practices (BCPs): organisations at risks should support relevant network infrastructure, architectural and operational best current practices (BCPs), for instance, proper network access policies and traffic filtering⁶⁴³.</p> <p>Update and patch your system: the basic rules of updating and patching all systems should become a mantra, especially in scenarios involving IoT and smart devices⁶⁴⁴. For instance, Mozi botnet continues to rely on the same set of older vulnerabilities, even those that are eight years old⁶⁴⁵.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.7 Threat intelligence A5.14 Information transfer A5.37 Documented operating procedures A.8.8 Management of technical vulnerabilities A8.19 Installation of software on operational systems A8.20 Networks security A8.21 Security of network services A8.25 Secure development life cycle A8.26 Application security requirements A8.32 Change management A8.27 Secure system architecture and engineering principles A8.31 Separation of development, test and production environments</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis DE.CM-01: Networks and network services are monitored to find potentially adverse events DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events DE.CM-06: External service provider activities and services are monitored to find potentially adverse events DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events ID.AM-03: Representations of the organization’s authorized network communication and internal and external network data flows are maintained ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked PR.IR-01: Networks and environments are protected from unauthorized logical access and usage PR.PS-01: Configuration management practices are established and applied PR.PS-02: Software is maintained, replaced, and removed commensurate with risk PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle</p>
<p>Deploy sufficient resources to increase the cost of an attack: DDoS attacks can be counteracted by deploying as much resources as possible or moving the target system to a powerful infrastructure (e.g. cloud infrastructure)⁶⁴⁶. For instance, the higher the bandwidth of a system or service, the more difficult or expensive a successful attack will be for a cybercriminal⁶⁴⁷.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.8 Information security in project management A5.22 Monitoring, review and change management of supplier services A7.13 Equipment maintenance A8.8 Management of technical vulnerabilities A8.25 Secure development life cycle A8.32 Change management</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles ID.RA-10: Critical suppliers are assessed prior to acquisition PR.IR-04: Adequate resource capacity to ensure availability is maintained</p>

⁶⁴³ <https://www.netscout.com/blog/asert/ddos-attack-campaign-targeting-multiple-organizations-ukraine>

⁶⁴⁴ <https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends>

⁶⁴⁵ eset_threat_report_t22021


⁶⁴⁶ Neustar, Pay Or Else: DDoS Ransom Attacks

⁶⁴⁷ <https://hacked.com/will-2022-be-the-year-of-the-ddos-attack/>



	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk
Model traffic trends and profiles: knowledge of the traffic trends and tendencies in the network is paramount to creating a baseline to simplify the detection of anomalies in the network activities that can be an indicator of a DDoS attack. Network and application monitoring tools can be used for this, further restricting the volume of incoming traffic^{648 649}.	
ISO/IEC 27001:2022 A5.28 Collection of evidence A5.33 Protection of records A8.15 Logging A8.16 Monitoring activities	NIST Cybersecurity Framework (CSF) Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events PR.PS-04: Log records are generated and made available for continuous monitoring
Cybersecurity training and education: DDoS attacks are often built on a strong set of activities in preparation that range from botnet building to attack coordination and orchestration⁶⁵⁰. The remediations for these threats depend on correct and complete training and education in cybersecurity⁶⁵¹.	
ISO/IEC 27001:2022 A5.2 Information security roles and responsibilities A6.3 Information Security Awareness, Education and Training	NIST Cybersecurity Framework (CSF) Awareness and Training (PR.AT): The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

INFORMATION MANIPULATION AND INTERFERENCE



Information manipulation and interference is a complex issue, where cybersecurity is only one of multiple components. Indeed, one problem in addressing information manipulation and interference is that, because of the multi-faceted nature of this threat, different organisations and governments act in an uncoordinated manner. A whole-of-society approach, which is an inclusive approach ensuring participation of parties with diverse backgrounds and perspectives can help addressing.

A number of recommendations are reported below⁶⁵²

Strategic level

- **Foster mutual exchanges between the cybersecurity and the community of defenders against information manipulation.** Concepts of cybersecurity can be applied to the detection and analysis of FIMI/disinformation incidents and operations. Existing frameworks, taxonomies, tools, structures and interoperable standards from cybersecurity can be adapted and adopted by the counter FIMI/disinformation community to speed up analytical maturity and interoperability within and beyond the field. For example, the EEAS is supporting the creation of an open source, decentralised and interoperable framework that increases the efficiency of sharing threat insights between the different stakeholders involved in FIMI analysis and disruption⁶⁵³.
- **Improve the availability and quality of data on information manipulation.** Aggregable, structured, machine-readable and representative data on information manipulation is so far mostly unavailable. While individual data and research exist and stakeholders do share highly relevant insights, the sector is still underdeveloped compared to the diversity, specialisation and quantity of information shared in the cybersecurity sector. In this sense, the

⁶⁴⁸ David Warburton, F5Labs, DDoS Attack Trends for 2020, May 2021, <https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020>

⁶⁴⁹ Neustar Security, Cyber Threats & Trends: Securing Your Network Pandemic-Style, 2020 <https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pdf>

⁶⁵⁰ D4.2 concordia

⁶⁵¹ H-ISAC. Distributed Denial of Service (DDoS) Attacks, March 2021 <https://www.aha.org/system/files/media/file/2021/03/distributed-denial-of-service-ddos-attacks-march-2021.pdf>

⁶⁵² These recommendations stem from the 2022 ENISA-EEAS joint report 'Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape'. For this edition of the ETL they have been updated as needed.

⁶⁵³ <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf>



adoption of standard formats to share information, such as such as STIX⁶⁵⁴, the Standard Threat Information Expression language, could be a crucial step to move beyond information sharing by written reports.

Policy level

- **Facilitating, including with financial support, institutional/organisational cooperation and capacity building, especially to prevent and handle crisis and surrounding important events.**

Operational level

- **Reporting on information manipulation should consider cybersecurity aspects more systematically and should be supported by structured and seamless incident reporting among different actors.** One of the most relevant limitations in the analysis of information manipulation events has been the quality of the data. Open-source data about information manipulation events might not contain sufficient information about its cybersecurity aspects. For example, in many cases the description of the cyber-component was not sufficiently detailed to identify the cybersecurity techniques utilised. This is particularly relevant also because the role of cybersecurity seems to be particularly important in establishing attribution.
- **Although the joint use of the DISARM and MITRE ATT&CK frameworks facilitates the identification of trends, their application relies on some degree of interpretation to adapt the former to cybersecurity and the latter to information manipulation.** For example, while DISARM's TTPs allow a fairly accurate description of the unfolding of information manipulation events, it encompasses only few tactics explicitly related to cybersecurity operations. Conversely, MITRE ATT&CK excels in capturing TTPs of cybersecurity threat actors, including, to some extent, the set-up of infrastructure to carry out information manipulation operations, but given its scope and main focus it does not go in detail in describing them. Other frameworks, in particular the Online Operations Kills Chain⁶⁵⁵, focus on disrupting the IT infrastructure used for information manipulation - regardless of the impact on the cybersecurity "CIA triad". **All of these frameworks have their strengths (such as openness to revision and accuracy in describing events from their own perspectives), hence it is recommended that the counter-disinformation community works on guidance on how different frameworks could coherently and seamlessly work together from an operational perspective, in order to cover the whole spectrum of information manipulation operations.** The ENISA-EEAS FIMI Threat landscape (reference) published in 2022 and the subsequent analyses in ETL 2023 and ETL 2024 serve this goal by aligning analysis of FIMI incidents using both DISARM and MITRE ATT&CK frameworks.
- **Given the role of cyber-attacks at initial stages of an information manipulation campaign, awareness raising is important to limit the development or acquisition of content and the compromise of infrastructure that facilitate dissemination.** In particular, since the more high-level the compromised account is, the more legitimacy it has, it is important that high-profile members of governmental/public and media/audio-visual sectors are aware of this.
- **It is important for organisations to strengthen practices for critical information gathering, triaging, and distribution processes also considering the need to verify the authenticity of the information in order to mitigate the impact of polluted data and mischaracterised information.**⁶⁵⁶
- **Social platform detection and mitigation are still among the most important technical countermeasures.** These countermeasures include, for example, the suspension of inauthentic accounts and identification and limitation of automated behaviours⁶⁵⁷. However, efforts to improve detection of upstream activities used to prepare information manipulation operations should be continued.

SUPPLY CHAIN ATTACKS



Establish a formal C-SCRM (Cyber Supply Chain Risk Management) programme and setup a dedicated third-party risk management office.

ISO/IEC 27001:2022

- A5.1 Policies for information security
- A5.14 Information transfer
- A5.19 Information security in supplier relationships

NIST Cybersecurity Framework (CSF)

Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders

⁶⁵⁴ See <https://stixproject.github.io/>

⁶⁵⁵ <https://carnegieendowment.org/research/2023/03/phase-based-tactical-analysis-of-online-operations?lang=en>

⁶⁵⁶ <https://www.ofcom.org.uk/news-centre/2022/one-in-three-internet-users-fail-to-question-misinformation>

⁶⁵⁷ <https://www.apa.org/monitor/2022/06/news-misinformation-attack>



<p>A5.20 Addressing information security within supplier agreements</p> <p>A5.21 Managing information security in the ICT supply chain</p> <p>A5.22 Monitoring, review and change management of supplier services</p> <p>A5.23 Information security for use of cloud services</p> <p>A5.31 Legislation, regulations and statutory and contractual requirements</p> <p>A6.2 Terms and conditions of employment</p> <p>A6.5 Responsibilities after termination or change of employment</p> <p>A8.30 Outsourced Development</p>	<p>GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered</p> <p>GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders</p> <p>Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies</p>
<p>Include key suppliers in business continuity and incident response plans and exercises.</p> <p>Get insight into the functioning and services of the PSIRTs of key vendors, possibly with the help of the FIRST PSIRT Services Framework. It is strongly recommended that vendors start a PSIRT (according to the FIRST PSIRT Services Framework⁶⁵⁸) and coordinate security communications with customers via this PSIRT.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.24 Information security incident management planning and preparation</p> <p>A5.25 Assessment and decision on information security events</p> <p>A5.26 Response to information security incidents</p> <p>A5.27 Learning from information security incidents</p> <p>A5.28 Collection of evidence</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions</p> <p>Incident Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities</p> <p>Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects</p> <p>Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies</p> <p>Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization, organisational assets, and individuals.</p> <p>RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared</p>
<p>In awareness campaigns include a warning that users should not re-use passwords at vendors.</p>	
<p>ISO/IEC 27001:2022</p> <p>A6.3 Information Security Awareness, Education and Training</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Awareness and Training (PR.AT): The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>
<p>Develop your defences based on the principle that your systems will be breached. Start small and log and track asset activity on and between internal networks (user, system and services logs, network data such as DNS queries and NetFlow, etc.).</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.22 Monitoring, review and change management of supplier services</p> <p>A5.25 Assessment and decision on information security events</p> <p>A5.28 Collection of evidence</p> <p>A5.33 Protection of records</p> <p>A8.8 Management of technical vulnerabilities</p> <p>A8.15 Logging</p> <p>A8.16 Monitoring activities</p> <p>A8.26 Application security requirements</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents</p> <p>Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events</p> <p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p> <p>GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties</p>

⁶⁵⁸ FIRST PSIRT Services Framework https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1



	<p>ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles</p> <p>PR.PS-04: Log records are generated and made available for continuous monitoring</p> <p>Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization</p> <p>RS.MA-02: Incident reports are triaged and validated</p>
<p>There should be no gap between physical security and cybersecurity. Ensure that physical access to devices is restricted and authenticated.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.9 Inventory of information and other associated assets</p> <p>A5.10 Acceptable use of information and other associated assets</p> <p>A5.11 Return of assets</p> <p>A7 Physical controls</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational object's risk strategy</p> <p>DE.CM-02: The physical environment is monitored to find potentially adverse events</p> <p>DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events</p> <p>DE.CM-06: External service provider activities and services are monitored to find potentially adverse events</p> <p>PR.AA-03: Users, services, and hardware are authenticated</p> <p>PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk</p> <p>PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p> <p>PR.IR-01: Networks and environments are protected from unauthorized logical access and usage</p> <p>PR.IR-02: The organization's technology assets are protected from environmental threats</p> <p>PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations</p> <p>PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk</p>
<p>Establish protocols for vulnerability disclosure and incident notification and establish protocols for communications with external stakeholders during incidents. Apply the FIRST659 guidelines and practices for multi-party vulnerability coordination and disclosure.</p> <p>Use third-party assessments, site visits and formal certification to assess critical suppliers. Look beyond the software (or hardware) product and examine a suppliers' approach towards cybersecurity. Do not rely solely on vendor supplied documentation or information. Trust, but verify.</p> <p>Create an inventory of all the hardware, software and service providers on which you rely and trust. Make sure this inventory is checked automatically. Connections from unknown devices or software or abnormal traffic patterns from service providers should trigger an alert for follow-up investigations.</p> <p>A patch management process should be implemented to check unused dependencies, unmaintained and/or previously vulnerable dependencies, unnecessary features, components, files and documentation. Ensure all software is up-to-date.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.7 Threat intelligence</p> <p>A5.9 Inventory of information and other associated assets</p> <p>A5.14 Information transfer</p> <p>A5.35 Independent review of information security</p> <p>A7.9 Security of assets off-premises</p> <p>A8.8 Management of technical vulnerabilities</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy</p> <p>DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis</p> <p>GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered</p>

⁶⁵⁹ FIRST SIG: <https://www.first.org/global/sigs/vulnerability-coordination/multi-party/guidelines-v1.1>



	<p>ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded</p> <p>ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated</p> <p>Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions</p> <p>PR.PS-02: Software is maintained, replaced, and removed commensurate with risk</p> <p>PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle</p>
<p>Document and align responsibilities in SaaS or PaaS managed cloud services.</p> <p>Have a vulnerability management policy. Ensure vulnerabilities are identified and tracked.</p> <p>Apply 'one strike and you're out' policies with respect to vendor products that are either counterfeit or do not match specifications as contractually agreed and/or documented.</p> <p>Include security requirements in all RFPs and contracts.</p> <p>Ensure boot integrity and require firmware and driver security. Ensure that all firmware and drivers installed on servers or end-user equipment follow the necessary security requirements and have the documentation needed to prove their compliance.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.1 Policies for information security</p> <p>A5.2 Information security roles and responsibilities</p> <p>A5.7 Threat intelligence</p> <p>A5.23 Information security for use of cloud services</p> <p>A5.31 Legislation, regulations and statutory and contractual requirements</p> <p>A5.32 Intellectual property rights</p> <p>A5.36 Conformance with policies, rules and standards for information security</p> <p>A8.7 Protection against malware</p> <p>A8.8 Management of technical vulnerabilities</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders</p> <p>DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis</p> <p>GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced</p> <p>GV.RR-04: Cybersecurity is included in human resources practices</p> <p>ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded</p> <p>ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated</p> <p>Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood</p> <p>PR.PS-02: Software is maintained, replaced, and removed commensurate with risk</p> <p>PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle</p>
<p>Implement continuous monitoring of sources of vulnerabilities and the use of tools for automatic and manual reviews of code.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.22 Monitoring, review and change management of supplier services</p> <p>A8.15 Logging</p> <p>A8.16 Monitoring activities</p> <p>A8.7 Protection against malware</p> <p>A8.8 Management of technical vulnerabilities</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents</p> <p>Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events</p> <p>ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained</p> <p>ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use</p>



	PR.PS-04: Log records are generated and made available for continuous monitoring
Setup tight controls on access by service vendors. Enforce the use of encrypted communications and multi-factor authentication.	
ISO/IEC 27001:2022 A5.16 Identity management A5.17 Authentication information A5.18 Access rights A8.4 Access to source code A8.18 Use of privileged utility programs	NIST Cybersecurity Framework (CSF) Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access and transactions. PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected
Setup communication channels with the various PSIRTs of your vendors.	
ISO/IEC 27001:2022 A5.5 Contact with authorities A5.6 Contact with special interest groups A5.7 Threat intelligence A5.13 Labelling of information	NIST Cybersecurity Framework (CSF) DE.AE-06: Information on adverse events is provided to authorized staff and tools Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies
Enable MFA for access to developer accounts⁶⁶⁰.	
ISO/IEC 27001:2022 A5.15 Access control A5.17 Authentication information A8.3 Information access restriction A8.5 Secure authentication	NIST Cybersecurity Framework (CSF) Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access and transactions. PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected
Apply code hashing authentication.	
Scan and audit containers before putting them into production.	
ISO/IEC 27001:2022 A8.24 Use of cryptography A8.31 Separation of development, test and production environments A8.34 Protection of information systems during audit testing	NIST Cybersecurity Framework (CSF) PR.PS-02: Software is maintained, replaced, and removed commensurate with risk PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected PR.IR-01: Networks and environments are protected from unauthorized logical access and usage
Isolate legacy systems and development ('non-production') systems in separate network segments.	
ISO/IEC 27001:2022 A8.20 Networks security A8.31 Separation of development, test and production environments	NIST Cybersecurity Framework (CSF) PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected

⁶⁶⁰ <https://github.blog/2022-03-28-how-to-secure-your-end-to-end-supply-chain-on-github/>



	<p>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected</p> <p>PR.IR-01: Networks and environments are protected from unauthorized logical access and usage</p> <p>PR.PS-01: Configuration management practices are established and applied</p>
<p>Use container image signing.</p>	
<p>ISO/IEC 27001:2022</p> <p>A5.31 Legislation, regulations and statutory and contractual requirements</p> <p>A8.24 Use of cryptography</p>	<p>NIST Cybersecurity Framework (CSF)</p> <p>PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected</p> <p>PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected</p> <p>PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected</p> <p>GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed</p> <p>PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk</p> <p>PR.IR-01: Networks and environments are protected from unauthorized logical access and usage</p>





ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA

European Union Agency for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office

95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu



ISBN 978-92-9204-675-0

DOI: 10.2824/0710888