enisa 20 years!

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

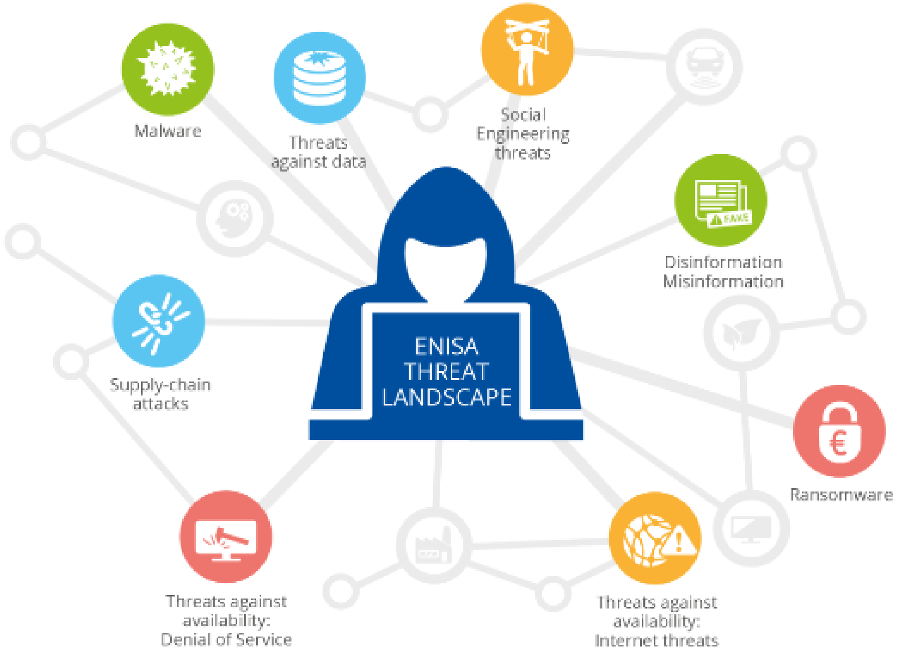
CYBERSECURITY TRENDS IN DIGITAL INFRASTRUCTURE

Ilias Bakatsis
Cybersecurity Expert

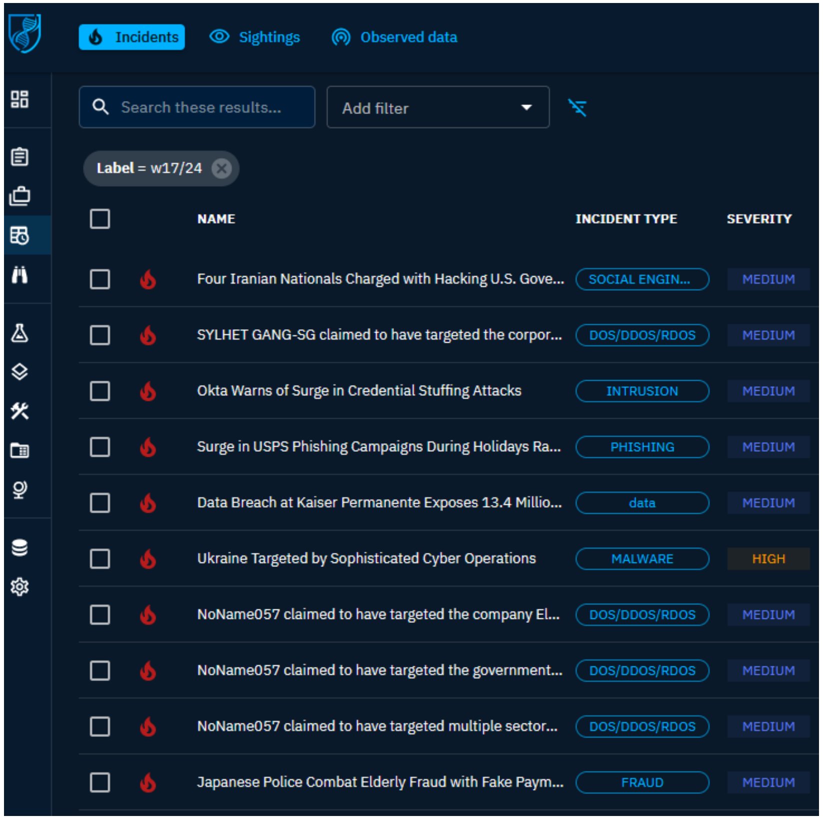
15 | 05 | 2024

ENISA SITUATIONAL AWARENESS

- **Information on Facts and Figures**
- **Threat and Incident Analysis**
- **Operational Risk Evaluation and Guidance**


Malware
Threats against data
Social Engineering threats
Disinformation Misinformation
Supply-chain attacks
ENISA THREAT LANDSCAPE
Ransomware
Threats against availability: Denial of Service
Threats against availability: Internet threats

OSINT REPORT: DATA COLLECTION



Incidents Sightings Observed data

Search these results... Add filter

Label = w17/24

□	NAME	INCIDENT TYPE	SEVERITY
□	Four Iranian Nationals Charged with Hacking U.S. Gove...	SOCIAL ENGIN...	MEDIUM
□	SYLHET GANG-SG claimed to have targeted the corpor...	DOS/DDOS/RDOS	MEDIUM
□	Okta Warns of Surge in Credential Stuffing Attacks	INTRUSION	MEDIUM
□	Surge in USPS Phishing Campaigns During Holidays Ra...	PHISHING	MEDIUM
□	Data Breach at Kaiser Permanente Exposes 13.4 Millio...	data	MEDIUM
□	Ukraine Targeted by Sophisticated Cyber Operations	MALWARE	HIGH
□	NoName057 claimed to have targeted the company El...	DOS/DDOS/RDOS	MEDIUM
□	NoName057 claimed to have targeted the government...	DOS/DDOS/RDOS	MEDIUM
□	NoName057 claimed to have targeted multiple sector...	DOS/DDOS/RDOS	MEDIUM
□	Japanese Police Combat Elderly Fraud with Fake Paym...	FRAUD	MEDIUM

How We Process the Data:

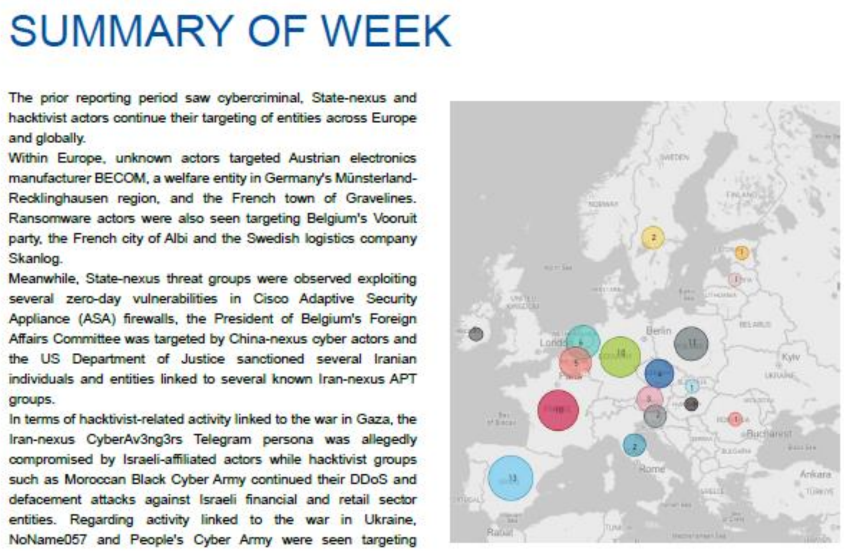
- **We gather data daily using OpenCTI, ensuring continuous monitoring and timely updates.**
- **We select the most compelling stories and proceed with data enrichment to provide deeper insights and enhanced value.**
- **After a transition phase through April, we standardized our data collection to a JSON format, optimizing data handling and analysis**

OSINT REPORT

ENISA OSINT REPORT WEEK 17

TLP:GREEN

Date: 30th April 2024 | Covering the period from 23rd April to 29th April 2024



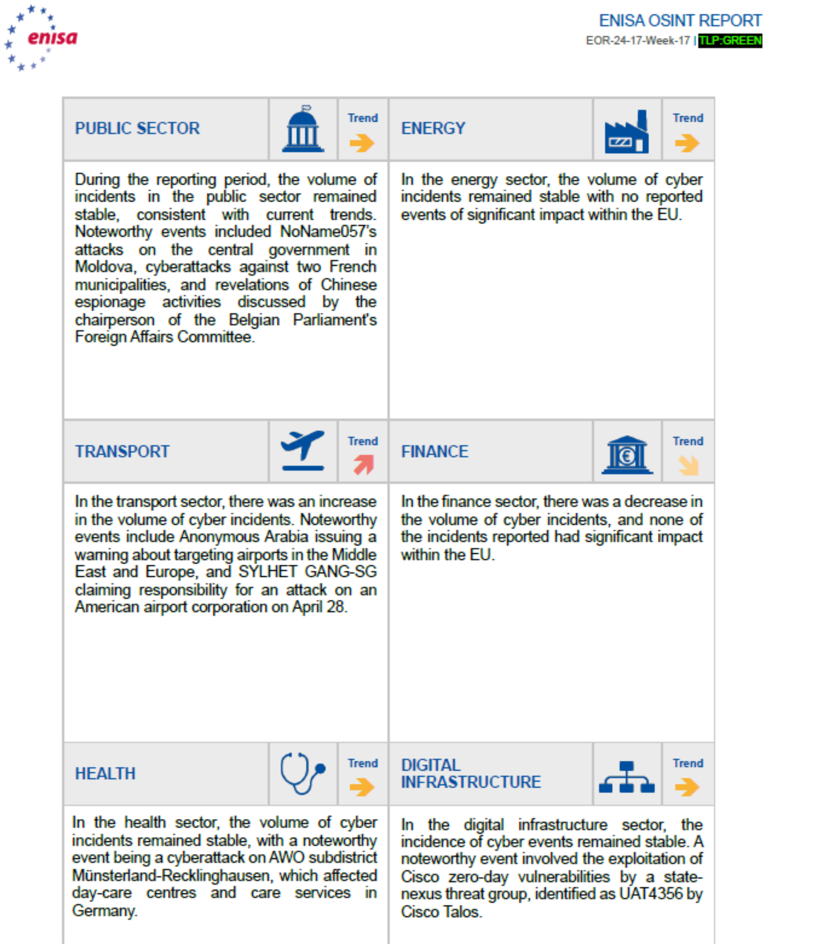
SUMMARY OF WEEK

The prior reporting period saw cybercriminal, State-nexus and hacktivist actors continue their targeting of entities across Europe and globally.

Within Europe, unknown actors targeted Austrian electronics manufacturer BECOM, a welfare entity in Germany's Münsterland-Recklinghausen region, and the French town of Gravelines. Ransomware actors were also seen targeting Belgium's Vooruit party, the French city of Albi and the Swedish logistics company Skanlog.

Meanwhile, State-nexus threat groups were observed exploiting several zero-day vulnerabilities in Cisco Adaptive Security Appliance (ASA) firewalls, the President of Belgium's Foreign Affairs Committee was targeted by China-nexus cyber actors and the US Department of Justice sanctioned several Iranian individuals and entities linked to several known Iran-nexus APT groups.

In terms of hacktivist-related activity linked to the war in Gaza, the Iran-nexus CyberAv3ng3rs Telegram persona was allegedly compromised by Israeli-affiliated actors while hacktivist groups such as Moroccan Black Cyber Army continued their DDoS and defacement attacks against Israeli financial and retail sector entities. Regarding activity linked to the war in Ukraine, NoName057 and People's Cyber Army were seen targeting



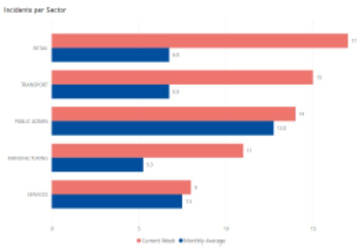
ENISA OSINT REPORT
EOR-24-17-Week-17 | TLP:GREEN

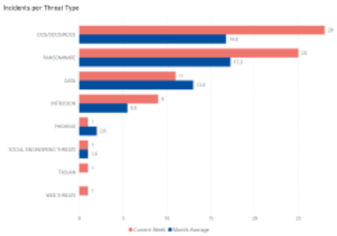
PUBLIC SECTOR	Trend →	ENERGY	Trend →
During the reporting period, the volume of incidents in the public sector remained stable, consistent with current trends. Noteworthy events included NoName057's attacks on the central government in Moldova, cyberattacks against two French municipalities, and revelations of Chinese espionage activities discussed by the chairperson of the Belgian Parliament's Foreign Affairs Committee.		In the energy sector, the volume of cyber incidents remained stable with no reported events of significant impact within the EU.	
TRANSPORT	**Trend ↗**	**FINANCE**	**Trend ↘**
In the transport sector, there was an increase in the volume of cyber incidents. Noteworthy events include Anonymous Arabia issuing a warning about targeting airports in the Middle East and Europe, and SYLHET GANG-SG claiming responsibility for an attack on an American airport corporation on April 28.		In the finance sector, there was a decrease in the volume of cyber incidents, and none of the incidents reported had significant impact within the EU.	
HEALTH	**Trend →**	**DIGITAL INFRASTRUCTURE**	**Trend →**
In the health sector, the volume of cyber incidents remained stable, with a noteworthy event being a cyberattack on AWO subdistrict Münsterland-Recklinghausen, which affected day-care centres and care services in Germany.		In the digital infrastructure sector, the incidence of cyber events remained stable. A noteworthy event involved the exploitation of Cisco zero-day vulnerabilities by a state-nexus threat group, identified as UAT4356 by Cisco Talos.	

OSINT REPORT

STATISTICS AND DASHBOARDS

THREAT TYPE AND SECTORS[1][2]





In the recent reporting period, the retail and transport sectors experienced a surge in incidents, exceeding their monthly averages, while public administration and manufacturing sectors also saw notable activity. DDoS attacks and ransomware continue to be prominent threats, with data breaches and intrusions also prevalent. Additionally, phishing and social engineering threats remain present, highlighting the diverse threat landscape across various sectors.

RECENT KNOWN EXPLOITED VULNERABILITIES[3]

CVE ID	CVSS v3	Date Added	Vendor	Product
CVE-2022-38028	7.8 HIGH	23/04/2024	Microsoft	Windows Print Spooler
CVE-2024-4040	10.0 CRITICAL	24/04/2024	CrushFTP	CrushFTP VFS
CVE-2024-20353	8.6 HIGH	24/03/2024	Cisco	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)

[DE] German AWO Münsterland-Recklinghausen subdistrict mail system gets compromised

Geography	Event noted on	Sector	Threat actor	Threat type	Relevancy	Confidence
Germany	29/04/2024	Public Administration	Unknown	Phishing	LOW	A1

On 22 April, the AWO Münsterland-Recklinghausen subdistrict's mail system was accessed by an unauthorized threat actor. This intrusion resulted in approximately 30,000 phishing emails being sent out. According to the official statement, to prevent further unauthorized access, the mail system was temporarily shut down. The AWO is encouraging email recipients to check emails for phishing attempts before opening them.

Analyst comment

As of the time of writing there is no information as to how the threat actor gained access to AWO's systems. This incident emphasises the importance of informing all stakeholders about the risks of phishing and how to identify suspicious emails, making them able to avoid one of the most widely used initial access methods by threat actors. This breach will likely be abused by threat actors to spread social engineered phishing campaigns targeting affected users.

Sources

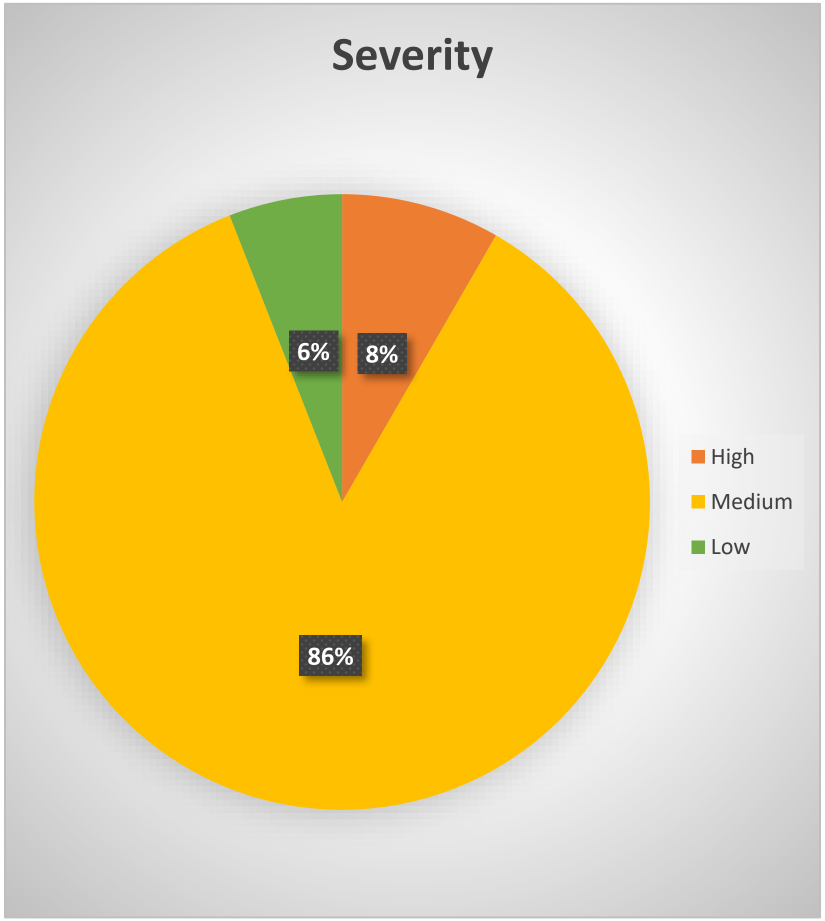
Source[1]: https://www.awo-msl-re.de/organisation/meldungen/vorsicht-vor-spam-und-phishing-mails

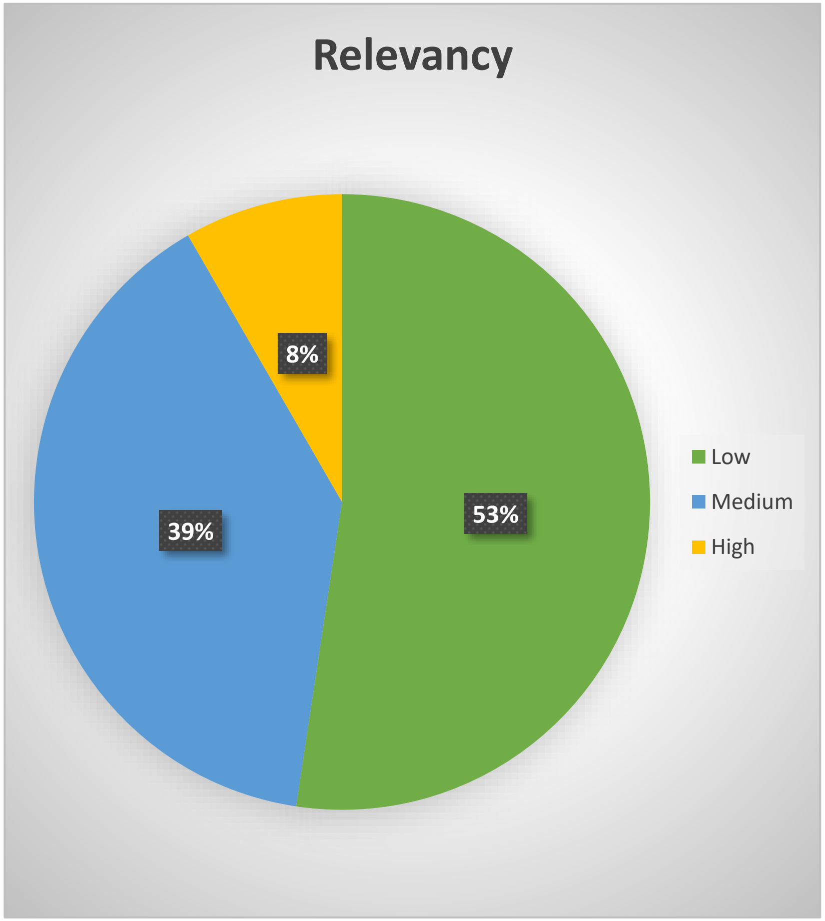
**Subscriptions:
sat@enisa.europa.eu**

How many Incidents?

Since January, we have recorded 84 incidents specifically affecting EU Member States, as part of a broader dataset comprising 345 events. This dataset includes vulnerabilities, campaigns, and outcomes of security research

INCIDENT SEVERITY AND RELEVANCY DISTRIBUTION

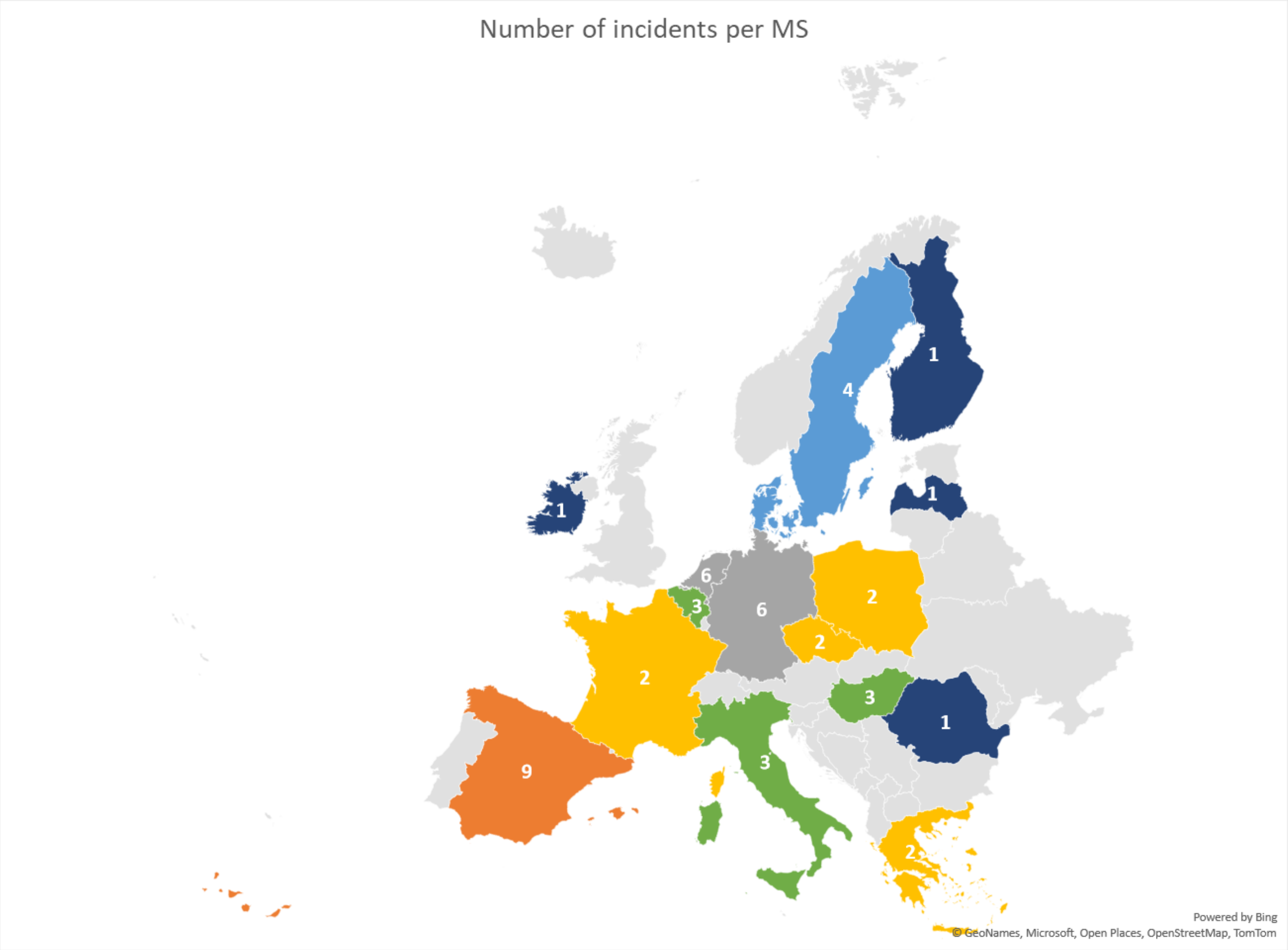




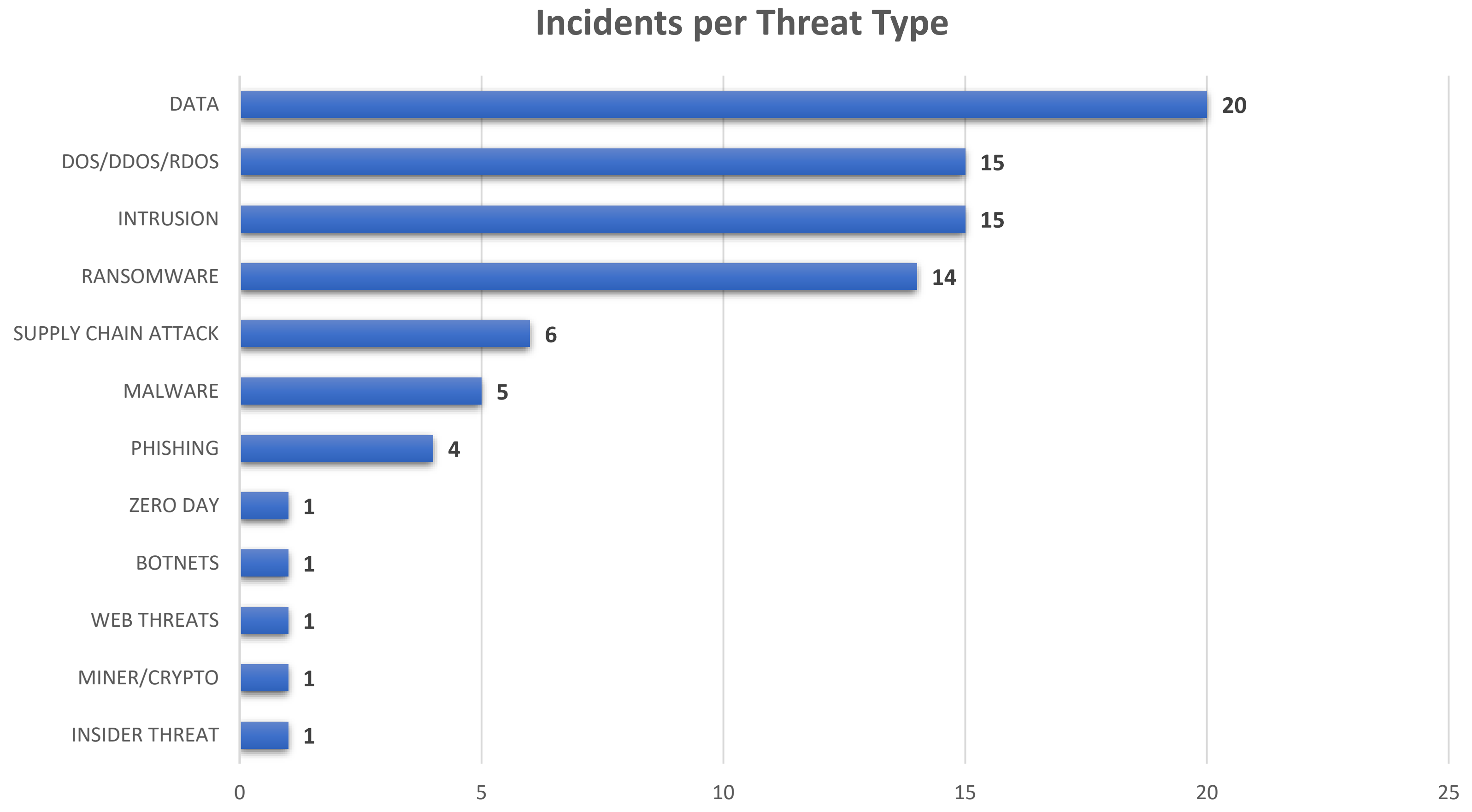
We have identified 70 distinct threat actors, with the following being the most active:

- Akira
- Cyber Army of Russia
- UTA0218
- Anonymous Collective
- Blacksuit
- CyberDragon
- People's Cyber Army
- RED ransomware
- UserSec

MOST AFFECTED MS


Number of incidents per MS
1
4
1
1
6
3
6
2
2
2
3
1
9
3
2
Powered by Bing
© GeoNames, Microsoft, Open Places, OpenStreetMap, TomTom

TOP THREAT TYPES



THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

☎ +30 28 14 40 9711

✉ info@enisa.europa.eu

🌐 www.enisa.europa.eu