



From January 2019 to April 2020

Phishing

ENISA Threat Landscape



Overview

Phishing is the fraudulent attempt to steal user data such as login credentials, credit card information, or even money using social engineering techniques. **This type of attack is usually launched through e-mail messages, appearing to be sent from a reputable source, with the intention of persuading the user to open a malicious attachment or follow a fraudulent URL.** A targeted form of phishing called 'spear phishing' relies on upfront research on the victims so that the scam appears more authentic, thereby, making it one of the most successful types of attack on enterprises' networks.¹

An emotional response justifies many people actions when they are phished and is exactly what hackers are looking for. In a training context, that is what a phishing simulation should try to achieve. Training e-mail users is one of the often used measures for preventing phishing, but results are not convincing since threat actors are constantly changing their *modus operandi*. The domain-based message authentication, reporting, and conformance (DMARC) standard ensures that e-mail from fraudulent domains is blocked, diminishing the rate of success of phishing, spoofing and spam² attacks.

In the future, e-mail continues to be the number one mechanism for phishing but not for long. We are already seeing an increase in the use of social media messaging, WhatsApp and others to conduct attacks. The most relevant change will be in the methods used to send the messages, which will become more sophisticated with the adoption of adversarial Artificial Intelligence (AI) to prepare and send the messages. Phishing and spear phishing are major attack vectors of other threats such as unintentional insider threats².



Findings

26.2_ billion of losses in 2019 with Business E-mail Compromise (BEC) attacks²⁰

42,8%_ of all malicious attachments were Microsoft Office documents²⁵

667%_ increase in phishing scams in only 1 month during the COVID-19 pandemic⁶

30%_ of phishing messages were delivered on Mondays²⁹

32,5%_ of all the e-mails used the keyword 'payment' in the e-mail subject²⁸



Kill chain



Phishing

Reconnaissance

Weaponisation

Delivery

Exploitation

-  *Step of Attack Workflow*
-  *Width of Purpose*





Installation

Command &
Control

Actions on
Objectives

The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

[MORE INFORMATION](#)

Most targeted types of services are webmail and software-as-a-service

According to some projections, phishing attacks targeting software-as-a-service (SaaS) and webmail services surpassed those against payment services for the first time in Q1 2019, making them the most targeted sector at 36% of all phishing attacks.² This new record follows the trend in 2018 when SaaS and webmail services had just overtaken the financial sector³. Although the figure had dropped to 30,8% by the end of 2019, the services mentioned above still remained at the top of the list^{2,3}, with **Microsoft 365 services being the phishers' top target.**⁴

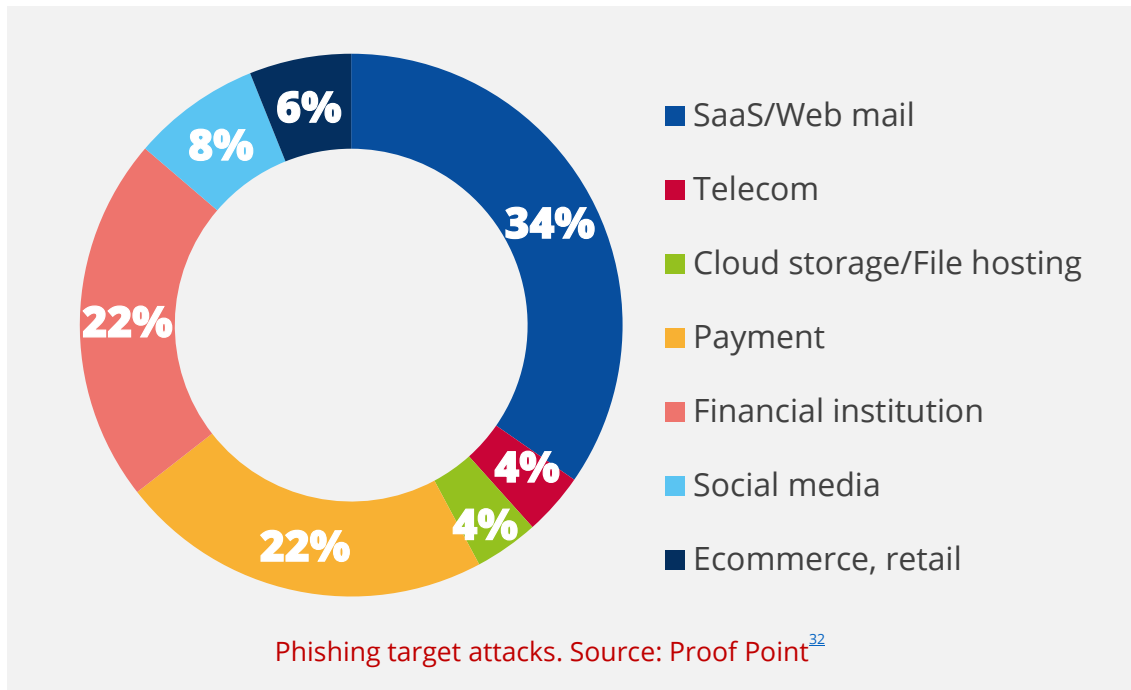
Business Email Compromise (BEC) attacks continued to be a problem

A recent study identified that 88% of worldwide organisations experienced spear phishing attacks and 86% of them faced BEC attacks.¹⁶ In 2019, one of the most targeted service was Microsoft 365 and the main focus was on harvesting credentials.¹⁷ Once these credentials had been acquired, the attacker was able to collect more organisational data, a process that could last for weeks or months¹⁸ and could then lead to spear-phishing attacks. The attacker would impersonate an employee, chief executive officer (CEO) or even a trusted supplier to divert funds or re-route payments to third-party accounts.¹⁴ In Q1 2019, companies were targeted by BEC attacks 120% more frequently than a year earlier¹⁹, resulting in losses as high as US \$26,2 billion (ca. €22,2 billion).²⁰

More than two thirds of phishing sites adopted HTTPS

There has been a steep increase¹³ over the past few years in the number of phishing sites that have adopted HTTPS. In the last quarter of 2019, 74% of phishing sites were using HTTPS³², a significant increase compared with just 32% only 2 years earlier. Although technologies such as HTTPS and SSL are designed to secure communications between a client and a server, the presence of a lock in an icon at the browser's address bar may create the illusion that a website can be trusted.

Threat actors may also use legitimate sites they have hacked to host phishing content, therefore making it challenging for the end-user to identify a site as unsafe¹⁴. Other factors contributing to the steep rise in HTTPS usage are the plethora of free certificate services such as Let's Encrypt¹⁵ and the fact that modern browsers mark every HTTPS site as secure, without any further checks.



Phishing-as-a-Service (PhaaS) on the rise

These types of services are typically subscription-based or in the form of a kit, available to download for a fee, and remove the technological barriers to entry, as they allow a less technically skilled individual to carry out a targeted attack. A report from a security researcher²¹ identified 5.334 unique phishing kits available by June 2019. What was even more concerning was the relatively low cost of these solutions, around US \$50-\$80 for a monthly subscription. The same report declared that 87% of the kits included evasion mechanisms such as HTML character encoding and content encryption. Interestingly, some of these services were hosted on legitimate cloud services with proper domain name system (DNS) names and certificates. Statistics from just one of these dark-net marketplaces show how successful these attacks are allowing the attacker or group to steal around 65.000 accounts per month.²²

Trends in incidents

- There was a change in the effectiveness of phishing attacks using cloud storage, DocuSign, and Microsoft cloud services.
- Impostor attacks include schemes like business e-mail compromise (BEC) and identity deception techniques based on social engineering to make phishing campaigns more effective.
- Microsoft 365 services phishing was the top scheme, but the focus remains on credential harvesting.
- Over 99% of e-mails distributing malware required human intervention - following links, opening documents, accepting security warnings, and other behaviours - to be effective.⁴⁴





Top phishing themes in 2019

- Generic Email Credential Harvesting
- Office 365 Account Phishing
- Financial Institution Phishing
- Microsoft OWA Phishing
- OneDrive Phishing
- American Express Phishing
- Chalbhai Generic Phishing
- Adobe Account Phishing
- Docusign Phishing
- Netflix Phishing
- Dropbox Account Phishing
- LinkedIn Account Phishing
- Apple Account Phishing
- Postal/Shipping Company Phishing
- Microsoft Online Document Phishing (Excel and Word)
- Windows Settings Phishing
- Google Drive Phishing
- PayPal Phishing

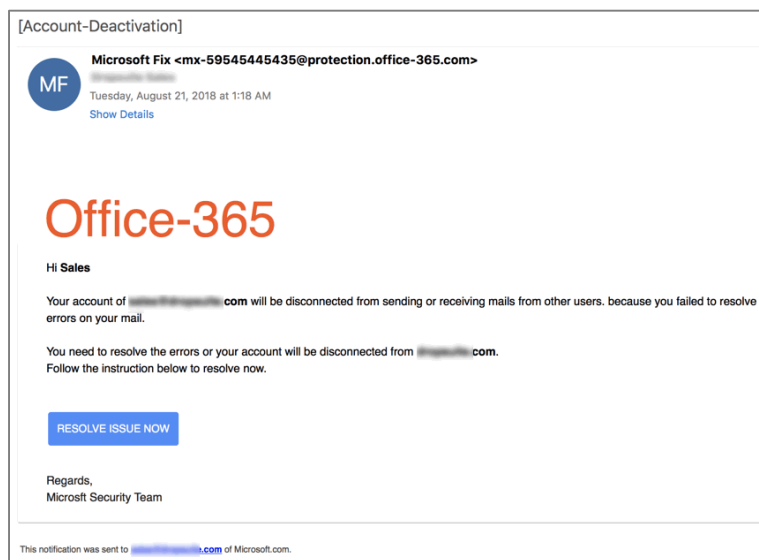
Source: Proof Point³²



COVID-19 used as a phishing lure

Cybercriminals are taking advantage of the public fear of the COVID-19 pandemic, which first appeared in late 2019. It has been reported that phishing attacks involving the virus increased by 667% in a 1-month period (between the end of February 2020 and the end of March 2020), and these types of schemes alone represented a notable 2% of all phishing scams.⁵

New scams involved phishing e-mails designed to look as if they originated from the United States Centre of Disease Control (CDC)⁶, the World Health Organisation⁷ or even from university health teams⁸. They either falsely claimed to showcase infection in the victim's area or shared medical experts' opinions to lure the victim to follow a malicious link. For this reason, the FBI and WHO have issued warnings.^{8,9} Because many people in quarantine were working from home, often using outdated security systems¹¹, cybercriminals were seeking to exploit emerging opportunities and vulnerabilities¹².



Office 365 Phishing e-mail, credit Dropsuite⁴⁵



ENISA's response to the COVID-19 pandemic

The outbreak of COVID-19 has brought an immense change in the way we conduct our lives. In this increasingly connected world, we can fortunately continue our professional and private lives virtually. During this unprecedented time, the EU Agency for Cybersecurity (ENISA) shared its cybersecurity recommendations⁴⁶ on a variety of topics including working remotely, shopping online, and e-health as well as providing updates on key security advice tailored to the sectors affected. ENISA reviews the threat landscape during the pandemic and produces advice on how to mitigate the risks from the most critical threats. Special attention given to phishing due to the escalation in the number of attacks.



ENISA YouTube video about COVID-19. Source ENISA

_ Targeted sectors

The healthcare sector was heavily targeted by phishing (or spear-phishing) attacks in 2019. A security researcher⁴² considered phishing as the main attack vector of the year, through the use of social engineering tactics to deliver e-mails infected with malware² or with links pointing to infected websites. Other sectors were also targeted by phishing attacks such as governments and other public administration entities. For example, in November and December 2019, several diplomats and officials from the Ukrainian government received spear-phishing e-mails directing them to compromised websites.⁴³

_ Attack vectors

Spear phishing remains an extremely prevalent initial access technique used by malicious actors. These use a variety of social engineering tactics to induce recipients to open attachments or navigate to a infected website. Spear-phishing messages typically contain malicious macro-enabled Microsoft Office documents, or a link to such documents. After a user selects 'Enable Content', the embedded macro will typically begin the execution of a chain of obfuscated scripts that ultimately results in the download of stage one or dropper malware. JavaScript and PowerShell appear to remain the most popular scripting languages for this purpose.



Examples

_A phishing attack to Lancaster University students' resulted in the loss of personal data³⁷

_Hackers phished login credentials of 2500 Discord users³⁸

_Online fitness service provider victim of a phishing attack³⁹

_Patients affected in UConn Health phishing attack⁴¹

_A car manufacturer subsidiary lost US \$37 million (ca. €31 million) due to a BEC scam³³



Mitigation

Proposed actions

- Educate staff to identify fake and malicious e-mails and stay vigilant. Launch simulated phishing campaigns to test organisation's infrastructure as well as the responsiveness of the staff.
- Consider the use of a security e-mail gateway with regular (possibly automated) maintenance of filters (anti-spam, anti-malware, policy-based filtering).
- Consider applying security solutions that use machine-learning techniques to identify phishing sites in real-time.
- Disable automatic execution of code, macros, rendering of graphics and preloading mailed links at the mail clients and update them frequently.
- Implement one of the standards for reducing spam e-mails: SPF (Sender Policy Framework)³⁴, DMARC (Domain-based Message Authentication, Reporting & Conformance)³⁵ and DKIM (Domain Keys Identified Mail).³⁶
- Ideally, use secure e-mail communication using digital signatures or encryption, for critical financial transactions or when exchanging sensitive information.
- Implement fraud and anomaly detection at the network level for both inbound and outbound e-mails.
- Avoid clicking on random links, especially short links found in social media.
- Do not click on links or download attachments if you are not absolutely confident about the source of an e-mail.





- Avoid over-sharing personal information on social media, e.g. duration of absence from office or home, flight information etc. as it is actively used by threat actors to collect information about their targets.
- Check the domain name of the websites you visit for typos, especially for sensitive websites, e.g. bank websites. Threat actors usually register fake domains that look similar to legitimate ones and use them to 'phish' their targets. Looking only for an HTTPS connection is not enough.
- Enable two-factor authentication whenever applicable to prevent account takeovers.
- Use a strong and unique password for every online service. Re-using the same password for various services is a serious security issue and should be avoided at all times. Using strong and unique credentials for every online service limits the risk of a potential account takeover to only the affected service. Using a password manager software will make managing of the whole set of passwords easier.
- When wiring money to an account, double-check the bank recipient's information through a different medium. Unencrypted and unsigned e-mails should not be trusted, especially for sensitive use-cases such as this.
- Check how contact, registration, subscription and feedback forms work on your website and add verification rules if necessary so that they cannot be exploited by attackers.

References

1. "What Is Phishing?". Cisco. <https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html>
2. "Phishing Activity Trends Report Q1". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf
3. "2018 Phishing Trends & Intelligence Report" 2018. Phishlabs. https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf
4. "Microsoft remains phishers' #1 target for the fifth straight quarter" August 22, 2019. Vade Secure. <https://www.vadesecond.com/en/phishers-favorites-q2-2019/>
5. "Threat Spotlight: Coronavirus-Related Phishing". March 26, 2020. <https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/>
6. "Coronavirus phishing emails: How to protect against COVID-19 scams" 2020. <https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html>
7. "Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer". 2020. IBM. <https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826>
8. "Abnormal Attack Stories #6: Coronavirus Credential Theft" March 13, 2020. <https://abnormalsecurity.com/blog/abnormal-attack-stories-6-coronavirus-credential-theft/>
9. "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic". March 20, 2020. FBI. <https://www.ic3.gov/media/2020/200320.aspx>
10. "Beware of criminals pretending to be WHO". 2020. WHO. <https://www.who.int/about/communications/cyber-security>
11. "Global police agencies issue alerts on Covid-related cyber-crime". April 6, 2020. SC Magazine. <https://www.scmagazineuk.com/global-police-agencies-issue-alerts-covid-related-cyber-crime/article/1679473>
12. "Catching the virus cybercrime, disinformation and the COVID-19 pandemic". April 3, 2020. EUROPOL. <https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic>
13. "New FireEye Email Threat Report Reveals Increase in Social Engineering Attacks". June 25, 2019. FireEye. <https://www.fireeye.com/company/press-releases/2019/new-fireeye-email-threat-report-reveals-increase-in-social-engin.html>
14. "HTTPS Protocol Now Used in 58% of Phishing Websites". June 24, 2019. Trend Micro. <https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/https-protocol-now-used-in-58-of-phishing-websites>
15. Let's Encrypt. <https://letsencrypt.org/>
16. "2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike". January 23, 2020. Proof Point. <https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical>
17. "Human factor report". 2019. Proof Point. <https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf>



18. "Phishing Activity Trends Report Q3". 2019. APWG.
https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf
19. "Business Email Compromise Results in \$26B in Losses Over the Last Three Years". September 12, 2019. Proof Point. <https://www.proofpoint.com/us/corporate-blog/post/business-email-compromise-results-26b-losses-over-last-three-years>
20. "Business Email Compromise The \$26 Billion Scam" September 10, 2019. FBI.
<https://www.ic3.gov/media/2019/190910.aspx>
21. "Evasive Phishing Driven by Phishing-as-a-Service". July 1, 2019. Cyren.
<https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service>
22. "Phishing made easy: Time to rethink your prevention strategy?". 2016. Imperva.
<https://www.imperva.com/docs/Imperva-Hill-phishing-made-easy.pdf>
23. "Q3 2019: Email Fraud and Identity Deception Trends". 2019. Agari.
<https://www.agari.com/insights/ebooks/2019-q3-report/>
24. "FBI: BEC Losses Soared to \$1.8 Billion in 2019". February 12, 2020. Infosecurity Magazine.
<https://www.infosecurity-magazine.com/news/fbi-bec-losses-soared-to-18/>
25. "Email: Click with Caution". June 2019. Cisco.
<https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf>
26. "Experts report a rampant growth in the number of malicious, lookalike domains". November 18, 2019. <https://securityaffairs.co/wordpress/94021/hacking/lookalike-domains-tls-certificate.html>
27. "Proofpoint Q3 2019 Threat Report — Emotet's return, RATs reign supreme, and more". November 7, 2019. Proof Point. <https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more>
28. "Human Factor Report." 2019. Proof Point.
<https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf>
29. "2019 Phishing and fraud report" 2019. F5 Labs. https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf
30. "Report: Microsoft, PayPal, and Netflix Most Impersonated Brands in Phishing Attacks in Q1 2019" May 8, 2019. Trend Micro.
<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/report-microsoft-paypal-and-netflix-most-impersonated-brands-in-phishing-attacks-in-q1-2019>
31. "Spam and phishing in Q3 2019". November 26, 2019. Kaspersky.
<https://securelist.com/spam-report-q3-2019/95177/>
32. "Phishing Activity Trends Report". 2019. APWG.
https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf
33. "Toyota Subsidiary Loses \$37 Million Due to BEC Scam" September 20, 2019. CPO Magazine.
<https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/>
34. Open SPF. <http://www.openspf.org/>
35. "Domain-based Message Authentication, Reporting & Conformance ". DMARC.
<https://dmarc.org/>

References

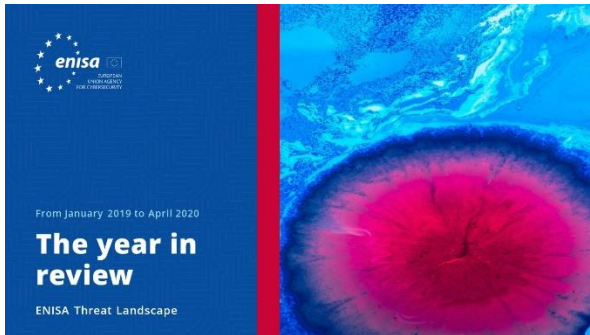
36. "DomainKeys Identified Mail (DKIM)". DKIM. <http://www.dkim.org/>
37. "Cyber incident". July 22, 2019. Lancaster University. <https://www.lancaster.ac.uk/news/phishing-attack>
38. "Hackers publish login credentials of 2500 Discord users" July 22, 2019. Cyware Social. <https://cyware.com/news/hackers-publish-login-credentials-of-2500-discord-users-8d3ea2c7>
39. "Bodybuilding.com Breach: Proof That An Organization's Biggest Cyber Risk Is Its People" April 24, 2019. Forbes. <https://www.forbes.com/sites/jameshadley/2019/04/24/bodybuilding-com-breach-proof-that-an-organizations-biggest-cyber-risk-is-its-people/#1ea113751bef>
40. "Phishing Attack Exposes 600k Health Records" June 19, 2019. Secure World. <https://www.secureworldexpo.com/industry-news/healthcare-data-breach-example-2019>
41. "326,000 Patients Impacted in UConn Health Phishing Attack". February 25, 2019. Health IT Security. <https://healthitsecurity.com/news/326000-patients-impacted-in-uconn-health-phishing-attack>
42. "Cybercrime Tactics and Techniques: the 2019 state of healthcare". 2019. Malwarebytes. <https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-the-2019-state-of-healthcare/>
43. "Significant Cyber Incidents". 2019. CSIS. <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>
44. "More Than 99% of Cyberattacks Need Victims' Help". September 9, 2019. Dark Reading. <https://www.darkreading.com/cloud/more-than-99--of-cyberattacks-need-victims-help/d/d-id/1335769>
45. "office-365-phishing-attacks-deconstructed" <https://dropsuite.com/office-365-phishing-attacks-deconstructed/>
46. ENISA. <https://www.enisa.europa.eu/topics/wfh-covid19>



“An emotional response justifies many people actions when they are phished and is exactly what hackers are looking for.”

in ETL 2020

Related



[READ THE REPORT](#)

ENISA Threat Landscape Report **The year in review**

A summary on the cybersecurity trends for the period between January 2019 and April 2020.



[READ THE REPORT](#)

ENISA Threat Landscape Report **List of Top 15 Threats**

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

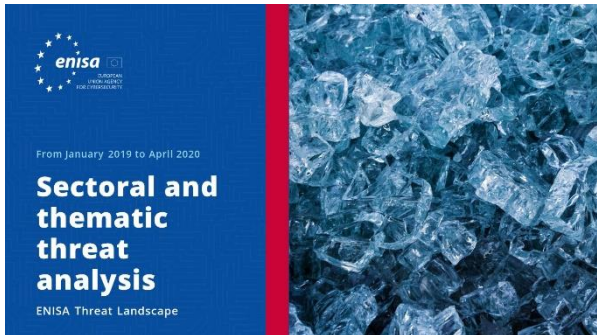


[READ THE REPORT](#)

ENISA Threat Landscape Report **Research topics**

Recommendations on research topics from various quadrants in cybersecurity and cyberthreat intelligence.





[READ THE REPORT](#)

ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.



[READ THE REPORT](#)

ENISA Threat Landscape Report **Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.



[READ THE REPORT](#)

ENISA Threat Landscape Report **Cyber Threat Intelligence overview**

The current state of play of cyberthreat intelligence in the EU.

– The agency

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 at www.enisa.europa.eu.

Contributors

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group*: Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

Editors

Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

Contact

For queries on this paper, please use enisa.threat.information@enisa.europa.eu.

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





Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

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

This publication is intended for information purposes only. It must be accessible free of charge. 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.

Copyright Notice

© European Union Agency for Cybersecurity (ENISA), 2020
Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover: © Wedia. 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: 978-92-9204-354-4

DOI: 10.2824/552242



Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece

Tel: +30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu



All rights reserved. Copyright ENISA 2020.

<https://www.enisa.europa.eu>

