enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Malware

ENISA Threat Landscape

Overview

Malware is a common type of cyberattack in the form of malicious software. Families of malware include cryptominers, viruses, ransomware, worms and spyware. Its common objectives are information or identity theft, espionage and service disruption.[1]

During 2019, cryptominers were one of the most prevalent malware family in the threat landscape,[2] resulting in high IT costs, increased electricity consumption and reduced employee productivity.[3] Ransomware presented a slight increase in 2019 compared with 2018, though still remaining at the bottom of the malware type list.[2]

Web and e-mail protocols were the most common initial attack vectors used to spread malware. However, using brute force techniques or exploiting system vulnerabilities, certain malware families were able to spread even further inside a network. Although global detections of attacks have remained at the previous year's levels, there was a noticeable shift from consumer to business targets.[4]

Findings

400.000_ detections of pre-installed spyware and adware on mobile devices[4]

13%_ increase in Windows malware detections at business endpoints globally[4]

71%_ of organizations experienced malware activity that spread from one employee to another[47]

46,5%_ of all malware in e-mail messages found in '.docx' file type[24]

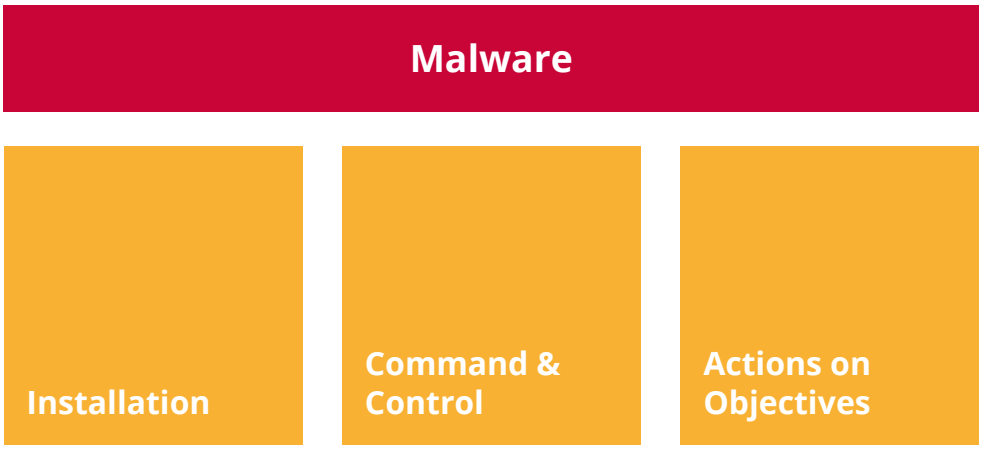
50%_ increase in malware designed to steal personal data or stalkerware[15]

67%_ of malware was delivered via encrypted HTTPS connections[48]

Kill chain

Step of Attack Workflow

Width of Purpose



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.

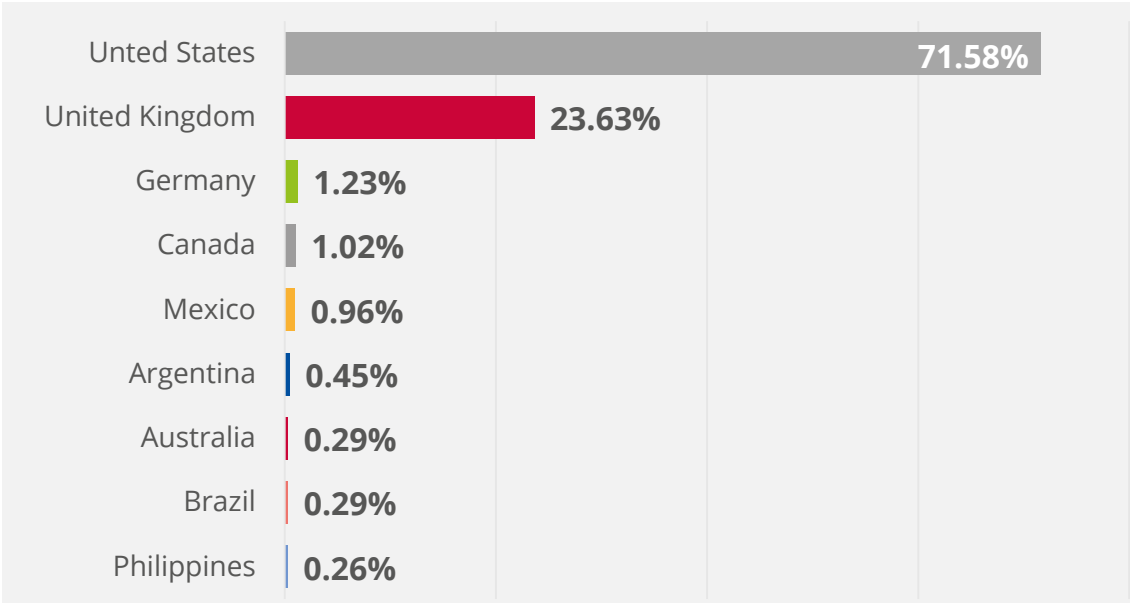
MORE INFORMATION

Trends

_Most prevalent malware types

Emotet was the most prevalent malware strain in 2019 and is evolving in 2020. Emotet was initially discovered in 2014 as a banking trojan. Since then, it has been upgraded with command and control (C2) functionality, additional evasion mechanisms such as the ability to tell whether if it is running in a sandbox environment and the ability to deliver dangerous payloads, such as Trickbot and Ryuk.[7] The figure above presents the raking of baking malware detected in 2019.

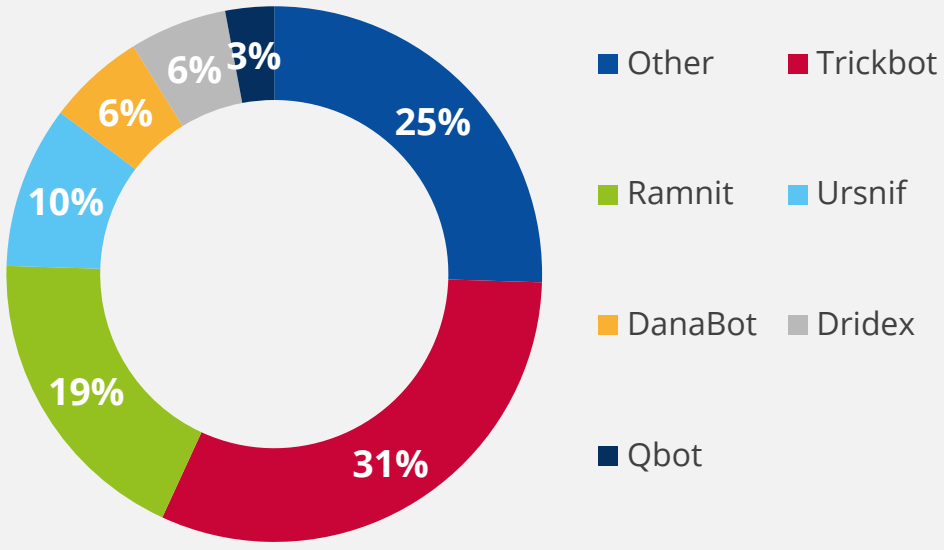
During the reporting period, Emotet evolved into a botnet[2], increased its activity[8] and initiated new localized spam campaigns with spear-phishing functionality to install ransomware or steal information.[5] During 2019, Emotet detections increased by 73% compared with previous year, mainly targeting business endpoints in the United States and the United Kingdom as presented in the figure below.[4]



2019 global Emotet detections by country. Source MalwareBytes[4]

A shift towards business targets

Although malware detections globally remained at the same levels as in 2018[4,9], a 13% increase in malware targeting businesses was observed in services, education and retail among the worst affected sectors.[4] It is estimated that over one third of banking malware attacks in 2019 targeted corporate users, with the intention of compromising the company's financial resources.[10] The top five strains of malware[4] targeting businesses were Trojan.Emotet, Adware.InstallCore, HackTool.WinActivator, Riskware.BitCoinMiner and Virus.Renamer. Ransomware attacks targeting the public sector increased in 2019 because of its ability to pay higher ransoms.[11] As Cybercriminals aim for high-value targets, new malware types were designed to spread laterally inside a corporate network rather than through the internet.[12]



Global banking malware detections in 2019. Source: CheckPoint[2]

Malware-as-a-service (MaaS)

Malware-as-a-service (MaaS) refers to a specific malware sold in underground forums which provides customers (cyber criminals) with the tools and infrastructure needed for targeted attacks. A MaaS owner provides this service through the delivery of a kit that includes an initial loader, command and control Server (C2) and a backdoor for taking full control of the infected computer.

A security researcher[46] recently identified four type of attacks using various tools from the Golden Chickens (GC) Malware-as-a-Service (MaaS) portfolio, confirming the release of improved variants with code updates to three of these tools.

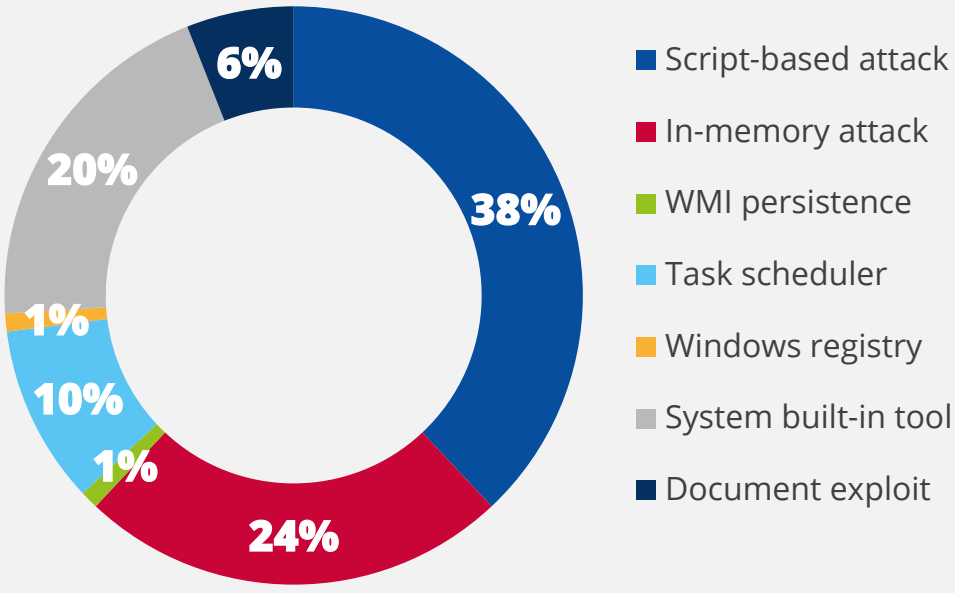
- **TerraLoader**. A multipurpose loader written in PureBasic. TerraLoader is a flagship product of GC MaaS service portfolio.
- **more_eggs**. A backdoor malware capable of beaconing to a fixed C2 server and executing additional payloads downloaded from an external web resource. The backdoor is written in JavaScript.
- **VenomLNK**. A Windows shortcut file likely generated by a newer version of the VenomKit building kit.

Mobile banking malware surged

Mobile applications designed to steal payment data, credentials and funds from victims' bank accounts increased by 50% in the first half of 2019.[13] Traditionally, threat actors have used phishing techniques to gain bank credentials, either by displaying a fake page that mimics the bank's login page or by introducing fake mobile apps that resemble the original banking apps. However, in 2019, cybercriminals became more creative, as in the case of Trojan-Banker.AndroidOS.Gustuff.a, which was able to control a legitimate banking app by misusing the operating system's accessibility functions, thereby automating malicious transactions.[14] New versions of mobile financial malware were commonly found for sale in underground forums[15] and new evasion techniques were continuously being developed. A notable new addition discovered in 2019 was the ability of malware to use motion sensors and be triggered only when a smartphone is moving, as used by the mobile banking trojanAnubis in an effort to detect a sandboxed environment.[16] The most popular banking malware during 2019[11] was Asacub (44,4%), Svpeng (22,4%), Agent (19,1%), Faketoken (12%) and Hqwar (3,8%).

File-less malware

Fileless malware does not contain an executable file and can evade common security filters and whitelisting techniques. For this reason, this malware family can be up to ten times more likely to succeed than the others.[18] Instead of an executable file, this type of malware requires the attacker to inject malicious code into already installed and trusted software, either remotely (e.g. in the case of Windows Management Instrumentation or WMI and PowerShell) or by actively downloading document files (i.e. office documents) containing malicious macros.[19] After a successful attack, the malware can gain persistence through the registry, built-in task scheduler or the WMI. Fileless malware attacks increased by 265% during the first half of 2019.[20] The majority of such attacks were script-based (38%), while others executed an in-memory attack (24%) or abused built-in system tools (20%).[21]



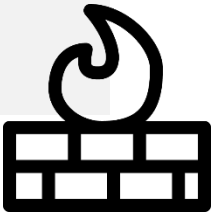
Percentage of file-less events detected in first half of 2019. Source: Norton[19]

How to prevent and defend from a file-less attack?

The most effective way for organisations to defend against fileless attacks is by keeping software up to date. Since most fileless infections happen with Microsoft applications and especially with '.docx' files, it is particularly important to keep updating this software to the latest version. Microsoft has also upgraded its Windows Defender package to detect irregular activity using the PowerShell application.

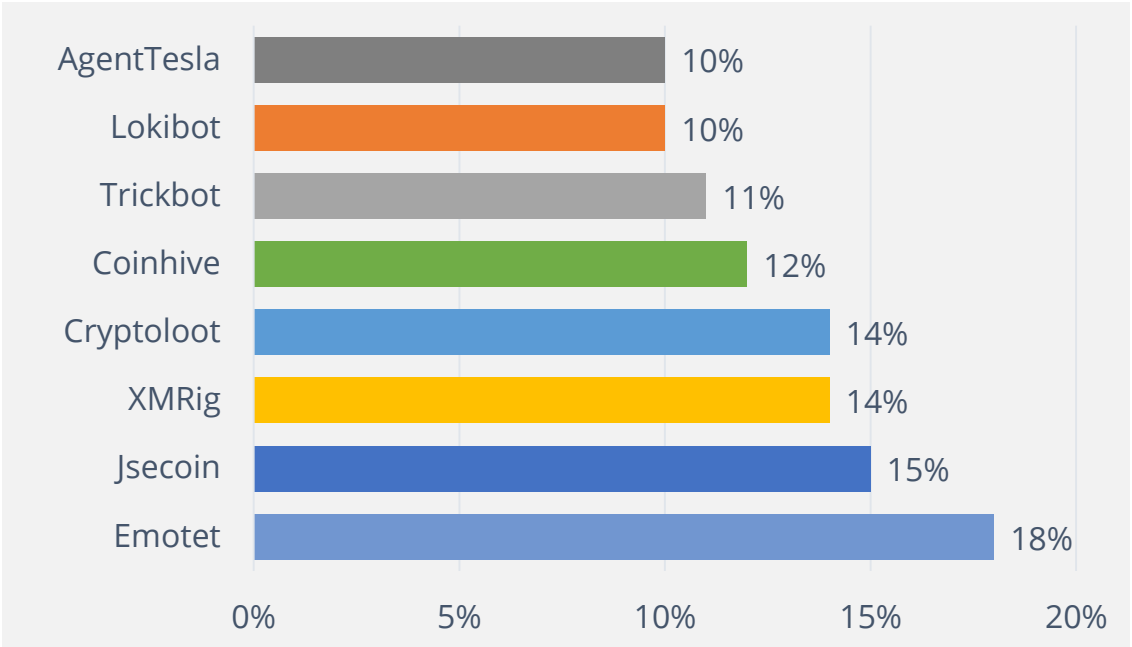
According to a security researcher[18], the key to successfully counteracting a fileless attack campaign is by dealing with each of the phases of the threat's life cycle with an integrated and multi-layered defence approach. In this approach, it is important to investigate the different stages of the attack and undertake the following activities:

- analyse and measure the actions performed by the attacker;
- identify the techniques used;
- monitor activities in PowerShell or other scripting engines;
- Access aggregated threat data;
- control the state of the targeted system;
- halt arbitrary processes;
- remediate processes that are part of the attack;
- isolate infected devices.



Botnet and Command and Control (C&C) landscape

Overall global botnet traffic increased by 71,5% since 2018[2]. The botnets most often observed were Emotet (41%), Trickbot (25%) and DanaBot (5%)[2]. A notable increase in botnet traffic was observed in Russia (143%), attributed mostly to relaxed registration procedures and less interest from law enforcement agencies.[14] During 2019, Russia hosted most botnet C2s, followed by the United States, the Netherlands, China and France. Domain name generation algorithms (DGAs) were used by cybercriminals to support many C2 communication. 50% of these registrations occurred in top-level domains (TLDs) '.com' and '.net'.[15] During the reporting period, such domain name registrations dropped by 71%, in favour of other communication protocols such as peer-to-peer (P2P).[13]



Malware types identified in 2019. Source: MalwareBytes[4]

How

According to a study from 2019, 94% of all malware types were delivered via e-mail.[24] Although this is counted as an entry point vector, it is interesting to note that, upon successful attack, the malware might download an additional payload that exhibits worm-like behaviour to allow laterally spread across the network (Emotet and Trickbot). Moreover, after the initial delivery of malware, in most cases (71%) it was spreading by employees' activity. Once again, new vulnerabilities in the remote desktop protocol (RDP) attracted attention, as they allow remote code execution (RCE) and are therefore wormable.[30] Although these newly discovered vulnerabilities have not been exploited on a large scale, it is expected that a new worm may target unpatched systems in the near future.[31]

Incidents

- **Airbus** suffered a data breach affecting employees in Europe.[34,35]
- Card skimming malware installed on the **American Medical Collection Agency's** web site resulted in the theft of 12 million patients' personal data.[36]
- Major provider of laboratory diagnostics **LifeLabs** fell victim to a ransomware attack, resulting in the theft of 15 million accounts containing the test results and health card numbers.[37,38]
- A ransomware attack on the **City of Pensacola, Florida** resulted in 2GB of data being made available online, possibly containing personally identifiable information (PII).[39]
- The personal data of 2.400 **Singapore armed forces staff** may have been leaked through e-mail phishing by malicious malware.[40]

Mitigation

Proposed actions

- Implement malware detection for all inbound/outbound channels, including email, network, web and application systems in all applicable platforms (i.e. servers, network infrastructure, personal computers and mobile devices).
- Inspect the SSL/TLS traffic allowing the firewall to decrypt what is being transmitted to and from websites, email communications, and mobile applications.
- Establish interfaces between malware detection functions (intelligence-led threat hunting) and security incident management to establish efficient response capabilities.
- Use the tools available for malware analysis for sharing malware information and malware mitigation (i.e. MISP).[32]
- Develop security policies that specify the processes to be followed in the event of infection.
- Understand the capabilities of various security tools and develop new security solutions. Identify gaps and apply the defence-in-depth principle.
- Employ mail filtering (or spam filtering) for malicious e-mails and remove executable attachments.
- Regularly monitor the results of antivirus tests.[30,42]
- Log monitoring using security incident and event management (SIEM) solution. Indicative log sources are anti-virus alerts, endpoint detection and response (EDR), proxy server logs, Windows Event and Sysmon[43] logs, intrusion detection system (IDS) logs[44], etc.
- Disable or reduce access to PowerShell functions.[45]

“The sophistication of threat capabilities increased in 2019, with many adversaries using exploits, credential stealing and multi-stage attacks.”

in ETL 2020

References

1. "What is Malware". Veracode. https://www.veracode.com/security/malware

2. "Cyber Security Report". 2019. Checkpoint. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

3. "Beapy: Cryptojacking Worm Hits Enterprises in China" April 24, 2019. Broadcom. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

4. "2020 State of Malware Report". February, 2020. Malware Bytes. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

5. "Evasive Threats,Pervasive Effects" 2019. Trend Micro, Research. https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

6. "SonicWall Cyber Threat Report". 2020. SonicWall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

7. "Emotet is back: botnet springs back to life with new spam campaign". September 16, 2019. Malwarebytes Labs. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

8. "Increased Emotet Malware Activity" January 22, 2020. US CERT. https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity

9. "SonicWall Security Metrics" SonicWall. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

10. "Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection". April 16, 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

11. "Internet organised crime threat assessment" 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

12. "Narrowed Sights, Bigger Payoffs: Ransomware in 2019" June 6, 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

13. "From Supply Chain to Email, Mobile and the Cloud" July 25, 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

14. "Mobile malware evolution 2019". February 25, 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

15. "Mobile banking malware surges in 2019". July 25, 2019. Computer Weekly. https://www.computerweekly.com/news/252467340/Mobile-banking-malware-surges-in-2019

16. "Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics". January 17, 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

17. "Spamhaus Botnet Threat Report 2019". January 28, 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

18. "What Is Fileless Malware?". McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

19. "What is fileless malware and how does it work?" . Norton. https://us.norton.com/internetsecurity-malware-what-is-fileless-malware.html

20. "Trend Micro Report Reveals 265% Growth In Fileless Events". August 28, 2019. Trend Micro. https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2019/2019-08-28.html

21. "Understanding Fileless Threats" July 29, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats

22. "SonicWall Sees Dramatic Jump In IoT Malware, Encrypted Threats, Web App Attacks Through Third Quarter". October 22, 2019. SonicWall. https://www.sonicwall.com/news/dramatic-jump-in-iot-malware-encrypted-threats-web-app-attacks-third-quarter/

23. "2020 Vulnerability and Threat Trends". 2020. SKYBOX. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020_VT_Trends-Report-reduced.pdf

24. "Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection". April 16, 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

25. "Internet organised crime threat assessment" 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

26. "Narrowed Sights, Bigger Payoffs: Ransomware in 2019" June 6, 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

27. "From Supply Chain to Email, Mobile and the Cloud" July 25, 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

28. "Mobile malware evolution 2019". February 25, 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

29. "Mobile banking malware surges in 2019". July 25, 2019. Computer Weekly. https://www.computerweekly.com/news/252467340/Mobile-banking-malware-surges-in-2019

30. "Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics". January 17, 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

31. "BlueKeep attacks are happening, but it's not a worm". November 3, 2019. ZDNet. https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/

32. MISP Projects. http://www.misp-project.org/

33. "PowerShell, fileless malware's great attack vector" . February 25, 2919. Panda. https://www.pandasecurity.com/mediacenter/malware/powershell-fileless-malware-attack-vector/

34. "Airbus Statement on Cyber Incident". January 30, 2019. Airbus. https://www.airbus.com/newsroom/press-releases/en/2019/01/airbus-statement-on-cyber-incident.html

35. "Airbus data breach impacts employees in Europe" January 30, 2019. ZDNet. https://www.zdnet.com/article/airbus-data-breach-impacts-employees-in-europe/

36. "Massive Quest Diagnostics data breach impacts 12 million patients". June 4, 2019. ZDNet. https://www.zdnet.com/article/massive-quest-diagnostics-data-breach-impacts-12-million-patients/

37. "Hackers crack 15M LifeLabs accounts, obtain lab results and health card numbers". December 17, 2019. Daily Hive. https://dailyhive.com/calgary/lifelabs-hacked-cyber-attack

38. "Why the LifeLabs Hack Likely Is Worse than Most". December 18, 2019. The Tyee. https://thetyee.ca/Analysis/2019/12/18/LifeLabs-Data-Hack/

39. "Personal Information in City of Pensacola Cyberattack". January 17, 2020. City of Pensacola. https://www.cityofpensacola.com/CivicSend/ViewMessage/Message/100944

40. "Personal data of 2,400 Mindef, SAF staff may have been leaked" December 22, 2019. The Straits Times - Singapore. https://www.straitstimes.com/singapore/personal-data-of-2400-mindef-saf-staff-may-have-been-leaked

References

41. AVTEST – The Independent IT-Security Institute**.** https://www.av-test.org/en/
42. "Real world protection tests." AV Comparatives. https://www.av-comparatives.org/dynamic-tests/
43. "The ThreatHunting Project." https://www.threathunting.net/data-index
44. Mark Russinovich, Thomas Garnier . "Sysmon v11.10." June 24, 2020. Microsoft. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

45. "Guide to Intrusion Detection and Prevention Systems (IDPS)." February 2007. CSRC. https://csrc.nist.gov/publications/detail/sp/800-94/final

46. "GOLDEN CHICKENS: Evolution of the MaaS". July 20, 2020. QuoIntelligence. https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/

47. "Most malware in Q1 2020 was delivered via encrypted HTTPS connections". June 25. 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

48. "Malware statistics and facts for 2020" July 29, 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/


“The threat landscape is becoming extremely difficult to map. Not only attackers are developing new techniques to evade security systems, but threats are growing in complexity and precision in targeted attacks.”
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

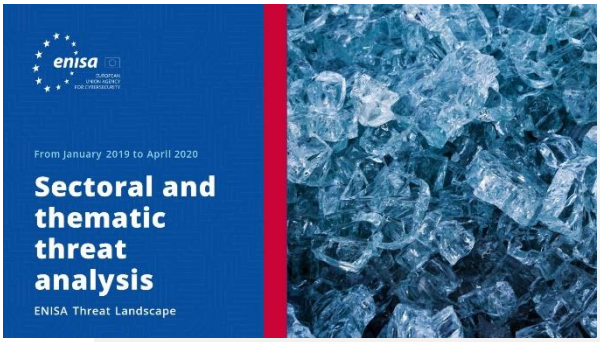
ENISA Threat Landscape Report
List of Top 15 Threats

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.

About

_ 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.

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

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu