enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Main incidents in the EU and worldwide

ENISA Threat Landscape

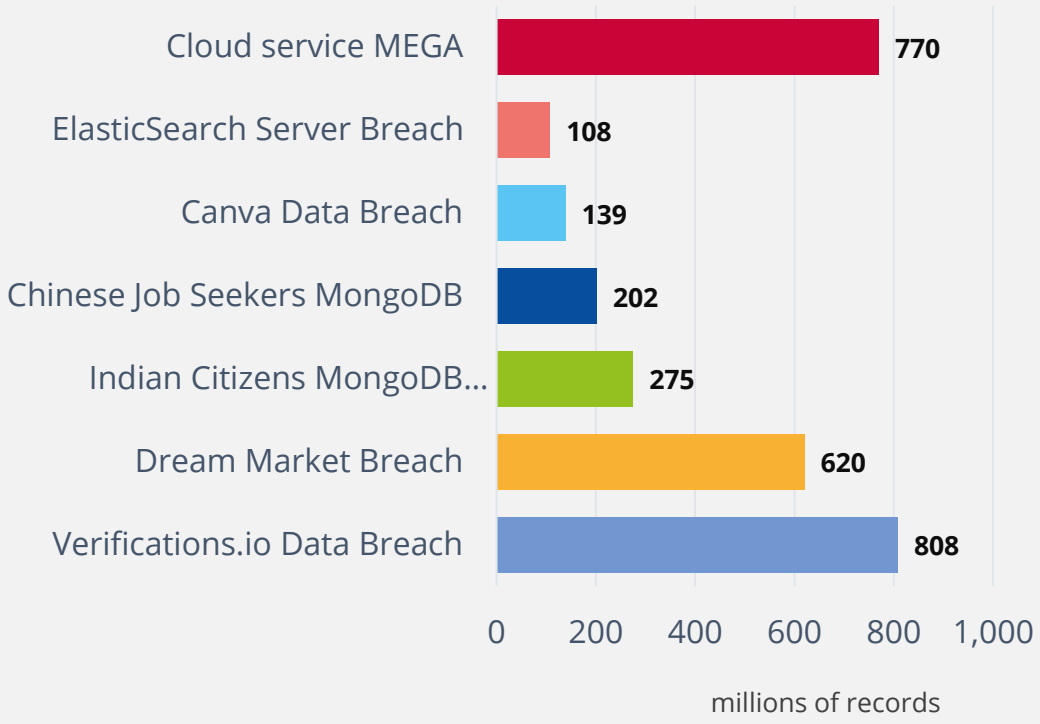
Overview

The sophistication of threat capabilities increased in 2019, with many adversaries using exploits, credential stealing, and multi-stage attacks. The number of data breach incidents is still very high, and the amount of stolen financial information and user credentials is growing. In some cases, the failure to patch a known vulnerability that has the potential to affect software or libraries in use - in a reasonable timeframe – may have serious repercussions.

During the past decade, **malware has made ENISA's list of top 15 threats, yet still many security systems are not able to detect this threat**. For many years, malware was spread mainly through malicious e-mail spam and more recently, using finely crafted phishing messages. Technology companies and e-mail providers alike invested in spam filters, improving the detection of malicious attachments. However, **adversaries are now innovating to increase their chances of reaching potential victims**. Many of these innovations have paid back to malicious actors during this period.

The COVID-19 pandemic has put healthcare organisations and professionals worldwide under pressure, and health has become one of the most critical sectors to protect against cyberattacks. The number of incidents involving ransomware targeting the healthcare sector was already high but increased during the pandemic.

Top data breaches incidents



Timeline

2019

_ January

MEGA cloud (NZ) suffered a data breach exposing 770 million emails and 21 million passwords.[1]

_ February

Verification.io (US) exposed ca. 800 million records.[2]

_ March

Norsk Hydro (NO) victim of a ransomware attack.[3]

_ August

Bulgarian (BG) Personal Tax Revenue office suffered a data breach exposing PII from all adult citizens.[8]

_ September

Mastercard (BE) suffered a data breach affecting ca. 90K customers in Europe.[9]

_ October

Websites and the national TV broadcaster in Georgia (GE) suffered a coordinated cyberattack.[30]

_ November

UniCredit (IT) victim of a data breach leaking 3M records.[10]

_ December

Prosegur (SP) suffered a ransomware attack disrupting its operation.[11]

2020

_ January

Austria's Foreign Ministry (AT) targeted by a cyberattack.[12]

_ April

Facebook (US) reported a data breach exposing 540 M user records on exposed servers.[4]

_ May

Thyssen-Krupp and Bayer (DE) targeted with espionage malware.[5]

_ July

City Power (ZA) victim of a ransomware attack disrupting the energy supply in Johannesburg.[7]

_ June

Five hospitals in Romania (RO) hit by Badrabbit ransomware.[6]

_ February

INA Group (HR) victim of ransomware attack.[13]

_ March

ENTSO-E (BE) network compromised, victim of an intrusion.[14]

_ April

Over 500K Zoom (US) accounts found for sale in the dark web.[31]

Most targeted sectors

In the line of fire

The sectors most targeted sectors during this period were digital services, government administration and the technology industry. Attacks on digital service providers often serve as proxies to reach other, more attractive targets. In contrast, attacks on the technology industry allowed malicious actors to compromise the supply chain or look for vulnerabilities to exploit.

The e-mail platform **verifications.io**[18], suffered a major data breach due to an unprotected MongoDB database. Data from over 800 million e-mails were exposed, containing sensitive information that included personally identifiable information (PII).

Over 770 million e-mail addresses and 21 million unique passwords were exposed in a popular hacking forum hosted by the cloud service **MEGA**[1]. It became the most significant collection of breached personal credentials in history, named 'Collection #1'.

The cloud and virtualisation provider **Citrix** was a victim of a targeted cyberattack. To gain access to Citrix's systems, the attackers exploited several critical software vulnerabilities such as CVE-2019-19781 and employed a technique called password spraying.

The cloud hosting provider **iNSYNQ**[19] experienced a ransomware attack that left customers unable to access their data for more than a week, forcing customers to rely on local backups.

_Most targeted sectors

Digital Services_ Services such as e-mail, social and collaborative platforms and cloud providers were under attack during 2019. These were also used as proxies for further attacks.

Government Administration_ The financial returns from ransoms paid makes the public sector one of the most attractive targets for ransomware attacks.

Technology Industry_ The technology industry was under attack in 2019 mainly through supply chain attacks trying to compromise the development of software through zero-day exploits and backdoors attacks.

Financial_ The number of incidents with financial organisations and not necessarily banks, increased substantially during the reporting period.

Healthcare_ The number of attacks against the healthcare sector continues to grow.

Trends

Across the board

- In 2019, intense **trojan-activity** was observed across the globe. Emotet and Agent Tesla were the most frequently and dangerous malwares[17].
- **Phishing** remained one of the most successful techniques for delivering malicious tools. Powerful phishing lures include phone scams, fake invoices, payments, quotations and purchase and sales orders.
- **Ransomware** continues to generate substantial financial rewards for malicious actors. A recent study identified human-operated ransomware campaigns[17], in which adversaries employ credential theft and lateral movement methods traditionally associated with targeted attacks such as those from nation-state actors.
- **Card-skimming** schemes have become a significant threat during 2019 and 2020 due to the increasing number of online shoppers.
- **Business e-mail compromise (BEC)** is a growing threat as a result of the vast amount of credentials and personal information stolen during the last decade.
- Companies experience an average of 12 **credential-stuffing** attacks each month, wherein the attacker is able to identify valid credentials.

Findings

84%_ of cyberattacks rely on social engineering

67%_ of malware was delivered via encrypted HTTPS connections[34]

230.000_ new strains of malware every day

6_ months in average is what it takes to detect a data breach

71%_ of organizations experienced malware activity that spread from one employee to another[35]

Actors

_Who

Knowing who is responsible or attributing responsibilities to a person or a group for a cybersecurity incident is still a very daunting task and often a worthless exercise. Yet, from a threat intelligence perspective, it is essential to classify behaviours, understand the dynamics and *modus operandi* used by certain adversaries. This analysis often helps defenders to look for specific tracks and try to anticipate the next adversarial action.

The **Lazarus Group** for example, an allegedly state-sponsored advanced persistent threat (APT) group, was reportedly more active during the reporting period in both financially and espionage motivated attacks. The group has been associated with several incidents, including the **AppleJeus campaign** targeting cryptocurrency trading platform users and their systems.[22] Major incidents attributed to this group include:

- hacking an Indian nuclear power plant and space research organisation in November 2019;
- compromising a cryptocurrency trading app targeting exchange administrators in October 2019;
- attacking automated teller machines (ATMs) and banks in India, identified in September 2019;
- targeting Android users in South Korea through trojanised apps in the Google Play Store identified in August 2019.

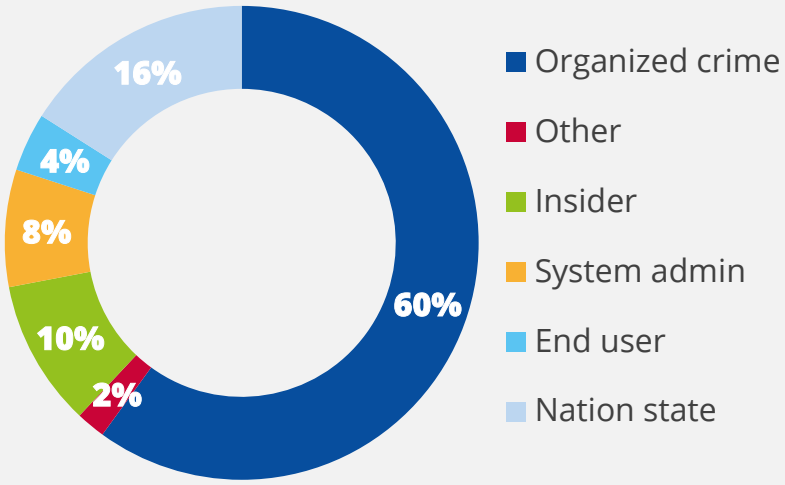
Most active actors

TURLA_ The group was reported to have targeted Microsoft Exchange e-mail servers in the education, government, military, research, and pharmaceutical sectors in more than 40 countries in 2019.[23]

APT27_ The group was reported to have compromised government organisations' SharePoint servers in two different countries in the Middle East.

VICIOUS PANDA_ In April 2020, the Mongolian Public Administration was allegedly targeted by the group.[24]

GAMAREDON_ The group, reportedly targeted the Ministry of Defence of Ukraine in a spear-phishing campaign from December 2019.[25]



Motivations

_Why

While it is challenging to determine the primary motivation behind a cyberattack, we can still categorise them based on the outcome of the incident.

Financial: The number of incidents resulting in the theft of information, data and user credentials is the highest observed during the reporting period. In most cases, the intention is to steal data/information and sell it on the dark web. Other uses of this information/data to enable other types of attacks with a completely different outcome such as espionage or financial fraud, can also be identified. More than 620 million account details were stolen from 16 hacked websites and offered for sale on the popular dark-web marketplace Dream Market.

Espionage: This is a motive behind an increasing number of reported attacks, mainly due to ongoing geopolitical and commercial tensions. The number of incidents is not substantial, but their size and magnitude put it second in ENISA's list of top 5 motivations. Some noteworthy incidents include that reported in April 2019, in which a General Electric's employee and a Chinese businessperson were charged by the United States Department of Justice with economic espionage and theft of General Electric's trade secrets.[20] AgenceFrance Presse (AFP) reported that Airbus had fallen victim to a sophisticated cyber-espionage campaign. Attackers reportedly breached the IT systems of several of Airbus's suppliers and, from there, penetrated the company's IT systems.[21]

Top five motivations: financial, espionage, disruption, political and retaliation.

Top motivations

The figure below shows that **Financial** is still the primary motive for the majority of cyberattacks. In some cases, multiple motivations can be identified within a single attack. For example, espionage, political, financial and disruption are often combined motives. Many incidents originate from automated systems and are delivered 'as-a-service', paid in cryptocurrency. These services include distribution of ransomware, command and control (C2), distributed denial of service (DDoS), spam and other illicit activities.

Attack vectors

How

Cyberattacks take on average three steps to reach a victim's valuable assets. When reviewing the most frequently used attack vectors, we must prioritise the entry point, course of action and action on assets. These are the most critical stages that should constitute distinct approaches in a defence strategy.

Entry point: During 2019, the techniques used most frequently to start a cyberattack include brute force with stolen credentials, social engineering, configuration errors and exploitation of web applications. The exploitation of web applications, for example, was often used as an entry point because of the growing uptake of this type of application to transfer data to the cloud. Errors in cloud configuration and misuse of systems were essential entry point in a large number of incidents. The use of social engineering to plan an attack leverages from tools such as phishing and business e-mail compromise (BEC)[16]. Other techniques less frequently but equally important are the exploitation of vulnerabilities (from unpatched systems and zero-days) and software backdoors, often used in more complex and sophisticated attacks.

Course of action: Installing malware is the technique most widely used during the 'course of action' stage. Once installed, it helps the adversary to do reconnaissance, move around the victim's systems and networks, install additional tools such as ransomware, steal data and communicate with a C2 server.

_Five most desired assets by cybercriminals

01_Industrial property and trade secrets

Industrial property and trade secrets are the most desirable assets because of their high value to their owners, the market and some cases the criminal world.

02_State/military classified information

This asset includes any information that a state deems sensitive. In 2019, the trade and diplomatic tensions between countries made this type of information even more attractive.

03_Server infrastructure

Server infrastructure is the first sensitive asset that is not data. In many attacks, taking over the victim's server infrastructure, is the primary objective.

04_Authentication data

Authentication data is valuable assets for generating profits but also as an objective to support an attack.

05_Financial data

Financial data such as credit card, banking and payment information is always value to cybercriminals.

Strategic intelligence

What changed in the landscape with the covid-19 pandemic?

In 2019, ENISA continued mapping the threat landscape, helping decision-makers and policymakers define strategies to defend citizens, organisations and cyberspace. This work is part of ENISA's strategy to provide strategic intelligence to its stakeholders. The central theme in 2019 was the next generation of mobile telecommunications, or 5G, following a request from the European Commission and Member States. **The agency will continue to produce these thematic threat landscapes and in 2020**, the focus is on artificial intelligence.

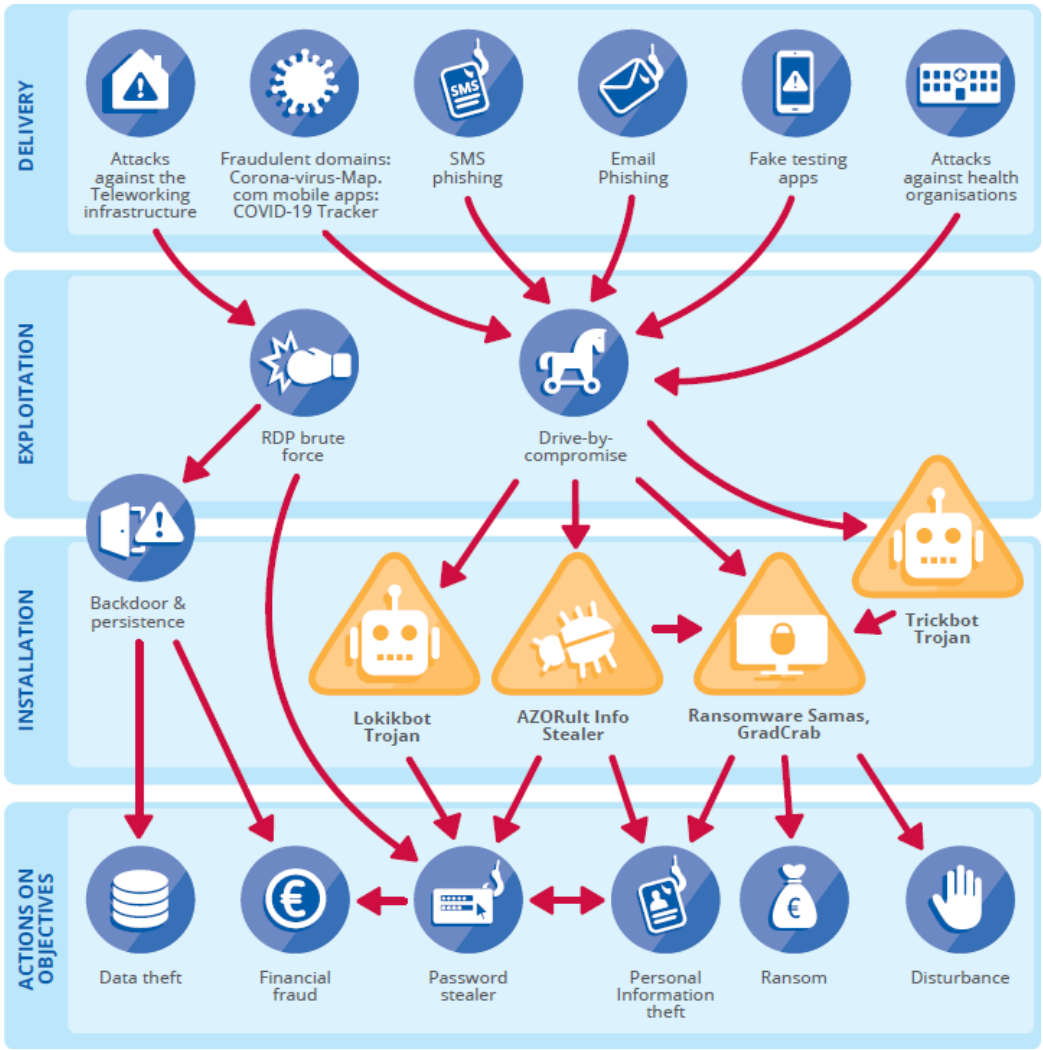
The COVID-19 pandemic has been a prolific period for malicious actors conducting attacks targeting sensitive areas such as healthcare service providers and people working from home. ENISA is mapping the threat landscape experienced during the pandemic and advising on mitigation measures that will attempt to reduce the exposure to threats.

ENISA shares its cybersecurity recommendations on the COVID-19 pandemic on a variety of topics including working remotely, online shopping and e-health, and it provides valuable up to date security advice to the sectors affected.[32]

The **Brno University Hospital** in the Czech Republic suffered a cyberattack[33] in the midst of the COVID-19 pandemic, which forced it to reroute patients and postpone surgery. The incident is considered critical since this Hospital is one of the Czech Republic's biggest COVID-19 testing laboratories.

_COVID-19 threat landscape

ENISA prepared many resources for an awareness-raising campaign and shared other internal and external resources dedicated to cybersecurity experts, covering security issues associated with challenges faced during the COVID-19 pandemic. One of these resources was an analysis of the most critical threats during this period.



References

1. "MEGA Data Breach Exposed 773 Million Email Addresses and Passwords." January 19, 2019. Latest Hacking News. https://latesthackingnews.com/2019/01/19/mega-data-breach-exposed-773-million-email-addresses-and-passwords/

2. "Largest Leak in History: Email Data Breach Exposes Over Two Billion Personal Records." April 8, 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/largest-leak-in-history-email-data-breach-exposes-over-two-billion-personal-records/

3. "LockerGoga Ransomware Disrupts Operations at Norwegian Aluminum Company." March 20, 2019. Recorded Future. https://www.recordedfuture.com/lockergoga-ransomware-insight/

4. "Researchers find 540 million Facebook user records on exposed servers." April 3, 2019. Tech Crunch. https://techcrunch.com/2019/04/03/facebook-records-exposed-server/

5. "Winnti: Attacking the Heart of the German Industry" July 24, 2019. Web.br. https://web.br.de/interaktiv/winnti/english/

6. "Cyber-attacks against 5 hospitals in Romania. CCR's website, also hacked" June 20, 2019. Romanian Journal. https://www.romaniajournal.ro/society-people/cyber-attacks-five-hospitals-romania-ccr-website-hacked/

7. "Here's how ransomware attacks like the one on CityPower work – and why some victims end up paying criminals millions" July 25, 2019. Business Insider South Africa. https://www.businessinsider.co.za/ransomware-attack-on-citypower-johannesburg-why-victims-pay-criminals-2019-7

8. "Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged." August 30, 2019. Bank Info Security. https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged-a-13000

9. "Breach Of Mastercard Loyalty Program Affected 90K Germans' Data" August 23, 2019.PYMNTS.com. https://www.pymnts.com/news/security-and-risk/2019/mastercard-loyalty-program-data-breach-germany/

10. "UniCredit confirms data breach" October 28, 2019. PrivSec Report. https://gdpr.report/news/2019/10/28/privacy-unicredit-confirms-data-breach/

11. "Prosegur Hacked: Spanish SOC Provider Hit by Ryuk Ransomware" November 28, 2019. Computer Business Review. https://www.cbronline.com/news/prosegur-hacked-ransomware

12. "Serious cyber-attack' on Austria's foreign ministry" January 5, 2020. BBC. https://www.bbc.com/news/world-europe-50997773

13. "Croatia's largest petrol station chain impacted by cyber-attack" February 20, 2020. ZDNet. https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/

14. "European power grid organization says its IT network was hacked" March 9, 2020. Cyberscoop. https://www.cyberscoop.com/european-entso-breach-fingrid/

15. "Fullz House hackers pivot from phishing to Magecart card skimming attacks" November 26, 2019. ZDNet. https://www.zdnet.com/article/fullz-house-threat-group-pivots-from-phishing-to-magecart-card-skimming-attacks/

16. "FBI warns of cloud based BEC attacks." April 8, 2020. Info Security. https://www.infosecurity-magazine.com/news/fbi-warns-of-cloudbased-bec-attacks/

17 "Microsoft Alerts Healthcare to Human-Operated Ransomware" April 1, 2020. Dark Reading. https://www.darkreading.com/vulnerabilities---threats/microsoft-alerts-healthcare-to-human-operated-ransomware/d/d-id/1337463

18. "Verification.io suffers major data breach." March 15, 2019. PrivSec Report. https://gdpr.report/news/2019/03/15/verification-io-suffers-major-data-breach/

19. "Inside the Insynq attack: 'We had to assume they were listening'" August 8, 2019. Accounting Today. https://www.accountingtoday.com/news/inside-the-insynq-ransomware-attack-we-had-to-assume-they-were-listening

20. "Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets". April 23, 2019.USA DoJ. https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

21. "Airbus supply chain hacked in a cyberespionage campaign" September 27, 2019. CERT-EU. https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190927-2.pdf

22. "Lazarus group's 'AppleJeus' sequel targets cryptocurrency traders" January 10, 2020. The Cyber-Security Source. https://www.scmagazineuk.com/lazarus-groups-applejeus-sequel-targets-cryptocurrency-traders/article/1670446

23 "Russian Nation-State Group Employs Custom Backdoor for Microsoft Exchange Server" July 7, 2019. Dark Reading. https://www.darkreading.com/application-security/russian-nation-state-group-employs-custom-backdoor-for-microsoft-exchange-server/d/d-id/1334628

24. "Vicious Panda: The COVID Campaign" March 12, 2020. Check Point Research. https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

25. "Gamaredon APT Improves Toolset to Target Ukraine Government , Military" February 5, 2020. Threat Post. https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/

26. "Virus attacks Spain's defense intranet, foreign state suspected: paper" March 26, 2019. Reuters. https://www.reuters.com/article/us-spain-security-cyberattack/virus-attacks-spains-defense-intranet-foreign-state-suspected-paper-idUSKCN1R7115

27 "115 Million Pakistani Mobile Users Data Go on Sale on Dark Web" April 10, 2020. Rewterz. https://www.rewterz.com/articles/115-million-pakistani-mobile-users-data-go-on-sale-on-dark-web

28. "Your business hit by a data breach? Expect a bill of $3.92 million" July 23, 2019. ZDNet. https://www.zdnet.com/article/your-business-hit-by-a-data-breach-expect-a-bill-of-3-92-million/

29. "Cyber Security Statistics for 2019" March 21, 2019. Cyber Defense. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

30. "Georgia 'I'll Be Back' Cyber Attack Terminates TV, Takes Down 15,000 Websites." October 29, 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/10/29/georgia-ill-be-back-cyber-attack-terminates-tv-takes-down-15000-websites/#1a5746347a48

31. "Half a million Zoom accounts for sale on the dark web." April 16, 2020. WeLiveSecurity by ESET. https://www.welivesecurity.com/2020/04/16/half-million-zoom-accounts-sale-dark-web/

32. "ENISA COVID-19 Resources". ENISA. https://www.enisa.europa.eu/topics/wfh-covid19

33. "Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak" March 17, 2020. Security Magazine. https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak

34. "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/

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

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

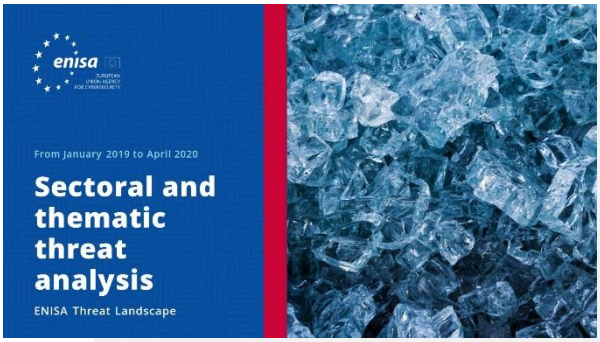
ENISA Threat Landscape Report
List of Top 15 Threats

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.

Other publications

Roadmap on the Cooperation Between CSIRTS and LE

A roadmap on the cooperation across CSIRTs in particular with national and governmental - law enforcement (LE) and the Judiciary.

READ THE REPORT

EU MS Incident Response Development Status Report

A study aiming at the analyses of the current operational Incident Response set-up within NISD sectors and identify the recent changes.

READ THE REPORT

ENSIA CSIRT maturity assessment model

An updated version of the "Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity" published by ENISA in 2017

READ THE REPORT

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

in ETL 2020

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

https://www.enisa.europa.eu