enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

EN

From January 2019 to April 2020

Emerging trends

ENISA Threat Landscape

Overview

What to expect

With the start of a new decade, we can expect significant changes in the way we perceive and understand cybersecurity or the security of cyberspace. Cyberspace as defined in **ISO/IEC 27032:2012**[1] is a ***"complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form"***. The protection of this complex environment will become even more challenging as we connect more people, devices, systems and run more processes and services in the network. We are also more dependent from its reliability, integrity, availability and trustworthiness to work, relate and do many of our day-to-day activities. With this growing dependency, more opportunities will arise for malicious actors to use cyberspace to manipulate, intimidate, deceive, harass and defraud individuals and organisations. The protection of individuals, business and organisations while using cyberspace will tend to shift during the next decade, from the traditional network and information security (NIS) to a wider concept including content and services.

During the last decade the 'fourth industrial revolution' has significantly accelerated the pace of change, transforming what people do, how they do it, what skills are required, where work is performed, how work relations are structured, and how work is organised, distributed and rewarded.

Because of the current COVID-19 pandemic, we initiate the decade with a new norm and profound changes in the physical world and cyberspace. With social distancing or confinement, people will tend to use the virtual space to communicate, relate and socialize. This new norm will introduce new challenges across the digital value-chain and in particularly, the cybersecurity industry.

During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface.

There are too many variables to consider when making cyber risk management effective. An important factor is the technological diversity most organisations experience today. Another aspect is the sophistication of tools, tactics techniques and procedures (TTPs) used by adversaries to conduct attacks. Malicious actors are adapting and adjusting the TTPs to their victim's environment as needed and collaborating with others to reach their goals.

Defining a risk posture, managing data, applying relevant metrics, and responding to change are obstacles to creating an effective cyber risk governance strategy. **New approaches will be required during the next decade to stay away from silo analysis and move closer to a matrix-type of interconnected factors, variables and conditions**. This constitutes a significant challenge for many organisations trying to protect their infrastructure, operations and data against stronger, better resourced and equipped adversaries.

Emerging trends

_Ten cybersecurity challenges

01_Dealing with systemic and complex risks.

Cyber risk is characterised by the speed and scale of its propagation as well as the potential intent of threat actors. The interconnectedness of various systems and networks enables cyber incidents to spread quickly and widely, making cyber risks harder to assess and mitigate.

02_Widespread of adversarial AI detection.

The detection of threats exploiting AI to launch an attack or avoid detection will constitute a major challenge for the future of cyber defence systems.[14]

03_Reduction of unintentional errors.

With the growing number of systems and devices connected to the network, unintentional errors continues to be one of the most exploited vulnerability in cybersecurity incidents. New solutions aiming at the reduction of these errors will provide an important contribution to reducing the number of incidents.

04_Supply chain and third party threats.

The diversified supply chain that characterizes the technology industry today provides new opportunities for threat actors to take advantage of these complex systems and exploit the multiple vulnerabilities introduced by a heterogeneous ecosystem of third party providers.[16]

05_Security orchestration and automation.

Cyber threat intelligence and behavioural analytics will gain importance with the automation of processes and analysis. Investing in automation and orchestration will allow cybersecurity professionals to invest in the design of more robust cybersecurity strategies.

06_ Reduction of false positives. This long waited promise is key in the future of the cybersecurity industry and in the fight against the alarm fatigue.

07_ Zero-trust security strategies. With an increasing pressure on IT systems from new business requirements such as remote working, digitalization of the business model and data sprawl, zero trust is seen by many decision makers as the solution de facto to secure corporate assets.

08_ Enterprise cloud migration errors. With many businesses migrating their data to cloud-based solutions, the number of configuration errors will increase exposing data to a potential breach. Cloud service providers will address the issue by implementing systems that identify these type of errors automatically.

09_ Hybrid threats. New *modus operandi* adopt virtual and physical world threats. The spread of disinformation or fake news for example, is a key fixture of the hybrid threat landscape. The EUvsDisinfo[15] is a flagship project of the European External Action Service's East StratCom Task Force established to address the disinformation threat.

10_ The attractiveness of the cloud infrastructure as a target will grow. The increasing reliance on public cloud infrastructure will surge the risk of outages. Misconfiguration of cloud resources is still the number one cause for cloud attacks, but attacks aiming directly at the cloud services providers gaining popularity among hackers.

Emerging trends

Cybersecurity spending

According to Gartner[17], many boards of directors will demand improved data and understanding of the returns after years of intensive investment in cybersecurity. This is mainly due to a growing spend in cybersecurity proportionately to the investment made in new technologies. According to a report from IDC[22], spending on cybersecurity reached $103 billion (ca. €87,5 billion) in 2019, which is 9.4% higher than the previous year. Security managers will soon be scrutinised for the results obtained from years of investment and are essential to maintain improved data about the results obtained.

Cyber threat intelligence will help defining cybersecurity strategies

Cyber threat intelligence (CTI)[7] aims at helping organisations becoming better prepared by improving their knowledge about the threat landscape. Instead of relying exclusively on information generated by internal systems or feeds (what is known about the known), the effectiveness of CTI will be determined by the knowledge about the *why*, the *how* and the *what* that is unknown to the cybersecurity team. The value proposition of any CTI capability or program is to improve the preparedness of the organisation to protect its critical assets from unknown threats.

Knowing the threat landscape

With more cybersecurity automation and orchestration seen as a growing trend, **cybersecurity teams will spend less time in monitoring activities and more in readiness and preparedness tasks**. A well-designed CTI capability can provide contextualised and actionable knowledge about threats to inform strategic, operational and tactical stakeholders across the organisation. In practical terms, a CTI capability should aim at responding to the following questions considering the stakeholders' requirements and the organisation's context and environment:

- What is the attack surface?
- What are the most valuable assets and the cyber terrain?
- What are the most critical vulnerabilities?
- What are the most used attack vectors?
- How adversaries typically behave and operate?
- How does the threat landscape looks like for:
    - the sector and type of business the organisation operates?
    - the technological environment adopted by the organisation?
- Who and what needs to be done to mitigate risks from these threats?

Shortage in cybersecurity skills

The lack of highly-skilled tech professionals is already issue for Europe's digitalisation ambition. According to a study[23], over 70% of European firms report that lack of skills is hampering their investment strategies, while 46% of firms report difficulties in filling vacancies due to skills shortages in key areas such cybersecurity.

Emerging trends

_ *Five* trends with cyber threats

01_Malware is getting an upgrade. Malware family strains are being upgraded into new versions with additional features, distribution and propagation mechanisms. Emotet for example, a malware originally designed as a banking Trojan back in 2014, has become one of the most effective malware distributors of 2019.[2]

02_Threats will become fully mobile. Users are increasingly dependent on mobile devices to secure their most sensitive accounts. The use of 2fa tied to an app authenticator or via a text message is one of the examples. With more malware going fully mobile, fraudulent apps, SIMJacking and operating systems exploits make these devices the weakest link and therefore, extremely vulnerable to attacks.

03_Attackers are using new file types such as disc image files (ISO and IMG) for spreading malware. DOC, PDF, ZIP and XLS files are still the most commonly used attachment type for spreading malware but other types are getting popular. A few campaigns distributing AgentTesla InfoStealer and NanoCore RAT were found using image file type in 2019.

04_Increase in targeted and coordinated ransomware attacks. In 2019, we saw an escalation of sophisticated and targeted ransomware exploits with the public sector, health care organisations and specific industries at the top of the list. Attackers are spending more time gathering intelligence about their victims, knowing exactly what to encrypt, achieving maximum disruption and higher ransoms.

05_Credential-stuffing attacks will widespread.
Credential stuffing - the automated injection of stolen username and password combinations through large-scale automated login requests directed against a web application - will proliferate as a result from a decade of an abnormal number of data breaches and trillions of personal data records stolen.


“During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface.”
in ETL 2020

Emerging trends

_Ten emerging trends in attack vectors

01_ Attacks will be massively distributed with a short duration and a wider impact

These attacks are meant to affect the highest number of devices possible to steal personal information or block the access to data by encrypting the files.

02_ Finely targeted and persistent attacks will be meticulously planned with well-defined and long-term objectives

Malicious actors plan this type of attacks to reach high value data such as financial information, intellectual and industrial property, trade secrets, classified information, etc.

03_ Malicious actors will use digital platforms in targeted attacks

Malicious actors will explore the potential of digital platforms to support targeted attacks (e.g. social media, gaming, messaging, streaming, etc.). From personal data theft for spear-phishing attacks to broad malware distribution, digital platforms with a high number of subscribers are efficient attack vectors increasingly popular among malicious actors.

04_ The exploitation of business processes will increase

With more automation and less human intervention, business processes can be maliciously altered to generate profit for an attacker. Commonly known as Business Process Compromise (BPC) this technique is often undervalued by process engineering specialists due to the lack of a proper risk assessment.

05_ The attack surface will continue expanding

E-mail is no longer the prime and only tool and top attack vector for phishing. Malicious actors are now using other platforms to communicate and attract victims to open compromised web pages. A new trend is emerging with the use of SMS, WhatsApp, SnapChat and social media messengers.

06_ Teleworking will be exploited through home devices

With more people in teleworking and connecting their devices to corporate networks, the risk of opening new entry points for attackers will increase. With the COVID-19 pandemic, this trend will urge IT Managers to tighten security policies and make urgent changes in the IT infrastructure.

07_ Attackers will come better prepared

Attackers choose their targets carefully, perform reconnaissance against specific employees, and target those with spear-phishing attacks to obtain usable credentials to target the organisation. Once the attackers gain access to a single machine, they may employ penetration-testing tools such as Mimikatz to gather and exploit credentials with elevated privileges.

08_ Obfuscation techniques will sophisticate

Threat actors are continuously innovating to make threats more effective and less susceptible to detections. The Anibus, an Android banking Trojan and bot, has been distributed by masquerading as innocuous app, primarily through Google Play Store.[1]

09_ The automated exploitation of unpatched systems and discontinued applications will increase

The abnormal increase in Telnet traffic to port 445 observed in 2019 unveiled the expansion of worms and exploits such as Eternal Blue. Telnet, which is no longer used except in the realm of IoT devices, saw the greatest volumes during the period.

10_ Cyber threats are moving to the edge

Edge devices are deployed at the boundaries between interconnected networks. We have seen a growing trend with attacks targeting these devices — such as routers, switches, and firewalls — having a significant impact to an enterprise and to the connected digital ecosystem.

References

1. "ISO/IEC 27032:2012". ISO. https://www.iso.org/standard/44375.html

2. "Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk." April 2, 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

3. "Understanding the relationship between Emotet, Ryuk and TrickBot." April 14, 2019. Intel471. https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

4. "Investigating WMI Attacks" February 9, 2019. SANS. https://www.sans.org/blog/investigating-wmi-attacks/

5. "RDP Abuse and Swiss Army Knife Tool Used to Pillage, Encrypt and Manipulate Data" December 18, 2019. Bitdefender. https://labs.bitdefender.com/2019/12/rdp-abuse-and-swiss-army-knife-tool-used-to-pillage-encrypt-and-manipulate-data/

6. "Europe's huge privacy fines against Marriott and British Airways are a warning for Google and Facebook" July 10, 2019. CNBC. https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html

7. "This is how we might finally replace passwords" May 27, 2019. C|Net. https://www.cnet.com/news/this-is-how-we-might-finally-replace-passwords/

9. "Authentication standards to help reduce the world's over-reliance on passwords." FIDO. https://fidoalliance.org/overview/

10. "How Much Cyber Sovereignty is Too Much Cyber Sovereignty?" October 3, 2019. Council on Foreign Relations. https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

11. "Conceptualising Cyber Arms Races". 2016. NATO. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

12. "Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training" 2018. UNESCO. https://en.unesco.org/fightfakenews

13. "The Big Connect: How Data Science is Helping Cybersecurity". June 12, 2019. Info Security Group. https://www.infosecurity-magazine.com/blogs/data-science-helping-cybersecurity-1/

14. "Are You Ready For The Age Of Adversarial AI? Attackers Can Leverage Artificial Intelligence Too". January 9, 2020. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/01/09/are-you-ready-for-the-age-of-adversarial-ai-attackers-can-leverage-artificial-intelligence-too/#2a76dee14703

15. https://euvsdisinfo.eu/

16. "FBI Alerts Companies of Cyber Attacks Aimed at Supply Chains". February 21, 2020. Bitsight. https://www.bitsight.com/blog/fbi-alerts-companies-of-cyber-attacks-supply-chains

17. "Gartner Identifies the Top Seven Security and Risk Management Trends for 2019". March 5, 2019. Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma

18. "Android banking trojan." October 3, 2019.Cyare. https://cyware.com/news/exploring-the-nature-and-capabilities-of-anubis-android-banking-trojan-6ea7dec4

19. "5 Top Trends for Mobile Cyber Security in 2020". January 9, 2020. Corrata. https://corrata.com/5-top-trends-for-mobile-cyber-security-in-2020/

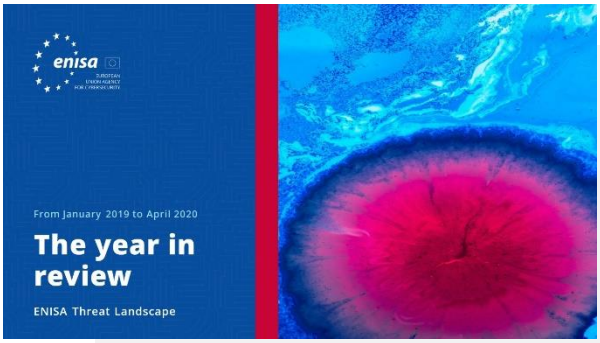
20. "Malicious Attachments Remain a Cybercriminal Threat Vector Favorite". August 27, 2020. Threat Post. https://threatpost.com/malicious-attachments-remain-a-cybercriminal-threat-vector-favorite/158631/

21. "10 trends shaping the future of work". October 2019. EPSC. https://op.europa.eu/en/publication-detail/-/publication/e77a1580-0cf5-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-121729338

22. "Global security spending to top $103 billion in 2019, says IDC", March 20, 2019. ZDNet. https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

23. **"**Insights into skills shortages and skills mismatch. learning from Cedefop's European skills and jobs survey". 2018. CEDEFOP. https://www.cedefop.europa.eu/files/3075_en.pdf

Related



READ THE REPORT

ENISA Threat Landscape Report
The year in review

A summary of the main cybersecurity trends for the year.

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

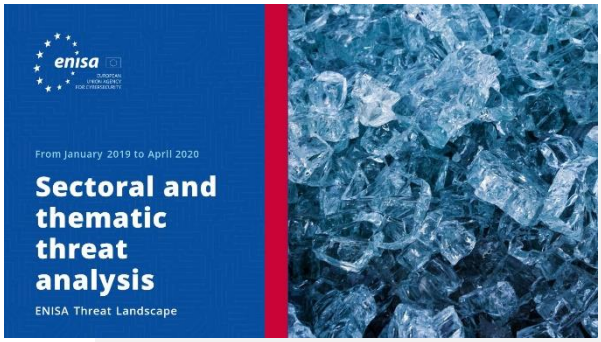
ENISA Threat Landscape Report
Research topics

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

READ THE REPORT

ENISA Threat Landscape Report
Main incidents in the EU and worldwide

Main cybersecurity incidents happening between January 2019 and April 2020.



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
Cyber Threat Intelligence overview

The current state of play of cyber threat intelligence in the EU.

Other publications

Advancing Software Security in the EU

Presents key elements of software security and provides a concise overview of the most relevant existing approaches and standards in the secure software development landscape.

READ THE REPORT

ENISA good practices for security of Smart Cars

Good practices for security of smart cars, namely connected and (semi-) autonomous vehicles to enhance car users' experience and improve car safety

.

READ THE REPORT

Good Practices for Security of IoT - Secure Software Development Lifecycle

ioT security with a particular focus on software development guidelines.

READ THE REPORT


“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

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