EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

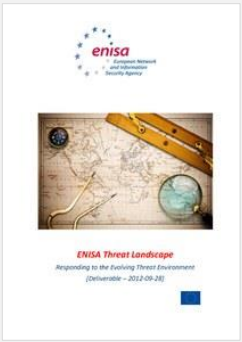
The year in review

ENISA Threat Landscape

Before we start

_ 8 years reviewing the threat landscape

This year, the **European Union Agency for Cybersecurity (ENISA)** celebrates one year of the new Cybersecurity Act and the eighth edition of the Threat Landscape Report (ETL). The Cybersecurity Act[1] revamps and strengthens ENISA's role by granting it a permanent mandate, more resources and new tasks. Furthermore, the agency is starting a new chapter with a new executive director, a new strategy and a new organisational structure. With all these changes taking place, it is time for the ETL to change too and to adopt a new structure and a modern look and feel, moving away from a lengthy and static type of report. With its new visual identity and format, the ETL report has become a versatile, dynamic and easy-to-use digital report, attempting to meet the expectations of a growing and demanding audience.



ETL 2012

ETL 2020

ENISA threat landscape journey from 2012 to 2020

_ ETL format

This edition reviews the threat landscape for the period between January 2019 and April 2020 and is structured in the following way.

THE YEAR IN REVIEW. This report provides a general overview of the threat landscape, outlining the most important topics referenced across all the other reports. It also provides ENISA's list of the top 15 threats, conclusions and recommendations.

CYBER THREAT INTELLIGENCE OVERVIEW. This report summarises the most important topics relevant to the cyber threat intelligence (CTI) community and those ones discussed in various forums.

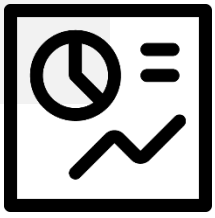
SECTORAL AND THEMATIC THREAT ANALYSIS. This report summarises the latest work produced by ENISA describing the threat landscape for specific sectors and technologies. This year we present the findings from the work done for 5G, the Internet of things (IoT) and smart cars.

MAIN INCIDENTS IN THE EU AND WORLDWIDE. This report provides an overview of major cybersecurity incidents happening in the EU and worldwide, highlighting the lessons we can learn from them.

RESEARCH TOPICS. This report presents key aspects related with the research and innovation in cybersecurity.

EMERGING TRENDS. This report identifies emerging trends and focuses on the challenges and opportunities for the future in the cybersecurity domain.

LIST OF TOP 15 THREATS. One report for each threat, presenting a general overview, the findings, major incidents, statistics, attack vectors and corresponding mitigation measures.



Before we start

Methodology

The content produced for the ETL report is based on information available from open-sources, mainly of a strategic nature, and covers more than one sector, technology and context. The report attempts to be industry and vendor agnostic and references or cites the work from various security researches, security blogs and news media articles, clearly identified throughout the text in multiple endnotes.

For the production of ENISA Threat Landscape Report, we followed a two-pronged approach. First, we conducted in-depth desk research of available literature from open sources such as news media articles, expert opinion, intelligence reports, incident analysis and security research reports. Second, we conducted interviews with members of the ETL stakeholders group who are experts in the field and members of the EU Cyber Threat Intelligence Community. The latter helped us defining the top 15 threats list and validating the assumptions over the trends and future challenges in cybersecurity.

We also thank the members of the CTI Stakeholders Group for all the support provided for the production of the reports during these eight editions. The members of this group review and validate the analysis produced for each ETL Report and vote on the annual list of top 15 cyber threats.

We would like to get your feedback on this report!
Please take a moment to fill in the questionnaire. To access the form, please click here.

Who should read what

The ETL report is part strategic and part technical, with information relevant to both technical and non-technical readers. The ETL targets different audiences and adopts different levels of technical language, depending on the domain and the importance of the topic for non-technical readers. The following table describes the type of audience and content for each ETL report.

ETL REPORT	TYPE OF CONTENT	TARGETED AUDIENCE
THE YEAR IN REVIEW	Generic	All
CTI OVERVIEW ↗	Specific	CTI community members and practitioners.
SECTORAL AND THEMATIC THREAT ANALYSIS ↗	Strategic	Strategic management experts, policymakers and decision-makers, risk analysts, cybersecurity managers and leaders.
MAIN INCIDENTS IN THE EU AND WORLDWIDE ↗	Strategic	Strategic management experts, policymakers and decision-makers, risk analysts, risk managers and leaders.
RESEARCH TOPICS ↗	Strategic	Strategic management experts, policymakers and decision-makers, risk analysts, risk managers and leaders.
EMERGING TRENDS ↗	Strategic	Strategic management experts, policymakers and decision-makers, risk analysts, risk managers and leaders.
LIST OF TOP 15 THREATS ↗	Technical	Information security managers (ISM), chief information security officers (CISO), cybersecurity specialists and CTI analysts.

Top 15 threats

Top Threats 2018		Assessed Trends
1	Malware	---
2	Web-based attacks	↗
3	Web application attacks	---
4	Phishing	↗
5	Denial of service	↗
6	Spam	---
7	Botnets	↗
8	Data breaches	↗
9	Insider threat	↙
10	Physical manipulation, damage, theft and loss	---
11	Information leakage	↗
12	Identity theft	↗
13	Crytojacking	↗
14	Ransomware	↙
15	Cyber espionage	↙

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, --- Stable, ↗ Increasing **Ranking**: ↗ Going up, --- Same, ↙ Going down

Overview

What changed in the landscape

The years 2019 and 2020 brought significant changes in the cyber threat landscape described in these reports. Two distinct facts have significantly contributed to these changes: the historically unique, abrupt transformation forces released by the **coronavirus disease 2019 (COVID-19) pandemic**; and the continuous increasing trend in the **advanced adversary capabilities of threat actors**. Remarkably, the latter has come to amplify the impact of the COVID-19 pandemic in cyberspace.

The COVID-19 pandemic forced large-scale adoption of technology to master a variety of critical aspects of the crisis, such as coordination of health services, the international response to spread of COVID-19, adoption of teleworking regimes, distance learning, interpersonal communication, control of lockdown measures, teleconferencing and many others. Given this situation, business leaders have assessed the emerging risks from abrupt (technological) adoption, which materialised from the transformation forced by the COVID-19 pandemic[2]. And **cybersecurity has been faced with a paradox: it has been both the challenge and the opportunity in this transformation**. The changes imposed in the information technology (IT) landscape weakened existing cybersecurity measures, turning their speedy adaptation into a challenge. At the same time, **cybersecurity is the enabler of trust in emerging use-cases for digital services and thus it has the opportunity to facilitate the transformation.**

While working from home, **cybersecurity specialists had to adapt existing defences** to a new infrastructure paradigm, attempting to minimise the exposure to a variety of novel attacks where the entry points are employees' Internet-connected home and other smart devices. At the same time and under high-pressure, they had to implement solutions based on previously less trusted components, such as remote access through the public Internet, cloud services, unsecured video streaming services and mobile devices and apps. The necessary reaction to the COVID-19 pandemic to guarantee safety and at the same reduce the impact on businesses, has pushed organisations to the limits of their ability to respond to changes. Furthermore, numerous *modus operandi* quickly adapted to the changing work patterns, **cybersecurity professionals found themselves acting at the limits of their capacities**.

In a short turnaround time, IT security professionals had to quickly respond to the challenges introduced by working from home arrangements such as enterprise data movements whenever employees use their home Internet to access cloud-based apps, corporate software, videoconferencing, and file sharing.

As the COVID-19 pandemic is not yet entirely under control, and because of the uncertainty of its future spread, it is expected that it will continue to challenge cybersecurity professionals. Moreover, given the lapsed time before incidents are spotted and analysed, it will leave its footprint on the cyber threat landscape for a long time to come. The COVID-19 pandemic showed that malicious actors had a level of capability that allowed them to adapt to this transformation quickly. In 2019-2020, adversarial *modus operandi* focused on the personalisation of attack vectors. Advanced credential-stealing methods, credential-stuffing, highly targeted phishing attacks, advanced social engineering attacks, advanced malware obfuscation techniques and more extensive penetration of mobile platforms are the main achievements of adversaries in the reporting period. If cybercriminals start combining these advances with artificial intelligence and machine learning, in the future we will see an increase in successful attacks and undetectable campaigns.

Overview

_ Summary

The list below summarises the main trends observed in the cyber threat landscape during the reporting period. These are also reviewed in detail throughout the different reports composing the threat landscape of 2020.

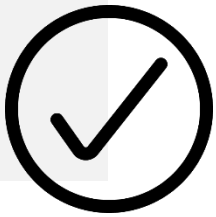
01_ Attack surface in cybersecurity continues to expand as we are entering a new phase of the digital transformation.

02_ There will be a new social and economic norm after the COVID-19 pandemic even more dependent on a secure and reliable cyberspace.

03_ The use of social media platforms in targeted attacks is a serious trend and reaches different domains and types of threats.

04_ Finely targeted and persistent attacks on high-value data (e.g. intellectual property and state secrets) are being meticulously planned and executed by state-sponsored actors.

05_ Massively distributed attacks with a short duration and wide impact are used with multiple objectives such as credential theft.



_ Summary

06_ **The motivation behind the majority of cyberattacks is still financial.**

07_ **Ransomware remains widespread with costly consequences to many organisations.**

08_ **Still many cybersecurity incidents go unnoticed or take a long time to be detected.**

09_ **With more security automation, organisations will be invest more in preparedness using Cyber Threat Intelligence as its main capability.**

10_ **The number of phishing victims continues to grow since it exploits the human dimension being the weakest link.**

With all the changes observed in the cyber threat landscape and the challenges created by the COVID-19 pandemic, there is still a long way before cyberspace becomes a trustworthy and safe environment for everyone.

Overview

_ Are EU citizens more aware of the risks and challenges cyberspace brings?

European Commission prepared a special Eurobarometer survey[4] in 2019 with the aim of understanding EU citizens' awareness, experiences and perceptions of cybersecurity.

EUROBAROMETER

The results of this survey show that Internet use in Europe continues to grow, particularly via smartphones, and citizens are more aware of the potential dangers when going online.

According to the survey's findings, concerns about online privacy and security have already led more than 9 in 10 Internet users to change their online behaviour – most often by not opening e-mails from unknown people, installing anti-virus software, visiting only known and trusted websites and using only their own computers.

While these results are quite encouraging, many users still fall into online fraud and e-mail phishing baits. This reveals that malicious actors are using sophisticated attacks that are harder to detect and avoid. Hence, mitigation strategies have to be updated regularly to accommodate the latest available intelligence (CTI) on attack techniques.


“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

What to expect

Nation-state sponsored actors are likely to

TREND	DESCRIPTION	THREAT
→	**Continue** using cyberspace to issue attacks against electoral processes of foreign countries threatening democratic systems and human rights.[5]	**Attacks against human rights and democratic systems**
→	**Continue** harassing oppositions and monitor their citizens through manipulation of information on social networks, coupled with spyware campaigns.	**Attacks against human rights and democratic systems**
↗	**Launch** sophisticated disinformation campaigns[6] designed to influence perceptions or manipulate opinions in favour of a certain political agenda or financial speculation goals.	**Disinformation campaigns**
↗	**Increase** the race for cyber-arms[7] in the attempt to develop cyber capabilities. With cyberspace considered as a warfare domain, nation-states are likely to scout for cyber-arms through sponsored agents in preparation of a cyber-conflict.	**Uncontrolled cyber-arms race**
↗	**Pursue** strategic objectives such as: obtaining industrial secrets through espionage, obtain leverage over political decision making, fund the regime through financial fraud, conduct cyber-enabled information operations and finally, weaken or demoralise the adversary through disruptive or destructive activities.	**Data theft**

Cyber-offenders are likely to

TREND	DESCRIPTION	THREAT
→	**Continue** targeting teenagers and young adults with sextortion attacks (webcam blackmail) affecting psychologically and ultimately physically the victims.[8]	**Sextortion (webcam blackmail)**
↗	**Increase** the number of cyberbullying attacks during and after the COVID-19 pandemic with adolescents using digital platforms even more for personal or educational purposes.[9]	**Cyberbullying**

Cyber-criminals are likely to

TREND	DESCRIPTION	THREAT
↗	**Increase** the use AI-based tools to create highly believable counterfeits (image, audio and video format) – commonly known as deep-fakes – to defraud companies.	**Deep fake**
→	**Improve** the tactics that compromise business processes to obtain financial advantage.	**Business process compromise (BPC)**
→	**Lower** one level in the organisation - below executive – to compromise business e-mails.	**Business e-mail compromise (BEC)**
→	**Increase** the use of managed service providers (MSPs) to distribute malware.	**Malware**

Conclusions and Recommendations

Policy conclusions/recommendations

- During the last decades, policymakers and technologists inhabited two separate worlds and spoke different languages. To address the challenges from digitalisation, these should **work together** from the ground up and develop a common approach. Since most of today's technology is connected to cyberspace, the contribution from cybersecurity experts in many of these discussions is of paramount importance.
- With the growing technological innovation and rapid expansion of cyberspace, effective and comprehensive EU cybersecurity policies are of critical importance. **Mature cybersecurity policies** will provide the necessary security capacity at all levels of society: governments, critical infrastructures, businesses, tertiary sector and individuals. Security capacity must be effective and flexible to deal with new challenges as they arise to cope with the ever-changing nature of cyberspace.
- Given the increasing number of EU and Member States stakeholders involved in CTI activities, **cooperation and coordination** of EU-wide CTI activities is key. ENISA will promote cooperation with various stakeholders and make an initial attempt to identify the CTI requirements of various stakeholder groups, especially within EU (i.e. the Commission, EU bodies, agencies and Member States).
- CTI should be considered as the main tool for **cybersecurity preparedness** and facilitation of risk-based approaches. Integrating CTI with security management processes will help CTI to proliferate spreading in related areas and will increase the agility of usually lengthy processes such as certification and risk assessment. Moreover, CTI will be seen as a facilitator of emergency decisions needed in crisis management.
- The relevance of CTI for strategic and political decisions is widely accepted and considered essential to facilitate the **connection to geopolitical information** and cyber-physical systems. This will enable CTI to be included in EU-wide decision-making processes but it will also allow its context to expand to identify hybrid threats.

Business conclusions/recommendations

- During 2019, an increasing number of **test labs and cyber-ranges**[10] became available on premises and with cloud offerings. These are important resources for training staff, simulating attacks and testing multiple defence strategies. All in a multipurpose virtual environment.
- Although some CTI criteria and requirements have been developed for various CTI user profiles**, similar requirements** will be necessary for further CTI products, services and tools. CTI vendors will need to take greater account of users' requirements to facilitate the adoption of CTI products and services.
- Investment in some basic CTI concepts, in particular **CTI maturity and threat hierarchies**, is very useful for the uptake of CTI. Vendors will need to orient their offerings to various CTI maturity levels to facilitate efficient use of CTI within organisations of various sizes and budgets.
- In the long run, it looks as if **OpenCTI**[11] may be a good solution to the fragmentation of CTI offerings, given its inherent capability to integrate CTI sources of various types into a single tooling environment. CTI vendors will need to provide the necessary 'bridges' from their products to enable their integration with OpenCTI. The Cyber Range concept was initially defined in 2013 by the European Defence Agency (EDA) in the report "Common staff target for military cooperation on cyber ranges in the European Union" as a multipurpose environment in support of three primary processes: knowledge development, assurance and dissemination.

Conclusions and Recommendations

Research and educational conclusions and recommendations

- The EU should continue investing in **cybersecurity R&D**, with an emphasis on long-term and high-risk research initiatives. Long-term research and innovation is a costly exercise out of reach for most private sector organisations.
- The expansion of knowledge and expertise in cybersecurity is crucial to improve preparedness and resilience. The EU should continue **building capacity** through the investment in cybersecurity training programs, professional certification, exercises and awareness campaigns.
- Cybersecurity research should include expertise from social, behavioural, and economic disciplines. **Multidisciplinary research** in cybersecurity should be promoted and incentivised across the EU.
- The results from research projects in the area of Cybersecurity and in particular on CTI need to be assessed and mapped to a wider context to identify **overlaps and gaps** and to make them comparable to existing commercial products, services and practices. This will help to disseminate these results to the user community.
- Novel approaches for the uptake of CTI knowledge by domains that can profit from it need to be developed. **Examples are cyber-ranges, hybrid threats and geopolitical assessments**. The synergies achieved may boost use-cases and content quality in a multidirectional manner.
- The use of **artificial intelligence (AI)** and machine learning (ML) within CTI should be further investigated. This will reduce the number of manual steps in analysing CTI and will increase the value of machine learning functions within CTI activities.
- The provision and use of open-source CTI material should be promoted. This will facilitate **knowledge transfer**, but it will also lower the threshold for the CTI skills required.

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

in ETL 2020

References

1. "EU Cybersecurity Act". April, 2019.EU Parliament and Council https://eur-lex.europa.eu/eli/reg/2019/881/oj

2. "COVID-19 Risks Outlook: A Preliminary Mapping and its Implications". May 19, 202. WEF. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications

3. "Joint communication to the European parliament, the European council, the council, the European economic and social committee and the committee of the regions. Tackling COVID-19 disinformation - Getting the facts right". June 2020. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0008

4. "Special Eurobarometer 499: Europeans' attitudes towards cyber security". January 29, 2020. https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

5. "EUvsDosinfo" https://euvsdisinfo.eu/european-elections-2019/

6. "Manipulating Social Media to Undermine Democracy". 2017. Freedom House. https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy

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

8. "How online 'sextortion' drove one young man to suicide". February 8. 2018. Today. https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735

9. "Cyberbullying may increase during COVID-19 pandemic, expert says". March 30, 2020. Healio. https://www.healio.com/news/pediatrics/20200330/cyberbullying-may-increase-during-covid19-pandemic-expert-says

10. The Cyber Range concept was initially defined in 2013 by the European Defence Agency (EDA) in the report "Common staff target for military cooperation on cyber ranges in the European Union" as a multipurpose environment in support of three primary processes: knowledge development, assurance and dissemination.

11. Open CTI. https://www.opencti.io/en/

“CTI has been firmly established in the cybersecurity domain as an essential tool for enhancing agility and efficiency in defending cyberattacks.”

in ETL 2020

Related

READ THE REPORT

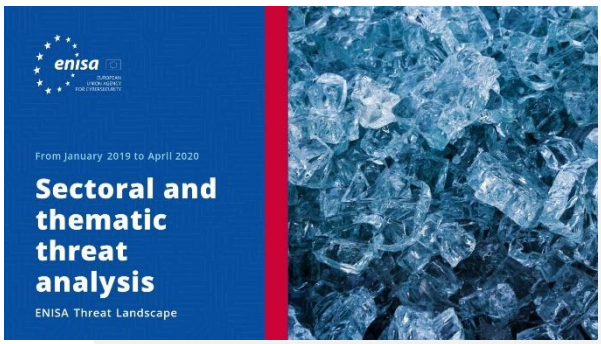
ENISA Threat Landscape Report
List of Top 15 Threats

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
Sectoral and thematic threat analysis

Contextualised threat analysis between January 2019 and April 2020.

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 **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 cyber threat 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 report, 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