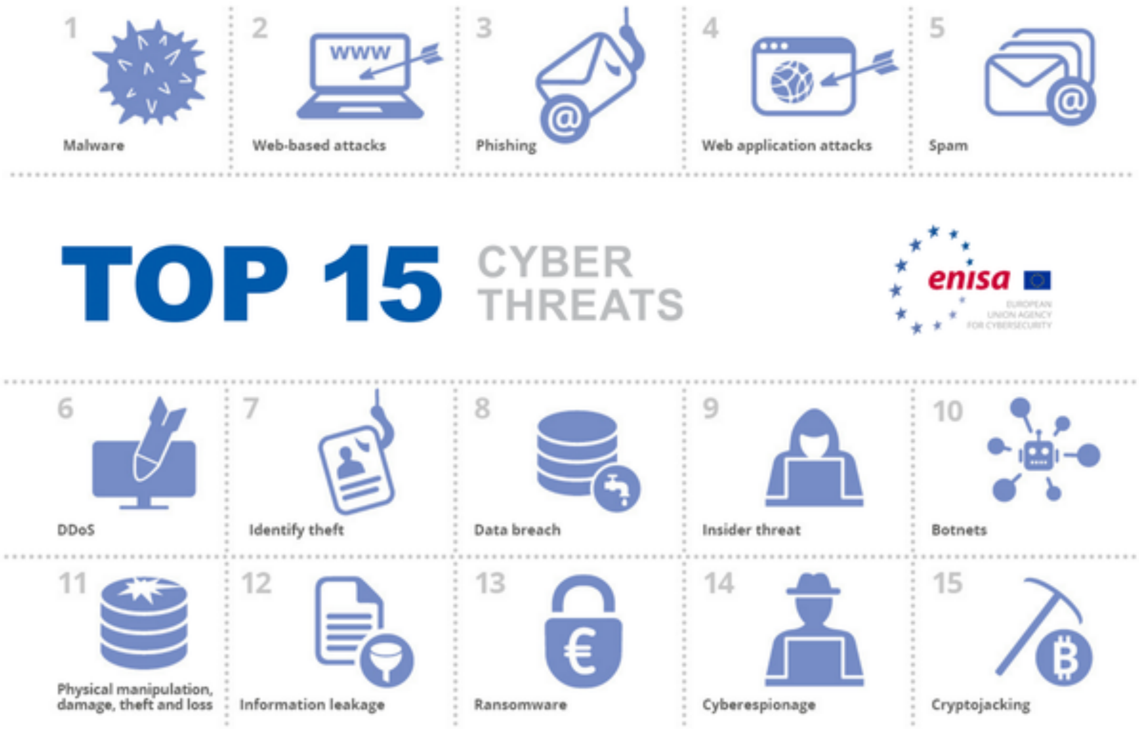
ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected

Threat landscape maps Malware standing strong as #1 Cyber Threat in the EU, with an increase in Phishing, Identity Theft, Ransomware; Monetisation holding its place as cyber criminals' top motivation; and the COVID-19 environment fuelling attacks on homes, businesses, governments and critical infrastructure.

Published on October 20, 2020



Tagged with

- Cyber Threat Intelligence
- Threat landscape

Today, the European Union Agency for Cybersecurity (ENISA), with the support of the European Commission, EU Member States and the CTI Stakeholders Group, has published the 8th annual ENISA Threat Landscape (ETL) 2020 report, identifying and evaluating the top cyber threats for the period January 2019-April 2020.

This year's publication is divided into 22 different reports, available in pdf form and ebook form. The combined report lists the major change from the 2018 threat landscape as the COVID-19-led transformation of the digital environment. During the pandemic, cyber criminals have been seen advancing their capabilities, adapting quickly and targeting relevant victim groups more effectively.

> EU Agency for Cybersecurity Executive Director **Juhan Lepassaar** said: *"Cyber threats are evolving and becoming increasingly complex. This is not new. The Agency has developed the latest 'ENISA Threat Landscape' into a more user-friendly format meeting the needs of its beneficiaries who can use it to advance their readiness and target the response better."*

The ETL report warns that there is a long road ahead to reach a more secure digital environment. This is mainly due to the weakening of existing cybersecurity measures through changes in working and infrastructure patterns caused by the COVID-19 pandemic. This global phenomenon has led to a surge in cyber criminals' personalised cyber attacks, using more advanced methods and techniques.

Boasting a new visual and digital format, this year's threat landscape contains seven strategic reports, along with 15 in-depth reports on the top cyber threats:

- **The Year in Review** report provides a general overview of the threat landscape, including the most important topics, and the top 15 threats, conclusions and recommendations.
- **Cyber Threat Intelligence Overview** summarises the most important topics relevant to the cyber threat intelligence (CTI) community.
- **Sectoral and Thematic Threat Analysis** reviews the threat landscape for specific sectors and technologies, including specifically the EU Agency for Cybersecurity's work on 5G, the Internet of Things (IoT) and smart cars.
- **Main Incidents in the EU and Worldwide** provides an overview of major cybersecurity incidents happening in the EU and worldwide, and highlights the lessons that can be learned.
- **Research Topics** report presents key aspects related to the research and innovation in cybersecurity surrounding the cyber
- threat intelligence domain.
- **Emerging Trends** focuses on the challenges and opportunities for the future in the cybersecurity domain.
- **ENISA's List of the Top 15 Threats**.

The top 15 cyber threat reports are of a technical nature, and include findings, major incidents, statistics and more. The threat reports are the following:

1. **Malware**
2. **Web-based Attacks**
3. **Phishing**
4. **Web Application Attacks**
5. **SPAM**
6. **Distributed Denial of Service (DDoS)**
7. **Identity Theft**
8. **Data Breach**
9. **Insider Threat**
10. **Botnets**
11. **Physical Manipulation, Damage, Theft and Loss**
12. **Information Leakage**
13. **Ransomware**
14. **Cyber Espionage**
15. **Cryptojacking**

The ETL report highlights important aspects and trends related to the threat landscape:

- There will be a new norm during and after the COVID-19 pandemic that is even more dependent on a secure and reliable cyberspace;
- The number of fake online shopping websites and fraudulent online merchants reportedly has increased during the COVID-19 pandemic. From copycats of popular brands

websites to fraudulent services that never deliver the merchandise, the coronavirus revealed weaknesses in the trust model used in online shopping;

- The number of cyberbullying and sextortion incidents also increased with the COVID-19 pandemic. The adoption of mobile technology and subscription to digital platforms makes younger generations more vulnerable to these types of threats;
- Malicious actors are using social media platforms to increase efficiency in targeted attacks;
- Financial reward is still the main motivation behind most cyber attacks;
- Finely targeted and persistent attacks on high-value data, such as intellectual property and state secrets, are being meticulously planned and executed often by state-sponsored actors;
- Massively distributed attacks with a short duration and wide impact are used with multiple aims such as credential theft;
- The number of phishing victims in the EU continues to grow with malicious actors using the COVID-19 theme to lure them in. COVID-19-themed attacks include messages carrying malicious file attachments and messages containing malicious links that redirect users to phishing sites or malware downloads;
- Business Email Compromise (BEC) and COVID-19-themed attacks are being used in cyber-scams resulting in the loss of millions of euros for EU citizens and corporations. European Small and Medium Enterprises (SMEs) have also fallen victim of these threats in a time when many are going through severe financial difficulties due to the loss of revenue;
- Ransomware remains widespread with costly consequences to many EU organisations;
- Many cybersecurity incidents still go unnoticed or take a long time to be detected;
- The number of potential vulnerabilities in a virtual or physical environment continues to expand as a new phase of digital transformation arises (as technology will keep diversifying);
- With more security automation, organisations will invest more in preparedness using CTI as their main capability.

Background

The ETL report maps the cyber threat landscape in a means to help decision-makers, policy-makers and security specialists define strategies to defend citizens, organisations and cyberspace. This work is part of the EU Agency for Cybersecurity’s annual work programme to provide strategic intelligence to its stakeholders. The report’s content is gathered from open sources such as media articles, expert opinions, intelligence reports, incident analysis and security research reports; as well as through interviews with members of the ETL Stakeholders Group, who are part of the EU Cyber Threat Intelligence Community. From the information collected, the Agency produces its own analysis and views of the threat landscape that are meant to be industry and vendor agnostic. The analysis of each report is reviewed and validated by the CTI Stakeholders Group, whose members also vote on the annual list of the top 15 cyber threats.