Annual Report on Cyber Threat Landscape

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

ISSN: 1862-6947
https://eucrim.eu

On 20 October 2020, the European Union Agency for Cybersecurity (ENISA) published the annual report on cyber threats – the "ENISA Threat Landscape 2020" (ETL 2020). The report identified and evaluated the top cyber threats in the EU between January 2019 and April 2020. It shows that cyberattacks are continuing to increase.

There still is a long way towards achieving a more secure and trustworthy digital environment, because existing cybersecurity measures have been weakened through changes in working and infrastructure patterns caused by the COVID-19 pandemic. Personalised cyberattacks have increased considerably, whereby cyber criminals are using more advanced, sophisticated methods and techniques. They are more widespread and often remain undetected.

The ETL 2020 actually consists of 22 different (digital) reports, which are designed for different readerships. "The year in review" is addressed to the general public and provides an overview of the threat landscape, outlining the most important topics referenced across all reports, the 15 most important threats, and conclusions and recommendations (for policy, business, and research/education). It summarizes the top ten trends observed during the reporting period:

- The attack surface in cybersecurity continues to expand due to digital transformation;
- There will be a new social and economic norm after the COVID-19 pandemic that is even more dependent on a secure and reliable cyberspace;
- Social media platforms are increasingly being used for targeted, more efficient attacks, entailing different types of threats;
- Finely targeted and persistent attacks on high-value data (e.g. 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;
- Financial reward is still the predominant motivation behind most cyberattacks;
- Ransomware remains widespread, with costly consequences for many organisations;
- Many cybersecurity incidents still go unnoticed or take a long time to be detected;
- Thanks to more security automation, organisations will invest more in preparedness using Cyber Threat Intelligence (CTI) as their main capability;
- The number of phishing victims continues to grow in the EU since it exploits the human dimension being the weakest link.

The top five threats in 2019/2020 were: malware; web-based attacks; phishing; web application attacks; and spam. As regards the question on the main change compared to previous years' report, it is observed that the COVID-19 pandemic showed the capability of malicious actors to quickly adapt to digital transformation processes, whereas cybersecurity professionals had difficulties responding to the challenges introduced by working-from-home arrangements. During the crisis, cyberattacks proved to be more sophisticated and advanced, such as credential stealing, targeted phishing, social engineering attacks, extensive penetration of mobile platforms, etc.

In addition to the review report, the ETS 2020 provides for the following six strategic and technical reports:

- Sectorial and thematic threat analysis, including 5G, the internet of things and smart cars;
- Main cybersecurity incidents happening in the EU and worldwide;
- Topics of research and innovation in cybersecurity;
- Emerging trends, focusing on the challenges and opportunities for the future in the cybersecurity domain;
- Overview of CTI;
- Report on the top 15 threats, presenting a general overview, the findings, major incidents, statistics, attack vectors and corresponding mitigation measures.

These reports are accompanied by 15 reports that publish detailed information on cyber threats, such as malware, phishing, identity theft, botnets, ransomware, etc.

The ETL is part of ENISA's mandate to provide strategic intelligence to stakeholders. The content is collected 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. The ETL 2020 contributes to the Commission's new cybersecurity strategy.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union