ENISA Report on Cyberthreat 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

The cyberthreat landscape changed significantly in 2018; the risk of becoming the victim of a cyberattack remains high. This is one of the main conclusions of the 2018 Threat Landscape Report by the European Union Agency for Network and Information Security (ENISA). The report (in short "ETL 2018") was released on 28 January 2019.

The ETL 2018 gives an overview of cyberthreat intelligence and provides in-depth analyses of the top 15 cyberthreats, e.g,. malware, web-based attacks, phishing, and botnets. In addition, the report includes analyses on trends and motives in relation to threat agents and attack vectors.

In 2018, the motives and tactics of the most daunting threat agent, namely cyber-criminals and state-sponsored agents, continued to develop. Cyber-jacking is new on the list of the top 15 threats. State-sponsored agents increasingly tend to apply low-profile social engineering attacks, thus shifting away from using complex malicious software and infrastructures.

On the positive side, the report states that defence against cyberattacks and cybercrime has progressed. In particular, threat agent profiling has led to a more efficient identification of attack practices and malicious artefacts. The combination of cyberthreat intelligence and traditional intelligence has also proven to be a successful approach that is to be pursued further. Increased training efforts resulted in better skills and capabilities which is an important factor in building up cyber-resilience.

The identified trends and the need for targeted actions led the ELT 2018 to make several conclusions in the areas of policy, business, and research/education:

- The EU must increase its personnel and technical capabilities in cyberthreat intelligence;
- Regulatory barriers to collecting cyberthreat intelligence should be removed;
- Businesses should make cyberthreat intelligence available to a greater number of stakeholders, especially those who lack technical knowledge;
- Businesses should counteract risks and threats along the entire supply chain;
- Accurate information on incidents and information from related disciplines is crucial for knowledge of cyberthreat intelligence; vendors and researchers must find ways to enlarge the scope of cyberthreat intelligence;
- Knowledge management should be standardised, e.g., by standard vocabularies, standard attack repositories, or automated information collection methods;
- Research should be carried out particularly in the areas of attack practices, malware, malicious infrastructures, and threat agent profiling.

ENISA's Executive Director *Udo Helmbrecht*said that the ETL 2018 "provides recommendations as to how the digital single market can prepare an adequate response to cyber threats, with certification and standardisation at the forefront."

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