Exposure to cyber-attacks in the EU remains high - New ENISA Threat Landscape report analyses the latest cyber threats

In 2018, the cyber threat landscape changed significantly. The most important threat agent groups, namely cyber-criminals and state-sponsored actors have further advanced their motives and tactics. Monetisation motives contributed to the appearance of crypto-miners in the top 15 cyber threats.

Published on January 28, 2019



Tagged with

* [Cyber Threats](https://www.enisa.europa.eu/search?Subject%3Alist=Cyber%20Threats)
* [Threat landscape](https://www.enisa.europa.eu/search?Subject%3Alist=Threat%20landscape)

Advances in defence have also been assessed: law enforcement authorities, governments and vendors were able to further develop active defence practices such as threat agent profiling and the combination of cyber threat intelligence (CTI) and traditional intelligence. This led to a more efficient identification of attack practices and malicious artefacts, leading in turn to more efficient defence techniques and attribution rates.

“We are witnessing the development and deployment of new technologies, which are reshaping the cyber landscape and significantly impacting society and national security. The European Union needs to be ready to adapt to and reap the benefits of these technologies to reduce the cyber-attack surface. This report raises awareness of the cyber dangers that citizens and businesses should be conscious of and responsive to. It provides recommendations as to how the digital single market can prepare an adequate response to cyber threats, with certification and standardisation at the forefront”, said ENISA’s Executive Director Udo Helmbrecht.

The report highlights some of the main trends relating to cyber threats in 2018:

* Mail and phishing messages have become the primary malware infection vector;
* Crypto-miners have become an important monetisation vector for cyber-criminals;
* State-sponsored agents increasingly target banks by using attack-vectors utilised in cyber-crime;
* The emergence of IoT environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices remains a pressing issue;
* Cyber threat intelligence needs to respond to increasingly automated attacks through novel approaches to the use of automated tools and skills.
* Skills and training are the main focus of defenders. Public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.

ENISA addresses these conclusions by making the following recommendations:

* Policy:
  + The EU should develop capabilities to address CTI knowledge management. EU Member States should take measures to increase their independence from currently available CTI sources (mostly from outside the EU) and to enhance the quality of CTI by adding a European context;
  + EU governments and public administrations should share “baseline CTI”, covering sectorial and low-maturity needs of organisations;
  + The collection of CTI should be made easier. Coordinated efforts among EU Member States are key in the implementation of proper defence strategies.
* Business:
  + Businesses need to work towards making CTI available to stakeholders, focusing on the ones that lack technical knowledge;
  + The security software industry needs to research and develop solutions using automation and knowledge engineering, helping end-users and organisations mitigating most of the low-end automated cyber threats, with minimum human intervention;
  + Businesses need to take into account emerging supply chain threats and risks and bridge the gap in security knowledge among the services operated and end-users of the service.
* Technical – research – education:
  + The ingestion of CTI knowledge needs to be enlarged to include accurate information on incidents and information from related disciplines;
  + CTI knowledge management needs to be the subject of standardisation efforts, in particular: standard vocabularies, standard attack repositories, automated information collection methods, and knowledge management processes;
  + Research needs to be conducted to better understand attack practices, malware evolution, malicious infrastructure evolution and threat agent profiling.

More details and context can be found in the report itself: [ENISA Threat Landscape Report 2018](https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018)