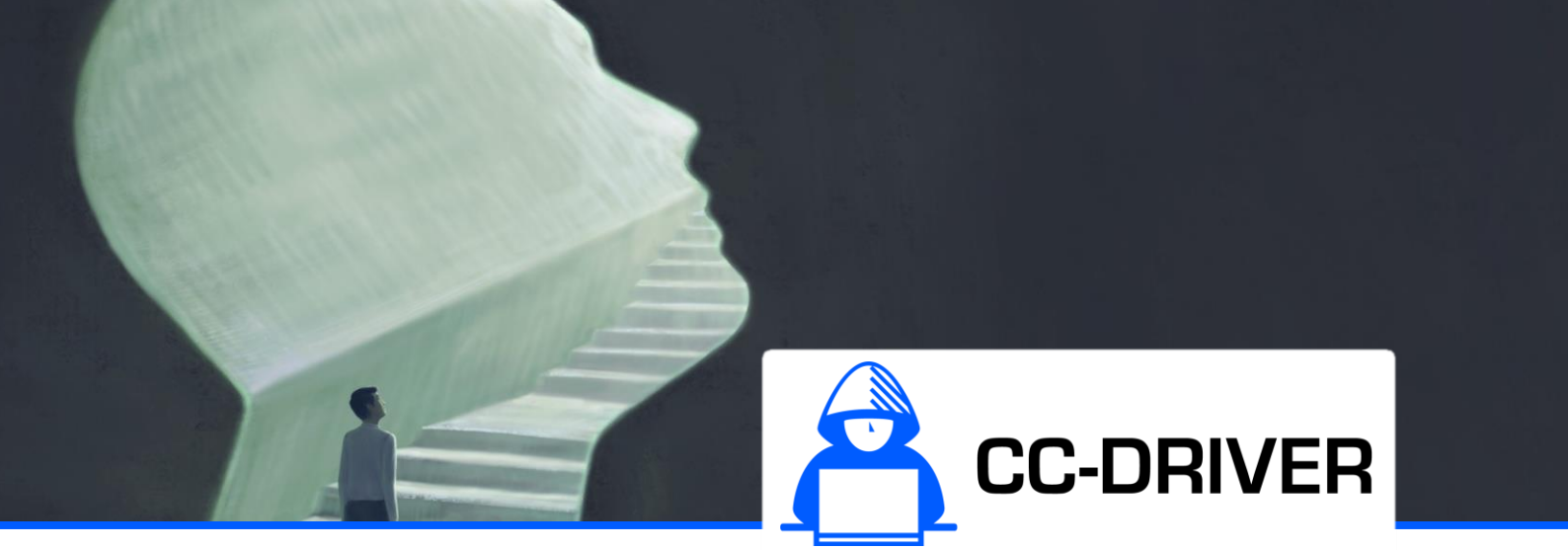

CC-DRIVER

Researching cybercriminality to design new methods to prevent, investigate and mitigate cybercriminal behaviour.

CC-DRIVER Policy Brief No. 2

30 September 2021

Who is this for?

The European Commission (REA, DG HOME, DG CONNECT), selected LEAs, the CC-DRIVER Stakeholder Board, the CC-DRIVER Security Advisory Board, and the CC-DRIVER Ethics Advisory Board.

Highlights

1. With the proliferation of "smart" devices and "Internet-connected" devices and the shift to remote working, cybercriminals have more opportunities to attack their victims.
2. It is recommended that Europe increases support for cutting-edge research and innovation to ensure European leadership in the area of cybersecurity.
3. Individuals may find it difficult to protect themselves from threats in cyberspace they are not familiar with. Therefore, an increased awareness is needed among people of all ages on the tactics and methods used by cybercriminals.
4. It is recommended that Europe trains its workforce to (i) *develop* more secure software, and (ii) *use* security as a key criterion when selecting software.
5. Law Enforcement Agencies should ideally collaborate closely with cybersecurity experts in order to stay ahead of the methods and tactics of cybercriminals.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

CC-DRIVER

The Technical Drivers of Cybercrime

Over the past few years, we have witnessed a significant increase in cybercriminal activities. For example:

- in 2017, the 'Wannacry worm' compromised more than 200,000 computers, crippling a large number of computers in the UK's National Health Service (NHS);
- in May 2021, cybercriminals compromised computers of the Colonial pipeline (a fuel delivery company) disrupting its regular operations; and
- on 30/05/2021, we learned that some of JBS' – the world's largest meat processing company – operations were shut down by hackers who asked for a ransom to be paid, which they eventually received.

The increasing prevalence of cyberattacks begs us to reflect on the following pertinent question:

Why do we have all these attacks? Can't we just solve the problem once and for all?

This is a very legitimate question and it has a surprisingly simple answer: The fast pace of *technological innovation increases the opportunities for and ease with which cybercriminals conduct their illegal activities*. In other words, the rate at which we are creating new digital technologies gives cybercriminals more opportunities to attack.

To explain this, let us consider some examples:

The Internet of Things (IoT) and Other Devices

Over the past few years we have seen an increasing number of devices connecting to the Internet: smart phones, smart wristbands, smart houses, smart refrigerators, smart cars, smart stoves, etc. The Internet-connected use thereof creates opportunities for cybercriminals to break into the individual devices and perform various nefarious activities. For example, consider a hospital that has some of its medical equipment connected to the Internet. If cybercriminals find a vulnerability in the software that runs on the medical equipment or find that one of the users of the equipment has a very weak user password, they can use such weaknesses for breaking into the medical equipment, encrypting important files, and demanding money – otherwise access to the data will be lost, and patients will not be able to receive timely treatment.

Shift to Remote Working

The shift to remote working, accelerated by the pandemic, has created new opportunities for cybercriminals. Organisational networks generally have stronger protections and better configured access control than a typical consumer Wi-Fi network. Besides, cybercriminals may find vulnerabilities in the platforms and tools supporting remote working. For example, the Colonial hack mentioned above started with a compromised virtual private network account, one of those which allow the employees to remotely access the company's computer network. The breach of Twitter in July 2020 was also attributed to remote working.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

Cryptocurrencies

The evolution of cryptocurrencies provides cybercriminals with an easy way to send and receive money. Indeed, as more people get access to cryptocurrencies and as cryptocurrencies are still outside the regulated banking systems, cybercriminals are able to send and receive money without the traditional banking regulations and controls. Moreover, the anonymity (or pseudonymity) provided by many of these currencies enables cybercriminals to do their transactions (practically) anonymously.

To summarise, technical developments, such as cryptocurrencies and smart devices, are being exploited as a springboard for cybercriminals in their illegal activities.

Recommendations

How should the EU respond to these attacks? Past policy interventions (such as the General Data Protection Regulation, GDPR) have demonstrated that strong policy decisions may help to improve security and privacy of EU citizens in cyberspace. Moreover, inaction (i.e., doing nothing) may lead to even worse outcomes. Indeed, doing nothing implies that cybercriminals will be almost free to dominate the cyberspace. To make matters worse, as cyberspace continues to evolve (with new applications and devices connecting to it), cybercriminals will be given a leveled landscape and a clear head start, while citizens and Law Enforcement Agencies may just watch the evolution without being able to keep up with cybercriminals. Some options for policy interventions may include:

Aiming Towards European Leadership in Cybersecurity Through Research and Innovation

This is one of the best options available to combat cybercrime. Indeed, if Europe is a latecomer in the area of cybersecurity, then Europe (along with its citizens) will continue to be an easy target for cybercriminals. On the contrary, if Europe becomes a world *leader* in the technical aspects of cybersecurity, it will be able to deal with cybercriminals and cybercrime more effectively. History suggests that *this technical leadership is usually achieved through high-end research and innovation*. Such research and innovation will (i) enable Europe to develop its own cybersecurity products, and (ii) allow European firms to successfully integrate IT components they receive from third parties. Such leadership will contribute towards Europe's autonomy in the area of cybersecurity and towards Europe's Digital Sovereignty.

Support Technical Training and Education of Europe's Workforce

To be able to defend against cybercrime, Europe needs a skilled workforce who is able to understand the technical aspects of cybersecurity, and how these aspects may act as a springboard for cybercrime. Indeed, vulnerabilities in software, hastily developed applications, and poorly tested components are all entry points for cybercriminals who want to compromise a computer. Educating a generation of European engineers, highly trained in the area of cybersecurity and vulnerabilities, can be one of the best defences against cybercrime. Europe will therefore ideally train its workforce to (i) develop more secure software, and (ii) focus on security as a key criterion when selecting software.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

Make Cybersecurity Experts Part of the Solution – Evidence-based Policy Making

Policy makers and scientists should work together in order to reach the best decisions with respect to cybercrime. Scientists can provide the scientific knowledge and the research results that can be used by policy makers to drive future policy decisions based on solid scientific evidence.

Support Awareness

In several cases, cyberattacks are the result of human error. For example, people may fall victim to phishing, and/or they may be inadvertently used as money mules, to name a few. This happens mainly because people cannot usually protect themselves against a threat (i) if they are unaware that such a threat exists or (ii) if they encounter this threat for the first time. Moreover, since the cyberspace is still new to many individuals, cybercrime methods and tactics are still unknown. *Increasing awareness* is one of the best ways to prevent cybercrime even before it occurs. This awareness covers all ages: from elementary school to senior citizens – Particularly because people of all ages can fall victim to cybercrime.

Facilitate the Collaboration Between Cybersecurity Experts and LEAs

In order to develop novel cybercrime-fighting mechanisms, cybersecurity experts need access to large data repositories. Such data repositories may include (i) malware databases, (ii) software used by cybercriminals, (iii) activity logs of the computers involved in cybercrime, (iv) detail accounts of the activities of cybercriminals, etc. Without access to such data, it is difficult for cybersecurity experts to develop new algorithms and subsequently train machine-learning-based cybercrime detection models. Unfortunately, such data are not usually readily available to cybersecurity experts and are accessible only by Law Enforcement Agents. Additionally, Law Enforcement Agencies have little access to cutting-edge algorithms which are usually developed in research labs of Universities and Research Centres. This division of labour (i.e., LEAs have the data and cybersecurity experts develop the algorithms) effectively cripples novel approaches to fighting cybercrime. If the algorithms are not trained on the most recent data, they will always be suboptimal and they will always give cybercriminals the opportunity to be one-step ahead. It seems that we need to develop a new framework that will allow LEAs to collaborate more closely with cybersecurity experts through a more meaningful sharing of data, algorithms, and results.

Further Reading

- EUROPOL: Internet Organised Crime Threat Assessment (IOCTA) 2020. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
- ENISA: ENISA Threat Landscape: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.