CYBERCRIME IS BECOMING BOLDER WITH DATA AT THE CENTRE OF THE CRIME SCENE

09 Oct 2019

Press Release


IOCTA
INTERNET
ORGANISED
CRIME THREAT
ASSESSMENT
[2019]

Europol's 2019 cybercrime report provides insights into emerging threats and key developments.

Cybercrime is continuing to mature and becoming more and more bold, shifting its focus to larger and more profitable targets as well as new technologies. Data is the key element in cybercrime, both from a crime and an investigate perspective.

These key threats demonstrate the complexity of countering cybercrime and highlight that criminals only innovate their criminal behaviour when existing modi operandi have become unsuccessful or more profitable opportunities emerge. In essence, new threats do not only arise from new technologies but often come from known vulnerabilities in existing technologies that remain unpatched for extended periods of time. Law enforcement must therefore not only focus on the potential impact of future technological developments in cybercrime, such as artificial intelligence but also approach cybercrime in a holistic sense, including prevention, awareness and increasing cyber education and resilience.

Europol's 6th annual Internet Organised Crime Threat Assessment (IOCTA), presented today at the Europol-INTERPOL Cybercrime Conference at Europol's headquarters, offers a unique law enforcement view of the emerging threats and key developments in the field of cybercrime over the last year.

In addition to the main trends of 2019, the IOCTA also recommends focusing on two cross-cutting phenomena that enhance all types of cybercrime. The full IOCTA 2019 report can be found on Europol's website.

CROSS-CUTTING CYBERCRIME PHENOMENA

1. Data is at the centre of crime scenes. Cybercriminals target data for their crimes, so data security and consumer awareness are paramount for organisations. Data security has once again taken centre stage following the implementation of the General Data Protection Regulation (GDPR).
2. Cybercrime is maturing and becoming bolder, shifting its focus to larger and more profitable targets.

2019 IOCTA MAIN TRENDS

1. Ransomware remains the top cybercrime threat in 2019. Even though law enforcement has witnessed a decline in the overall volume of ransomware attacks, those that do take place are more targeted, more profitable and cause greater economic damage. As long as ransomware provides relatively easy income for cybercriminals and continues to cause significant damage and financial losses, it is likely to remain the top cybercrime threat.

2. DDoS attacks: while using ransomware to deny an organisation access to its own data may be the primary threat in this year's IOCTA, denying others access to that organisation's data or services is another significant threat. Distributed Denial of Service (DDoS) was one of the most prominent threats reported to Europol. Many banks report that DDoS attacks remain a significant problem, resulting in the interruption of online bank services, creating more of a public impact rather than direct financial damage.

3 **Data overload in fighting child sexual exploitation material:** the amount of material detected online by law enforcement and the private sector continues to increase. This increase puts considerable strain on law enforcement resources. One development that could be of concern for online child sexual exploitation is the ongoing improvements of deepfakes. Deepfake technology is an AI-based technique that places images or videos over another video.

4 **Self-generated explicit material** is more and more common, driven by a growing number of minors with access to high-quality smartphones. A lack of awareness about the risks on the side of minors exacerbates the problem.

5 **Smart cities**: the most visible ransomware attacks in 2019 were those against local governments, specifically in the United States. Whether this trend will also become a threat tc EU Member States is something to be seen, but experiences in the US are a warning.

6 **Law enforcement is increasingly responding to attacks on critical infrastructure.** Law enforcement appears to have become involved in a much wider variety of investigations into attacks on critical infrastructures, including attacks on the energy, transport, water supply, and health sectors. Attacks on these infrastructures by financially motivated criminals remain unlikely, as such attacks draw the attention of multiple authorities and as such pose a disproportionate risk.

7 **The Darknet is becoming more fragmented:** there are increases in single-vendor shops and smaller fragmented markets on Tor, including those catering for specific languages. Some organised crime groups are also fragmenting their business over a range of online monikers and marketplaces, therefore presenting further challenges for law enforcement.

8 **Blockchain marketplaces:** in addition to circumventing law enforcement, criminal developers are also motivated by the need to increase trust with their customer base on Tor, both in terms of anonymity but also by reducing the risk of exit scams. An example of such a market is Black Dog, scheduled for launch in August 2019. It claims to be the 'first-ever truly decentralised crypto market' and depends on the Ethereum blockchain to facilitate transactions.

9 **Business email compromise:** data returns to the discussion of business email compromise, which is a crucial priority reported by both Member States and the private industry. While this crime is not new, it is evolving. This scam exploits the way corporations do business, taking advantage of segregated corporate structures, and internal gaps in payment verification

processes.

10 EU law enforcement emergency response protocol: the coordinated response to large-scale cyber-attacks remains a key challenge to effective international cooperation in the cybersecurity ecosystem. The development of the EU law enforcement emergency response protocol has significantly improved the cyber preparedness by shifting away from incongruent incident-driven and reactive response measures and acting as critical enablers for rapid response capabilities that support cyber resilience.

Catherine De Bolle, Europol's Executive Director commented: "This year's IOCTA demonstrates that while we must look ahead to anticipate what challenges new technologies, legislation, and criminal innovation may bring, we must not forget to look behind us. 'New' threats continue to emerge from vulnera¬bilities in established processes and technologies. Moreover, the longevity of cyber threats is clear, as many long-standing and established modi operandi persist, despite our best efforts. Some threats of yesterday remain relevant today and will continue to challenge us tomorrow. Also, the global impact of huge cybersecurity events has taken the threat from cybercrime to another level. At Europol, we see that key tools must be developed to keep cybercriminals at bay. This is all the more important, considering that other crime areas are becoming increasingly cyber-facilitated."

European Commissioner for Migration, Home Affairs and Citizenship, Dimitris Avramopoulos, said: "Cybercriminals are becoming bolder than ever and so should we in our common European response. I am glad to see that Europe's efforts to tackle large-scale cyber-attacks across borders are bringing results. But I am distraught by the fact that child sexual abuse material continues to thrive online. We all need to step up our efforts at all levels, because cybersecurity isn't just the task of national law enforcement. It is a responsibility for all of us towards our citizens."

European Commissioner for the Security Union, Julian King, said: "Cybercrime is a rapidly evolving threat both in its own right but also as a tool of serious and organised crime. I fully support the excellent work done by EC3 @Europol to help Member States in the fight against this growing menace."

CRIME AREAS Cybercrime • Forgery of money and means of payment • Economic Crime • Money Laundering • Organised property crime • Intellectual property crime • Counterfeiting and Product Piracy
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

ENTITIES European Cybercrime Center (EC3)

Source URL: https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene