15 WAYS YOU COULD BE THE NEXT VICTIM OF CYBERCRIME

18Sep2018

Press Release

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

IOCTA 2018 / Report (pdf)

IOCTA 2018 dedicated page

Cybercriminals are adopting creative new techniques to target their victims at an unprecedented pace and are constantly seeking methods to avoid law enforcement detection. To stay ahead of them, law enforcement should target cybercriminals offering "off-the-shelf" cyber-attack services or products to make it more difficult for low-level cybercriminals to carry out high-level attacks.

Europol's fifth annual Internet Organised Crime Threat Assessment (IOCTA), presented today at the INTERPOL-Europol Cybercrime Conference in Singapore, offers a unique law enforcement view of the emerging threats and key developments in the field of cybercrime over the last year. But more than that, it describes anticipated future threats and provides recommendations to law enforcement authorities in Europe to adequately deal with these challenges. The report only has one goal in mind: to stop cybercriminals from making you their next victim.

We'll shed some light on some of the main trends here. A complete overview can be found in the full

report on Europol's website.

RANSOMWARE, MALWARE, BEWARE!

1. Ransomware has become a standard attack tool for cybercriminals. However, criminals are moving from random attacks to targeting companies or individuals where greater potential benefits lie.

2. Mobile malware may grow as users shift from online to mobile banking.

3. Cyber-attacks have become increasingly stealthy and harder to detect. Attacks using fileless malware have become a standard component of the crime-as-a-service[1] industry.

4. The GDPR legislation requires breaches to be reported within 72 hours. Criminals may try to extort breached organisations. While this is not new, it is possible that hacked companies will prefer to pay a smaller ransom to a hacker for non-disclosure than the steep fine that might be imposed by the authorities.

5. The motive behind network intrusions is the illegal acquisition of data, for a variety of purposes, including phishing or payment fraud.

6. DDoS attacks continue to grow and tools to launch them are easily available as a service, allowing unskilled individuals to launch significant DDoS attacks.

7. Continued growth in the volume of social engineering attacks is expected, but as a key component of more complex cyber-attacks. West African fraudsters are likely to have a more significant role within the EU in the future, as Africa continues to have the fastest growing internet usage globally.

CRYPTOCURRENCIES ARE NO SAFE HAVEN

8. Criminals will continue to abuse cryptocurrencies. Cyber-attacks which historically targeted traditional financial instruments are now targeting businesses and users of cryptocurrencies. Cryptomining has been exploited by financially motivated cybercriminals, who for instance hack legitimate websites to cryptojack[2] users visiting those sites. Such attacks are much more appealing to cybercriminals wishing to keep a low profile, requiring little or no victim engagement and, at least currently, minimal law enforcement attention (with browser-based mining not actually being illegal). Another emerging threat is 'true' cryptomining malware which uses the processing power of infected machines to mine cryptocurrencies.

9. We anticipate a more pronounced shift towards more privacy-oriented currencies. An increase in extortion demands and ransomware in these currencies will exemplify this shift.

ONLINE CHILD SEXUAL EXPLOITATION

10. Online child sexual exploitation continues to be the most disturbing aspect of cybercrime with volumes of material that were unimaginable ten years ago, partly because of the growing number of young children with access to internet-enabled devices and social media.

11. This leads to an explosion of self-generated material. Such images are often initially produced and shared voluntarily and end up in the hands of online child sex offenders. Offenders might also obtain images through sexual extortion of minors.

12. Offenders continuously seek new ways to avoid detection from law enforcement, including anonymisation and encryption tools, everyday communication applications with end-to-end encryption, social media platforms or even within Bitcoin's blockchain. Most material is still found on the surface internet, but some of the more extreme material tends to be found on hidden services that can only be accessed on the Darknet.

13. Live streaming of child sexual abuse remains a particularly complex crime to investigate and is likely to further increase in the future. It often leaves few forensic traces and the live streamed material does not need to be downloaded or locally stored. It will most likely move to other parts of the world, where legislation and law enforcement are not always able to keep up with the rapid developments in this area. The live streaming of self-generated material is also expected to increase.

PAYMENT CARD FRAUD

14. Skimming is still successful as card magnetic stripes continue to be used. Instant payments may reduce detection and intervention opportunities by banks. This can potentially lead to a higher fraud rate.

15. Telecommunications fraud represents an old but growing trend in fraud involving non-cash payments.

Europol's Executive Director Catherine De Bolle: "Cybercrime cases are increasingly complex and sophisticated. Law enforcement requires additional training, investigative and forensic resources in order to adequately deal with these challenges. The policing opportunities arising from emerging technologies, such as big data analytics and machine learning, need to be seized. Europol will continue its efforts to enhance cooperation with international law enforcement and government agencies, tech companies, academia and other relevant stakeholders. Only if we do this, can cybercrime be combated effectively."

European Commissioner for Migration, Home Affairs and Citizenship, Dimitris Avramopoulos, added: "Cybercriminals continue to threaten and attack our citizens online, endangering both their virtual and physical integrity, especially the most vulnerable ones. Together with Europol, the EU is committed to step up its fight against all areas of cybercrime and especially the sexual exploitation

of children as well as terrorist content online, both legally and operationally. As this report highlights, to tackle these threats we need to foster trust, information sharing and cooperation between all stakeholders."

European Commissioner for the Security Union, Sir Julian King, concluded: "As the report shows, Europe is still faced with a range of security threats from terrorism and cyber. We will continue to take decisive action, with the support of Europol, to tackle these threats, through our proposals on terrorist content online, electronic evidence and on election security, and through our cybersecurity strategy."

---

[1] The Crime-as-a-Service (CaaS) model describes a criminal business model that drives the digital underground economy, providing a wide range of commercial services and tools that facilitate crime online and enables a broad base of unskilled, entry-level cybercriminals to commit cybercrime.

[2] Cryptojacking refers to any process that uses the processing power or bandwidth of a device to mine cryptocurrencies without the user's permission.

EN Internet Organised Crime Threat Assessment 2018 [11.4 MB]

CRIME AREAS Cybercrime • High-Tech crimes • Social engineering
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/15-ways-you-could-be-next-victim-of-cybercrime