THE RELENTLESS GROWTH OF CYBERCRIME

27 Sep 2016

Press Release

Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA)

Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA) identifies an expanding cybercriminal economy exploiting our increasingly Internet-enabled lives and low levels of digital hygiene. Informed largely by Europol's law enforcement and cooperation partners, the report identifies eight main cybercrime trends and provides key recommendations to address the challenges.

The volume, scope and material cost of cybercrime all remain on an upward trend and have reached very high levels. Some EU Member States now report that the recording of cybercrime offences may have surpassed those associated with traditional crimes. An expansion both in the number of cybercriminal actors and opportunities to engage in highly profitable illegal activities has partly fuelled this trend, as has the development of new cybercrime tools in areas such as ATM fraud and mobile malware. However, a large part of the problem relates to poor digital security standards and practice by businesses and individuals. A significant proportion of cybercrime activity still involves the continuous recycling of relatively old techniques, security solutions for which are available but not widely adopted.

Europol's Director Rob Wainwright: "The relentless growth of cybercrime remains a real and significant threat to our collective security in Europe. Europol is concerned about how an expanding cybercriminal community has been able to further exploit our increasing dependence on technology and the Internet. We have also seen a marked shift in cyber-facilitated activities relating to trafficking in human beings, terrorism and other threats. In response law enforcement authorities have increased their skill-sets and their capability to work together in platforms such as the European Cybercrime Centre at Europol, but the growing misuse of legitimate anonymity and encryption services for illegal purposes remain a serious impediment to the detection, investigation and prosecution of criminals."

The Head of the European Cybercrime Centre, Steven Wilson: "2016 has seen the further evolution of established cybercrime trends. The threat from ransomware has continued to grow and has now expanded into sectors such as healthcare. Europol has also seen the development of malware targeting the ATM network, impacting cash services worldwide. Online child sexual abuse continues to be a very high priority for all countries, with international cooperation established as a significant part of the strategy to protect children and identify victims. However there are many positives to be

taken from this year's report. Partnerships between industry and law enforcement have improved significantly, leading to the disruption or arrest of many major cybercriminal syndicates and high-profile individuals associated with child abuse, cyber intrusions and payment card fraud, and to innovative new prevention programmes such as the no more ransom campaign."

The eight cybercrime trends from the 2016 IOCTA:

Trend 1: Crime-as-a-Service
The digital underground is underpinned by a growing Crime-as-a-Service model that interconnects specialist providers of cybercrime tools and services with an increasing number of organised crime groups. Terrorist actors clearly have the potential to access this sector in the future.

Trend 2: Ransomware
Ransomware and banking Trojans remain the top malware threats, a trend unlikely to change for the foreseeable future.

Trend 3: The criminal use of data
Data remains a key commodity for cyber-criminals. It is procured for immediate financial gain in many cases but, increasingly, also acquired to commit more complex fraud, encrypted for ransom, or used directly for extortion.

Trend 4: Payment fraud
EMV (chip and PIN), geo-blocking and other industry measures continue to erode card-present fraud within the EU, but logical and malware attacks directly against ATMs continue to evolve and proliferate. Organised crime groups are starting to manipulate or compromise payments involving contactless (NFC) cards.

Trend 5: Online child sexual abuse
The use of end-to-end encrypted platforms for sharing media, coupled with the use of largely anonymous payment systems, has facilitated an escalation in the live streaming of child abuse

Trend 6: Abuse of the Darknet
The Darknet continues to enable criminals involved in a range of illicit activities, such as the exchange of child sexual exploitation material. The extent to which extremist groups currently use cyber techniques to conduct attacks are limited, but the availability of cybercrime tools and services, and illicit commodities such as firearms on the Darknet, provides opportunity for this to change.

Trend 7: Social engineering
An increase of phishing aimed at high value targets has been registered by enforcement private sector authorities. CEO fraud, a refined variant of spear phishing, has become a key threat.

Trend 8: Virtual currencies

Bitcoin remains the currency of choice for the payment for criminal products and services in the digital underground economy and the Darknet. Bitcoin has also become the standard payment solution for extortion payments.

Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA) is produced by the European Cybercrime Centre (EC3) at Europol. It informs decision-makers at strategic, policy and tactical levels in the fight against cybercrime, and focuses on three crime areas: cyber-attacks, child sexual exploitation online and payment fraud.

The 2016 IOCTA provides a predominantly law enforcement focussed assessment of the key developments, changes and emerging threats in the field of cybercrime over the last few years. It is based on contributions by EU Member States and the expert input of Europol's staff, which has been further enhanced and combined with input from Europol's partners in private industry, the financial sector and academia. A key role for the IOCTA is to inform priority setting for the operational action plans in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

The publication of the 2016 IOCTA is the starting point of Europol's engagement in the European Cyber Security Month (ECSM). The ECSM is the European Union's annual advocacy campaign that takes place in October and aims to raise awareness of cyber security threats, promote cyber security among citizens and provide up to date security information, through education and sharing of best practices.

Read more in the IOCTA 2016 Report

CRIME AREAS Cybercrime • High-Tech crime • Social engineering • Child Sexual Exploitation • Forgery of money and means of payment • Payment Fraud • Money Muling
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
GENERAL TERMS EU Police Cycle (EMPACT) • Law Enforcement
ENTITIES European Cybercrime Center (EC3)

Source URL: https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime