INTERNET ORGANISED CRIME THREAT ASSESSMENT 2018

IOCTA 2018 / Download the full report(pdf)

FOREWORD

It is my pleasure to introduce the 2018 Internet Organised Crime Threat Assessment (IOCTA), not only as it is the fifth anniversary edition of the report, but also my first as the Executive Director of Europol.

The IOCTA has been and continues to be a flagship strategic product for Europol. It provides a unique law enforcement focused assessment of the emerging threats and key developments in the field of cybercrime over the last year. This is of course only possible thanks to the invaluable contributions from European law enforcement and the ongoing support we receive from our partners in private industry, the financial sector and academia.

Each year the report highlights cyber-attacks of an unprecedented scope and scale. This year is no different, demonstrating the continuing need for greater cooperation and collaboration within our law enforcement community, an ethos at the very heart of Europol's mission. The report also brings to our attention previously underestimated threats, such as telecommunication frauds, demonstrating the necessity for law enforcement to constantly adapt and develop and the need for continued training in all aspects of cybercrime.

While some cyber-attacks continue to grab headlines with their magnitude, other areas of cybercrime are no less of a threat or concern. Payment fraud continues to emphasise significant financial losses, criminal gains and the facilitation of other crime; while online child sexual exploitation epitomises the worst aspects of the internet and highlights the ever present danger to our children from those who would seek to exploit or abuse them.

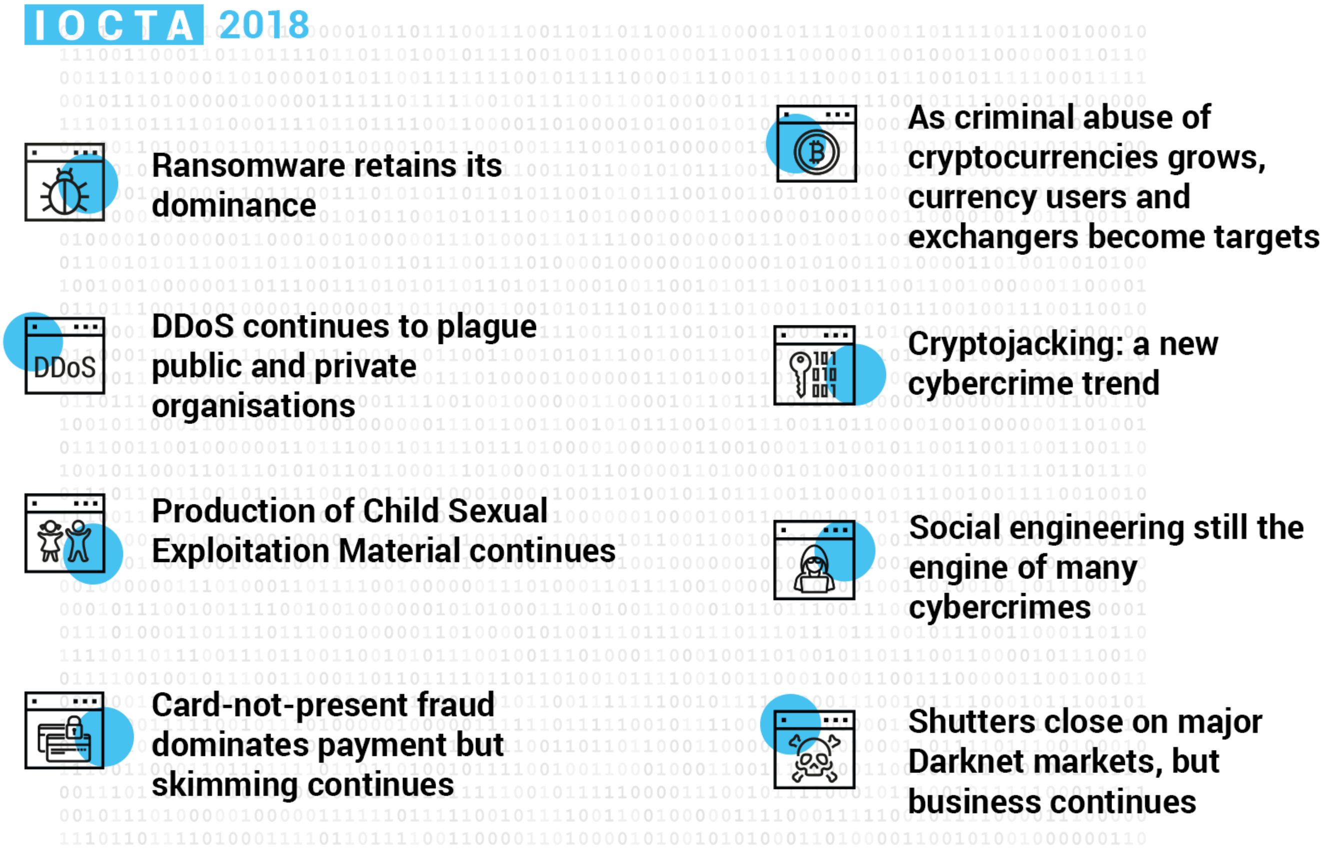
This year's report also describes a number of key legislative and technological developments, such as the introduction of the General Data Protection Regulation (GDPR), the Network and Information Security (NIS) directive and 5G technology. While these developments are positive, all will in some way impact on our ability as law enforcement officers to effectively investigate cybercrime. This emphasises the need for law enforcement to engage with policy makers, legislators and industry, in order to have a voice in how our society develops.

The IOCTA also celebrates the many successes of law enforcement in the fight against cybercrime. As long as European Union law enforcement continues to grow and evolve and to forge new bonds with global partners in both the public and private sector, I am confident that we can continue to report such successes for years to come.

Catherine De Bolle, Executive Director of Europol

EXECUTIVE SUMMARY

For the fifth year in a row, Europol has produced the Internet Organised Crime Threat Assessment (IOCTA). The aim of this Assessment is to provide a comprehensive overview of the current, as well as anticipated future threats and trends of crimes conducted and/or facilitated online. While current events demonstrate how cybercrime continues to evolve, this year's IOCTA shows us how law enforcement has to battle both innovative as well as persistent forms of cybercrime. Many areas of the report therefore build upon previous editions, which emphasises the longevity of the many facets of cybercrime. It is also a testimony to an established cybercrime business model, where there is no need to change a successful modus operandi. The report also highlights the many challenges associated with the fight against cybercrime, both from a law enforcement and, where applicable, a private sector perspective.



IOCTA 2018

Ransomware retains its dominance

As criminal abuse of cryptocurrencies grows, currency users and exchangers become targets

DDoS continues to plague public and private organisations

Cryptojacking: a new cybercrime trend

Production of Child Sexual Exploitation Material continues

Social engineering still the engine of many cybercrimes

Card-not-present fraud dominates payment but skimming continues

Shutters close on major Darknet markets, but business continues

Ransomware retains its dominance

Even though the growth of ransomware is beginning to slow, ransomware is still overtaking banking Trojans in financially-motivated malware attacks, a trend anticipated to continue over the following years. In addition to attacks by financially motivated criminals, significant, public reporting increasingly attributes global cyber-attacks to the actions of nation states. Mobile malware has not been extensively reported in 2017, but this has been identified as an anticipated future threat for private and public entities alike.

Illegal acquisition of data following data breaches is a prominent threat. Criminals often use the obtained data to facilitate further criminal activity. In 2017, the biggest data breach concerned Equifax, affecting more than 100 million credit users worldwide. With the EU GDPR coming into effect in May 2018, the reporting of data breaches is now a legal requirement across the EU, bringing with it hefty fines and new threats and challenges.

DDoS continues to plague public and private organisations

Criminals continue to use Distributed-Denial-of-Service (DDoS) attacks as a tool against private business and the public sector. Such attacks are used not only for financial gains but for ideological, political or purely malicious reason. This type of attack is not only one of the most frequent (only second to malware in 2017); it is also becoming more accessible, low-cost and low-risk.

Production of CSEM continues

The amount of detected online Child Sexual Exploitation Material (CSEM), including Self-Generated Explicit Material (SGEM), continues to increase. Although most CSEM is still shared through P2P platforms, more extreme material is increasingly found on the Darknet. Meanwhile, Live Distant Child Abuse (LDCA), facilitated by growing internet connectivity worldwide, continues to be a particularly complex form of online CSE to investigate due to the technologies and jurisdictions involved.

As increasing numbers of young children have access to internet and social media platforms, the risk of online sexual coercion and extortion continues to rise. The popularity of social media applications with embedded streaming possibilities has resulted in a strong increase in the amount of SGEM live streamed on these platforms.

Card-not-present fraud dominates payment but skimming continues

Skimming remains a common issue in most of the EU Member States. As in previous years, this continues to decrease as a result of geoblocking measures. Skimmed card data is often sold via the Darknet and cashed out in areas where Europay, MasterCard and Visa (EMV) implementation is either slow or non-existent.

Toll fraud has received a considerable amount of attention this year, with criminal groups using counterfeit fuel and credit/debit cards to avoid paying toll fees. Many Member States also reported an increase in the creation of fake companies to access and abuse Points of Sale (PoS), as well as profit from compromised information. Meanwhile, CNP fraud continues to be a key threat for EU Member States, with the transport and retail sectors highlighted as key targets within the EU.

As criminal abuse of cryptocurrencies grows, currency users and exchangers become targets

Previous reports indicated that criminals increasingly abuse cryptocurrencies for funding criminal activities. While Bitcoin has lost its majority of the overall cryptocurrency market share, it still remains the primary cryptocurrency encountered by law enforcement. In a trend mirroring attacks on banks and their customers, cryptocurrency users and facilitators have become victim of cybercrimes themselves. Currency exchangers, mining services and other wallet holders are facing hacking attempts as well as extortion of personal data and theft. Money launderers have evolved to use cryptocurrencies in their operations and are increasingly facilitated by new developments such as decentralised exchanges which allow exchanges without any Know Your Customer requirements. It is likely that high-privacy cryptocurrencies will make the current mixing services and tumblers obsolete.

Cryptojacking: a new cybercrime trend

Cryptojacking is an emerging cybercrime trend, referring to the exploitation of internet users’ bandwidth and processing power to mine cryptocurrencies. While it is not illegal in some cases, it nonetheless creates additional revenue streams and therefore motivation for attackers to hack legitimate websites to exploit their visitor systems. Actual cryptomining malware works to the same effect, but can cripple a victims system by monopolising their processing power.

Social engineering still the engine of many cybercrimes

The significance of social engineering for cyber-dependent and cyber-enabled crime continues to grow. Phishing remains the most frequent form of social engineering, with vishing and smishing less common. Criminals use social engineering to achieve a range of goals: to obtain personal data, hijack accounts, steal identities, initiate illegitimate payments, or convince the victim to proceed with any other activity against their self-interest, such as transferring money or sharing personal data.

Shutters close on major Darknet markets, but business continues

The Darknet will continue to facilitate online criminal markets, where criminals sell illicit products in order to engage in other criminal activity or avoid surface net traceability. In 2017, law enforcement agencies shut down three of the largest Darknet markets: AlphaBay, Hansa and RAMP. These takedowns prompted the migration of users towards existing or newly-established markets, or to other platforms entirely, such as encrypted communications apps.

Although cybercrime continues to be a major threat to the EU, last year again saw some remarkable law enforcement success. Cooperation between law enforcement agencies, private industry, the financial sector and academia is a key element of this success.

CRIME PRIORITY: CYBER-DEPENDENT CRIME

Cyber-dependent crime can be defined as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). In essence, without the internet criminals could not commit these crimes. It includes such activity as the creation and spread of malware, hacking to steal sensitive personal or industry data and denial of service attacks to cause financial and/or reputational damage.

Key findings

- Ransomware remains the key malware threat in both law enforcement and industry reporting.

- Ransomware remains the key malware threat in both law enforcement and industry reporting.
- Cryptomining malware is expected to become a regular, low risk revenue stream for cybercriminals.
- The use of exploit kits (EKs) as a means of infection continues to decline, with spam, social engineering and newer methods such as RDP brute-forcing coming to the fore.
- New legislation relating to data breaches will likely lead to greater reporting of breaches to law enforcement and increasing cases of cyber-extortion.

RECOMMENDATIONS

Cooperation

The combination of factors behind the WannaCry and NotPetya attacks of mid-2017 have taken malware attacks to a level where they can be an impossible challenge for national law enforcement agencies to handle alone. This calls for greater and enhanced cooperation between international law enforcement agencies, private sector companies, academia and other appropriate stakeholders.

Moreover, the initial uncertainly regarding the actors and motivations behind any particular cyber-attack calls for increased cooperation between the law enforcement, the CSIRT community and intelligence services.

The low impact of cryptomining attacks mean that not only are few complaints likely to be made to law enforcement, but those that are will likely may not be given a high priority. It is therefore essential that law enforcement works with the internet security industry to curtail this activity and restrict this source of criminal revenue.

Cybercrime reporting

Awareness campaigns to highlight the range of cybercrime threats and how to respond to them can be used to increase public knowledge and perception and lead to more and more accurate cybercrime reporting.

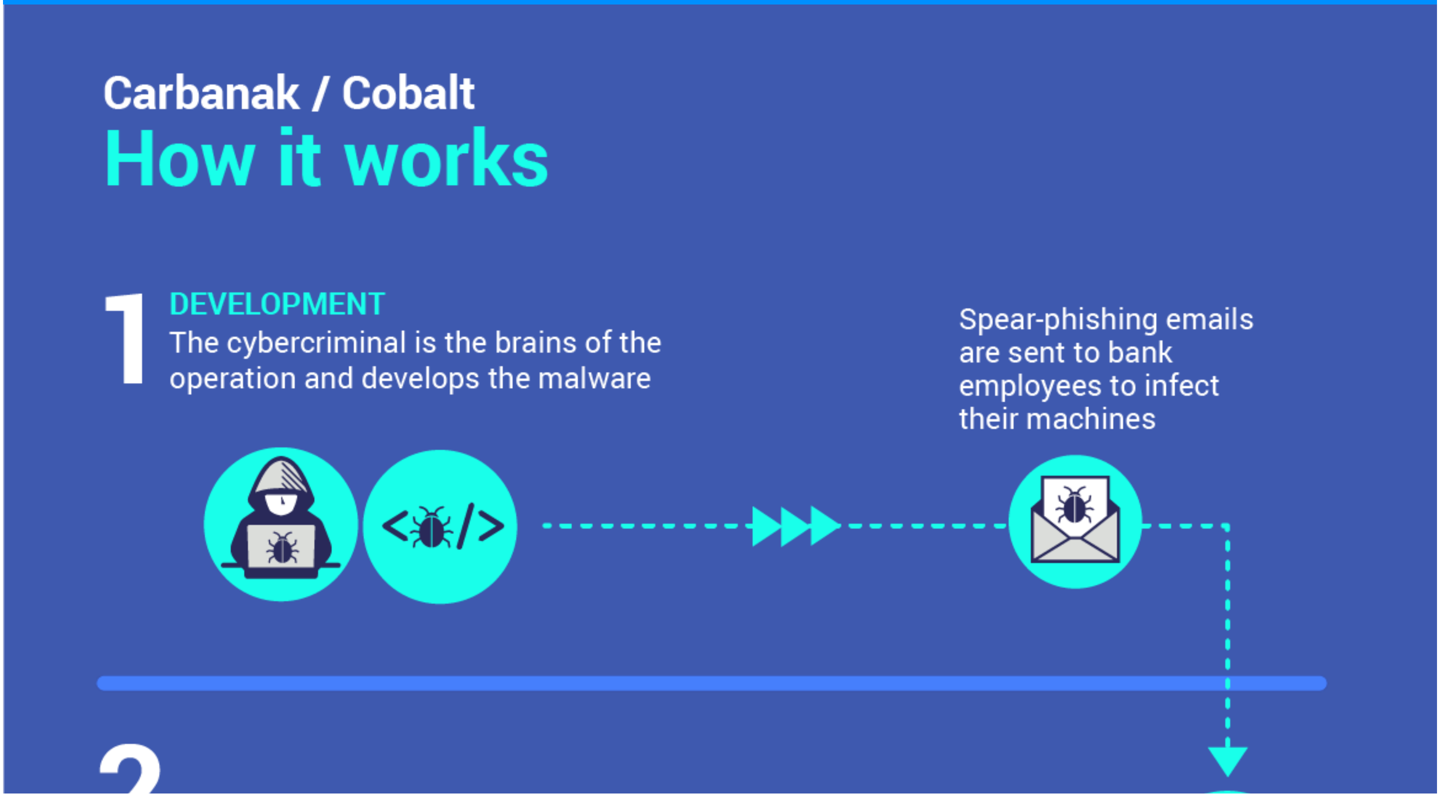
Law enforcement in each Member State should identify what implication the NIS directive will have in their country and plan accordingly, as it may result in a substantial increase in the reporting of network attacks.

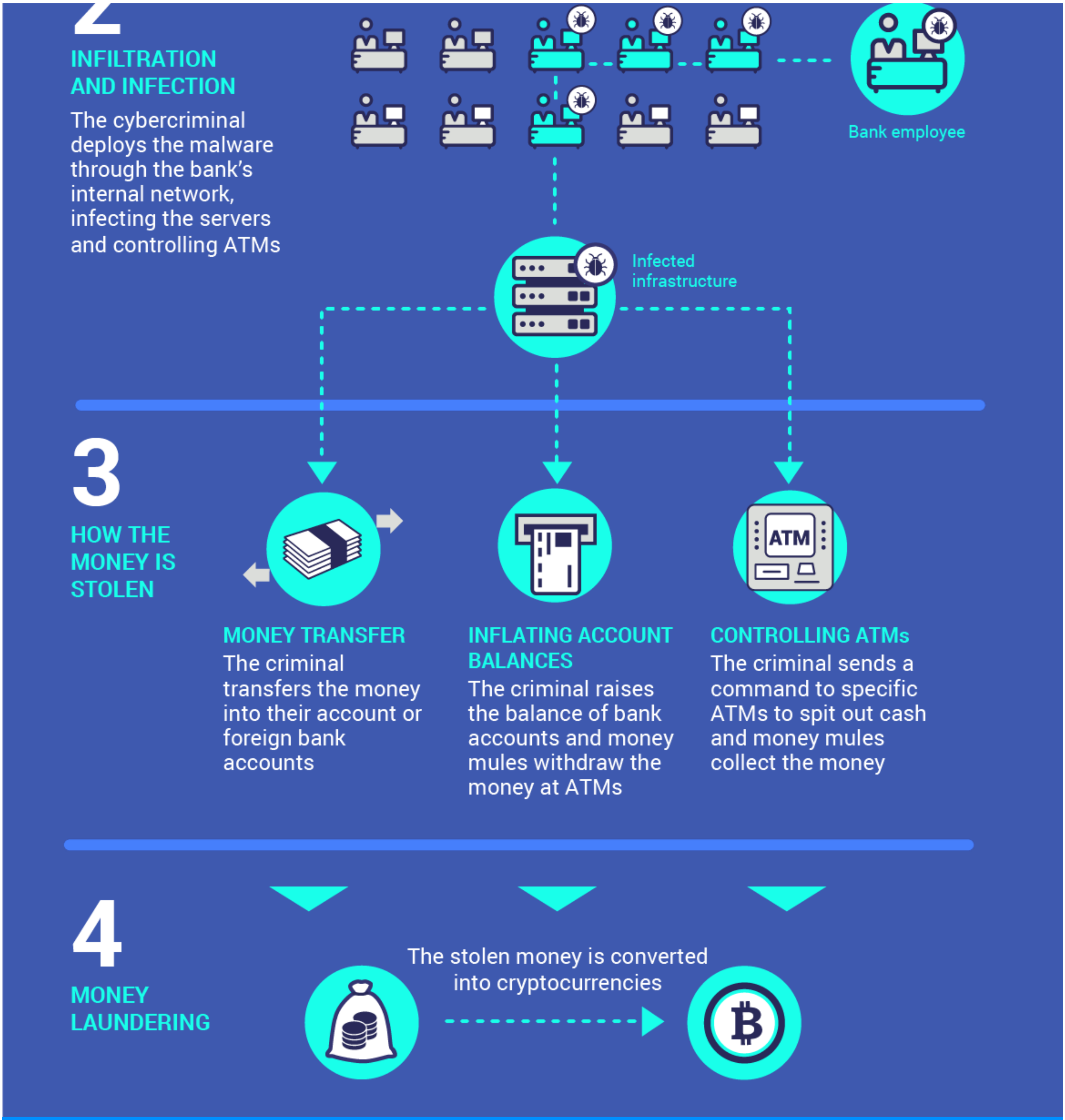
Investigation

To cope with a predicted growth in investigative and forensically challenging cyber-attacks, such as the use of fileless malware, law enforcement requires additional training, investigative and forensic resources in order to deal with increasingly complex and sophisticated cybercrime cases.

Law enforcement must continue to explore the investigative, analytic and policing opportunities arising from emerging technologies, such as artificial intelligence (AI) and machine learning. Such tools will become invaluable for dealing with modern crime and for intelligence led policing.

The growing number of affiliate programmes and as-a-service cyber-attacks (ransomware, DDoS, etc.) creates easy access to potentially highly-impactful cyber-attack tools to anyone who desires them. Therefore, law enforcement should focus on targeting cybercriminals offering cyber-attack services or products in order to make it harder for low level cybercriminals to carry attacks disproportionate to their skills.


Carbanak / Cobalt
How it works
1
DEVELOPMENT
The cybercriminal is the brains of the operation and develops the malware
Spear-phishing emails are sent to bank employees to infect their machines
2



2

INFILTRATION AND INFECTION

The cybercriminal deploys the malware through the bank’s internal network, infecting the servers and controlling ATMs

3

HOW THE MONEY IS STOLEN

MONEY TRANSFER

The criminal transfers the money into their account or foreign bank accounts

INFLATING ACCOUNT BALANCES

The criminal raises the balance of bank accounts and money mules withdraw the money at ATMs

CONTROLLING ATMs

The criminal sends a command to specific ATMs to spit out cash and money mules collect the money

4

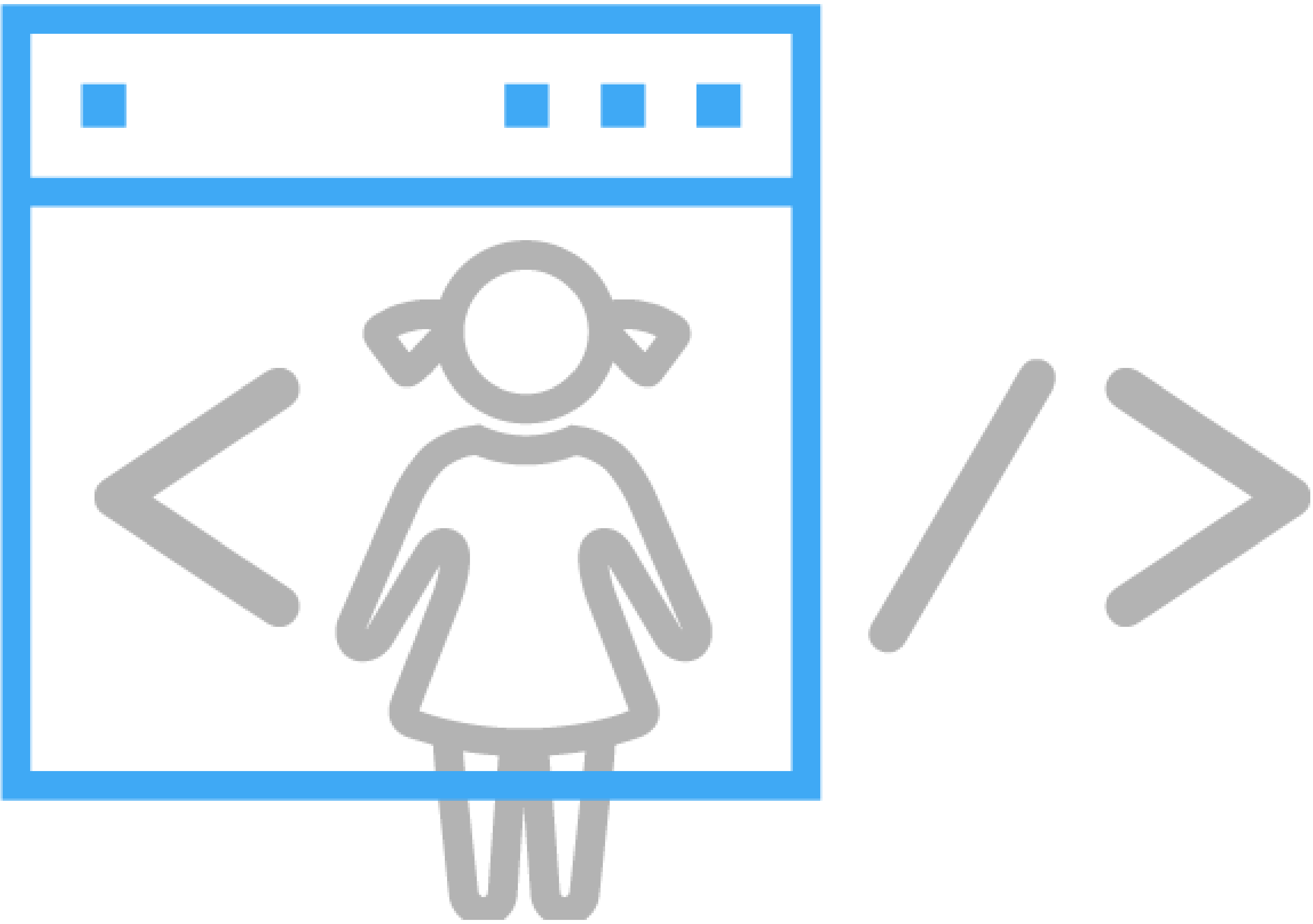
MONEY LAUNDERING

The stolen money is converted into cryptocurrencies

Read more:

The No More Ransom Project
Cyber Crime versus Cyber Security: what will you choose?
Five arrested for spreading ransomware throughout Europe and US
Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain

CRIME PRIORITY: CHILD SEXUAL EXPLOITATION ONLINE



Online child sexual exploitation (CSE) continues to be the worst aspect of cybercrime. Whereas child sexual abuse existed before the advent of the internet, the online dimension of this crime has enabled offenders to interact with each other online and obtain Child Sexual Exploitation Material (CSEM) in volumes that were unimaginable ten years ago. The growing number of increasingly younger children with access to internet enabled devices and social media enables offenders to reach out to children in ways that are simply impossible in an offline environment. This trend has considerable implications for the modi operandi in the online sexual exploitation of children.

Key findings

- The amount of detected online Child Sexual Exploitation Material continues to grow, creating serious challenges for investigations and victim identification efforts.
- As technologies are becoming easier to access and use, the use of anonymisation and encryption tools by offenders to avoid law enforcement detection is more and more common.
- Children increasingly have access to the internet and social media platforms at a younger age, resulting in a growing number of cases of online sexual coercion and extortion of minors.
- Live streaming of child sexual abuse remains a particularly complex crime to investigate. Streaming of self-generated material has significantly increased.

RECOMMENDATIONS

Cooperation

Tackling online CSE requires cooperation with the private sector, civil society and academia. Cooperation with the private sector – in particular internet service providers – can help to limit access to online CSEM and to divert potential offenders from consuming CSEM to seeking help with their sexual preferences.

Alternative responses to the threat of CSE are crucial to effectively tackle this issue. One alternative method would be to provide support to persons with a sexua interest in children who have the capacity to control their tendency to offend. An initiative in this regard is the website helplinks.eu, which provides a collection of links for help and prevention in countries worldwide.

It is crucial that law enforcement continue to work together with payment companies to limit the ability for online CSEM, especially LDCA. An example of such efforts is the European Financial Coalition against Commercial Sexual Exploitation of Children Online (EFC). Several major credit card companies have been successful in limiting the use of their services to pay for child sexual abuse and exploitation. Such approaches should be expanded to other types of commonly used payments methods.

Investigation

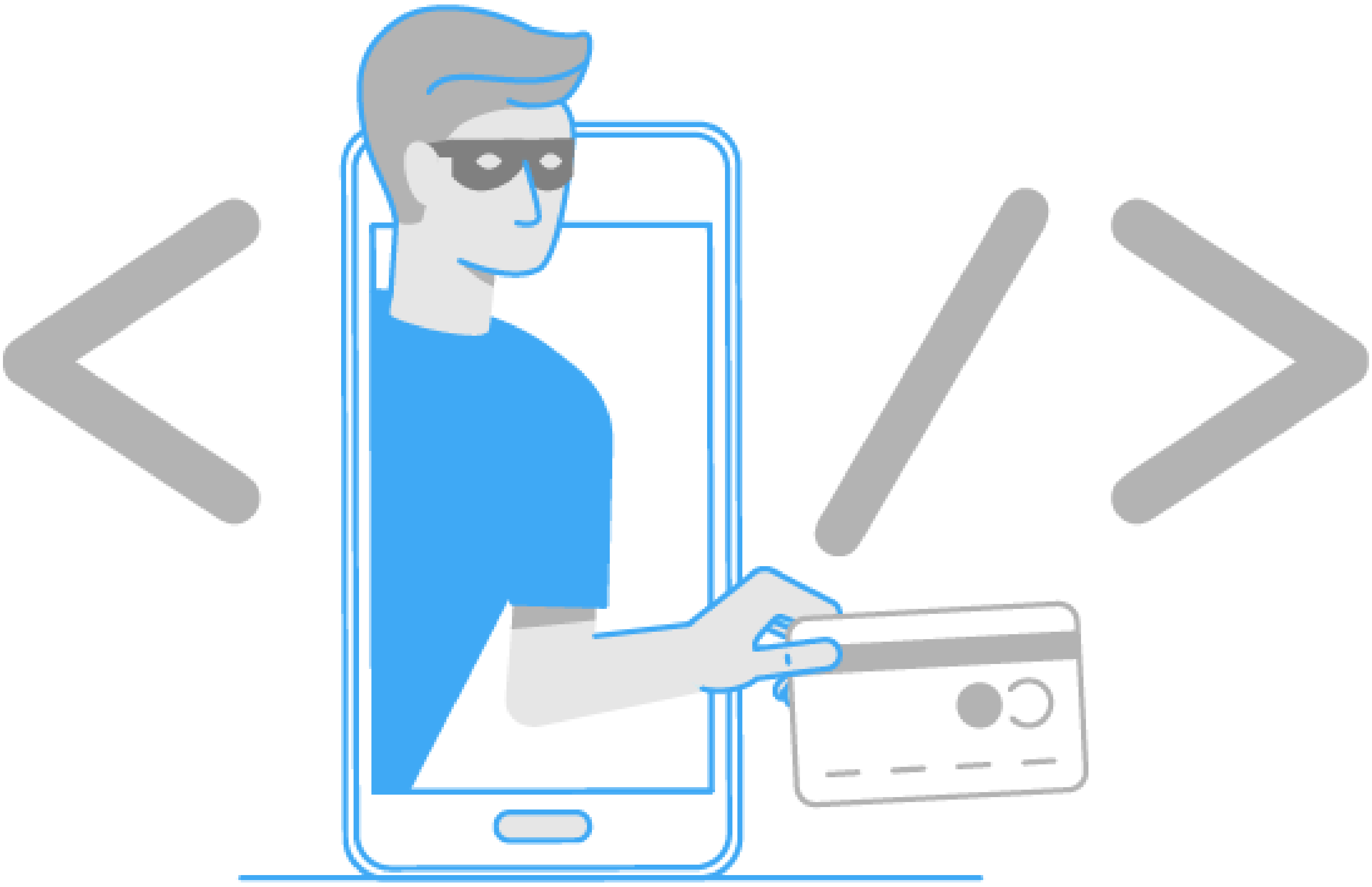
For an effective use of limited resources, investigations into online CSE should be aimed at high-value targets, such as administrators of large online forums who promote operational security. Europol should assist Member States and third partners in the identification of such key individuals.

Prevention and awareness

Education initiatives and standardised EU-wide prevention and awareness campaigns – such as Europol's Say No Campaign – are of crucial importance in reducing the risk of children falling victim to online solicitation or sexual coercion and extortion. Such initiatives should look to include younger children.

Read more:
Online sexual coercion and extortion – Say No! Campaign
Online resources for those with a sexual interest in children – Helplinks.eu
Stop Child Abuse – Trace an Object
Eight arrested for distribution of child sexual abuse material through skype and the darknet

CRIME PRIORITY: PAYMENT FRAUD



This chapter covers areas of payment fraud which are considered well known as they have been reported on in previous editions as well as new developments in the area of payment fraud. New is a relative concept since criminals generally vary their existing modus operandi. Such variations, however, do introduce different threats. Therefore, well-known and new developments are included in a complementary manner, based both on what law enforcement agencies have witnessed in their investigations as well as what private sector parties have observed.

Key findings

- The threat from skimming continues and shall do as long as payment cards with magnetic stripes continue to be used.
- The abuse of PoS terminals is taking on new forms: from manipulation of devices to the fraudulent acquisition of new terminals.
- Telecommunications fraud is a well-established crime but a new challenge for law enforcement.

RECOMMENDATIONS

While not a new threat, telecommunications fraud may represent a new crime area for many law enforcement agencies. Investigating these crimes will require additional training and close collaboration with the telecommunication industry.

Law enforcement and private industry should seek to engage in the growing number of join action days successfully tackling fraud involving non-cash payments. Global Airline Action Days, e-Commerce Actions and European Money Mule Actions (EMMA), all rely on close cooperation and collaboration between law enforcement and the private sector and the greater numbers of participants only adds to their success.

Despite the likelihood that further EMV adoption will result in the transference of more card fraud to CNP, implementation of EMV should continue.

Read more:
Online scammers captured after causing EUR 18 million of damage in more than 35.000 cases
141 arrested in worldwide crackdown on airline fraud
#2good2btrue: beware of the criminals out to ruin your holidays
Europol brings together three regions of the world to tackle payment card fraud

CRIME PRIORITY: ONLINE CRIMINAL MARKETS

Illicit online markets, both on the surface web and on the dark web, provide criminal vendors the opportunity to purvey all manner of illicit commodities, with those of a more serious nature typically found deeper, in the dark web. Many of these illicit goods and services, such as cybercrime toolkits or fake documents, are enablers for further criminality.

Key findings

- The Darknet market ecosystem is extremely unstable. While law enforcement shut down three major marketplaces in 2017, at least nine more spontaneously closed or exit scammed.
- The almost inevitable closure of large, global Darknet marketplaces has led to an increase in the number of smaller vendor shops and secondary markets catering to specific language groups or nationalities.

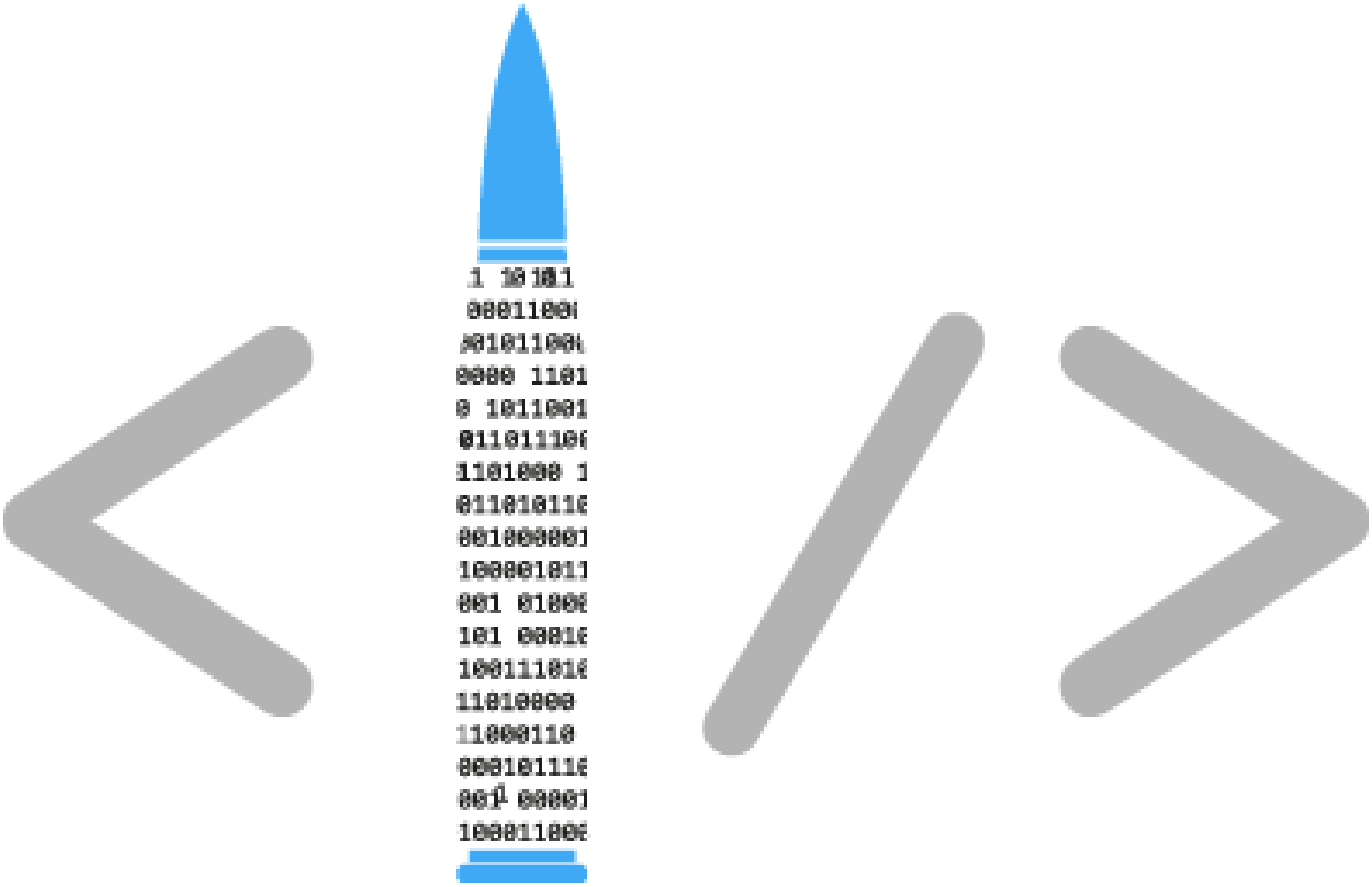
RECOMMENDATIONS

Criminality on the dark web spans multiple areas and involves a wide range of criminal commodities. An effective countermeasure will therefore require a suitably coordinated, cross-cutting response, involving investigators with equally diverse expertise. This will require additional capacity building and training of officers not involved in computer crime.

There is a need for a global strategy to address the abuse of the dark web and other emerging platforms for illicit trade.

Read more:
Europol establishes dedicated Dark Web Team
Joint action day targets counterfeiters on the darknet
Biggest hit against online piracy: over 20.520 internet domain names seized for selling counterfeits

THE CONVERGENCE OF CYBER AND TERRORISM



The Islamic State's (IS) loss of territory from 2016 to 2017 did not equate to a loss of authority among its followers or a manifest decrease in its ability to inspire attacks. Instead, the group continues to use the internet to promote its doctrine and inspire acts of terrorism. In many ways, military defeat has made the internet even more important for the IS; the difference being that it has since shifted from using it to support its state-building ambitions toward inspiring and attempting to direct terrorist attacks in the West.

Key findings

- Islamic State continues to use the internet to spread propaganda and to inspire acts of terrorism.
- Law enforcement and industry action has pushed IS sympathisers into using encrypted messaging apps which offer private and closed chat groups, the dark web, or other platforms which are less able or willing to disrupt their activity.
- While IS sympathisers have demonstrated their willingness to buy cyber-attack tools and services from the digital underground, their own internal capability appears limited.

RECOMMENDATIONS

Terrorist groups continue to abuse online platforms and social networking tools, distributing propaganda material in their efforts to recruit, fundraise and organise attacks. In doing so, they make use of legitimate services (e.g. purchasing hosting services and downloading available social media platforms) and continue to innovate in their bid to evade detection, develop their technical capabilities and raise funds via cryptocurrencies.

While it is impossible to completely eradicate terrorist propaganda from the internet, it is possible to minimise its impact. With this in mind, two separate but interlinked strategies must be deployed:

The first focus should be on countering terrorist groups' online propaganda and recruitment operations. This will require closer coordination and information-sharing across law enforcement agencies and enhanced cooperation from the private sector. In particular, Online Service Providers (OSPs) should develop their own capacity and share best practises amongst themselves in order to restrict access to hateful and dangerous messages.

The second must focus on the groups' ability to carry out cyber-attacks.

The two strategies reinforce each other: disrupting propaganda will hinder terrorists' access to human expertise, funding and cyber tools; similarly thwarting cyber-attacks will help limit the groups' attractiveness to potential recruits.Links

Read more:

Islamic State propaganda machine hit by law enforcement in coordinated takedown action
Europol's EU Internet Referral Unit partners with Belgium, France and the Netherlands to tackle online terrorist content
EU law enforcement and Google take on terrorist propaganda in latest Europol Referral Action Days

CROSS-CUTTING CRIME FACTORS

Cross-cutting crime factors are those which impact, facilitate or otherwise contribute to multiple crime areas but are not necessarily inherently criminal themselves. This includes topics such as methods of communication, financing, encryption, IoT and social engineering. In this chapter we will also address common challenges faced by EU law enforcement.

Key findings

- West African fraudsters have evolved to adopt emerging fraud techniques, including those with more sophisticated, technical aspects, such as business email compromise.
- Phishing continues to increase and remains the primary form of social engineering. Although only a small proportion of victims click on the bait, one successful attempt can be enough to compromise a whole organisation.
- Many of the classic scams, such as technical support scams, advanced fee fraud and romance scams still result in a considerable numbers of victims.
- An increase in HTTPS encryption protocol by phishing sites misleads victims into thinking a website is legitimate and secure.
- Cyber-attacks which historically targeted traditional financial instruments are now targeting businesses and users of cryptocurrencies.
- While Bitcoin's share of the cryptocurrency market is shrinking, it still remains the predominant cryptocurrency encountered in cybercrime investigations.
- A combination of legislative and technological developments, such as 5G and the redaction of WHOIS, will significantly inhibit suspect attribution and location for law enforcements and security researchers.

RECOMMENDATIONS

The most effective defence against social engineering is the education of potential victims. Law enforcement should therefore continue to support prevention and awareness campaigns aimed at raising awareness in relation to these threats.

Many social engineering scams targeting EU citizens are carried out by West African organised crime groups (OCGs). In order to effectively tackle this threat requires stronger cooperation with West African states, including capacity building and training of law enforcement officers.

Prevention and awareness campaigns should be tailored to include advice on how users of cryptocurrencies can protect their data and wallets.

Investigators should identify and build trust relationships with any cryptocurrency related businesses operating in their jurisdiction, such as exchangers, mining pools or wallet operators.

Member States should increasingly invest or participate in appropriate specialist training and investigative tools in order to grow their capacity to effectively tackle issues raised by cryptocurrencies during investigations. Investigating cryptocurrencies must become an integral skill for cybercrime investigators.

EN Internet Organised Crime Threat Assessment (IOCTA) 2018 [11.66 MB]

CRIME AREAS:	Cybercrime
ENTITIES:	European Cybercrime Center (EC3)
TARGET GROUPS:	

General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

Source URL: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018#comment-0