IOCTA

INTERNET ORGANISED CRIME THREAT ASSESSMENT

2018

EUROPOL

EC3
European Cybercrime Centre

IOCTA
2018

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2018

www.europol.europa.eu

ISBN 978-92-95200-94-4
DOI 10.2813/858843
QL-AL-18-001-EN-N

contents

foreword

It is my pleasure to introduce the 2018 Internet Organised Crime Threat Assessment (IOCTA), which has been and continues to be one of the flagship strategic products 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. This report embodies Europol's keywords: trust, sharing and cooperation.

> **Only if law enforcement, the private sector and the academic world work together closely, can cybercrime be combated effectively.**

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 criminal gains and the facilitation of other crimes, as well as significant financial losses for citizens and financial institutions alike. 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. The fight against this heinous crime must continue unabated. After all, every child, wherever they are in the world, has the right to grow up in a safe environment.

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

abbreviations

ACS Automated Card Shop

AI Artificial Intelligence

APT Advanced Persistent Threat

APWG Anti-Phishing Working Group

ASCS Australian Cyber Security Center

ATM Automated Teller Machine

BEC Business Email Compromise

ccTLD country code Top Level Domains

CAV Counter Anti-Virus

CEO Chief Executive Officer

CERT Computer Emergency Response Team

CNP Card-Not-Present

CSEM Child Sexual Exploitation Material

CSE Child Sexual Exploitation

CSIRT Computer Security Incident Response Team

CTB Curve-Tor-Bitcoin

DDoS Distributed Denial of Service

DEA United States Drug Enforcement Agency

DPA Data Protection Agency

DSP Digital Service Providers

EBF European Banking Federation

EC3 European Cybercrime Centre

EMCDDA European Monitoring Centre for Drugs and Drug Addiction

EMMA European Money Mule Actions

EMPACT European Multidisciplinary Platform Against Criminal Threats

EMV Europay, MasterCard and Visa

ENISA European Union Agency for Network and Information Security

EK Exploit Kits

EPC European Payment Council

EPT Electronic Payment Terminal

EUCTF European Cybercrime Task Force

FSAG (Europol) Financial Services Advisory Group

FBI United States Federal Bureau of Investigation

GAAD Global Airport Action Days

GDPR General Data Protection Regulation

GPS Global Positioning System

GSMA Global System for Mobile Communications Association

gTLD Generic Top Level Domain

HTTPS HyperText Transfer Protocol Secure

I2P Invisible Internet Project

ICANN Internet Corporation for Assigned Names and Numbers

ICS Industrial Control Systems

ICT Information and Communications Technology

IOCTA Internet Organised Crime Threat Assessment

IOS In Our Sites

IoT Internet of Things

IP Internet Protocol

IPC^3 Intellectual Property Crime Coordinated Coalition

IRSF International Revenue Share Fraud

IS Islamic State

ISAG (Europol) Internet Security Advisory Group

ISP Internet Service Provider

IVTS Informal Value Transfer System

IWF Internet Watch Foundation

J-CAT Joint Cybercrime Action Taskforce

KYC Know Your Customer

LDCA Live Distant Child Abuse

NCMEC National Center for Missing and Exploited Children

NIS Network and Information Systems

NSA National Security Agency

OCG Organised Crime Group

OES Operators of Essential Services

OSP Online Service Providers

P2P Peer to Peer or People to People

PBX Private Branch Exchange

PITA Pacific Island Telecommunication Association

PoS Point of Sale

PSD Payment Services Directive

RAMP Russian Anonymous Marketplace

RAT Remote Access Trojan

RDP Remote Desktop Protocols

RIG EK RIG Exploit Kit

SCADA Supervisory control and data acquisition

SEPA Single Euro Payments Area

SGEM Self-Generated Explicit Material

SIENA Secure Information Exchange Network Application

SMS Short Message Service

SSL Secure Sockets Layers

SWIFT Society for Worldwide Interbank Financial Telecommunications

Tor The Onion Router

TPP Third Party Provider

URL Uniform Resource Locator

VPN Virtual Private Network

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.

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, a significant volume of 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.

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 significant increase in the amount of SGEM live streamed on these platforms.

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 (second only to malware in 2017); it is also becoming more accessible, low-cost and low-risk.

Card-not-present fraud dominates payment fraud but skimming continues

Skimming remains a common issue in most of the EU Member States. However, 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, card-not-present 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 to fund 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 victims 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.

Social engineering still the engine of many cybercrimes

The significance of social engineering for cyber-dependent and cyber-enabled crime continues to grow. Phishing via email remains the most frequent form of social engineering, with vishing (via telephone) and smishing (via SMS) 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.

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's systems. Actual cryptomining malware works to the same effect, but can cripple a victims system by monopolising their processing power.

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.

01_ key findings

Cyber-dependent crime

- 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 Remote Desktop Protocol (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.

Child sexual exploitation online

- 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.

Payment fraud

- 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.

Online criminal markets

- The Darknet market ecosystem is extremely unstable. While law enforcement shut down three major marketplaces in 2017, at least nine more closed either spontaneously or as a result of their administrators absconding with the market's stored funds.
- 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.

The convergence of cyber and terrorism

- Islamic State (IS) 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.

Cross-cutting crime factors

- West African and other 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.
- 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 the attribution and location of suspects for law enforcements and security researchers.

2 recommendations

Cyber-dependent crime

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

Cryptomining attacks may have minimal impact on their victims, resulting in few complaints made to law enforcement. Those which are reported may also 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 cyber-attacks which are challenging in terms of both investigation and forensics, 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.

Child sexual exploitation online

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 sexual 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 live-distant child abuse (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 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.

Payment fraud

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 increasing 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.

Online criminal markets

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 an international strategy to address the abuse of the dark web and other emerging platforms for illicit trade.

The convergence of cyber and terrorism

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 should 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.

Cross-cutting crime factors

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). Tackling 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 a core skill for cybercrime investigators.

3_introduction

The Internet Organised Crime Threat Assessment (IOCTA) aims to inform decision-makers at strategic, policy and tactical levels in the fight against cybercrime, with a view to directing the operational focus for EU law enforcement. The 2018 IOCTA will contribute to the setting of priorities for the 2019 EMPACT operational action plan in the three sub-areas of the cybercrime priority: cyber-attacks, payment fraud and child sexual exploitation online, as well as cross-cutting crime enablers.

Scope

The 2018 IOCTA focuses on the trends and developments pertinent to the above-mentioned priority crime areas. In addition to this, the report will discuss other cross-cutting factors that influence or impact the cybercrime ecosystem, such as criminal use of the Darknet and social engineering. The report will also examine some of the common challenges to law enforcement.

This report provides an update on the latest trends and the current impact of cybercrime within Europe and the EU. Each chapter provides a law enforcement centric view of the threats and developments within cybercrime, based predominantly on the experiences of cybercrime investigators and their operational counterparts from other sectors. It draws on contributions from more strategic partners in private industry and academia to support or contrast this perspective. The reports seeks to highlight future risks and emerging threats and provides recommendations to align and strengthen the joint efforts of EU law enforcement and its partners in preventing and fighting cybercrime.

Methodology

The 2018 IOCTA was drafted by a team of Europol analysts and specialists drawing predominantly on contributions from Member States, the European Union Cybercrime Taskforce (EUCTF), Europol's Analysis Projects Cyborg, Terminal and Twins and EC3's Cyber Intelligence Team, via structured surveys and interviews. This has been enhanced with open source research and input from the private sector, namely EC3's Advisory Groups on Financial Services, Internet Security and Communication Providers. These contributions have been essential to the production of the report.

Acknowledgements

Europol would like to extend thanks to all law enforcement and private sector partners who contributed to this report, in particular the European Banking Federation (EBF) and the EC3's Academic Advisory Network.

4_

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[1]. 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.

4.1 / Key findings

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 remote desktop protocol (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.

4.2 / Malware

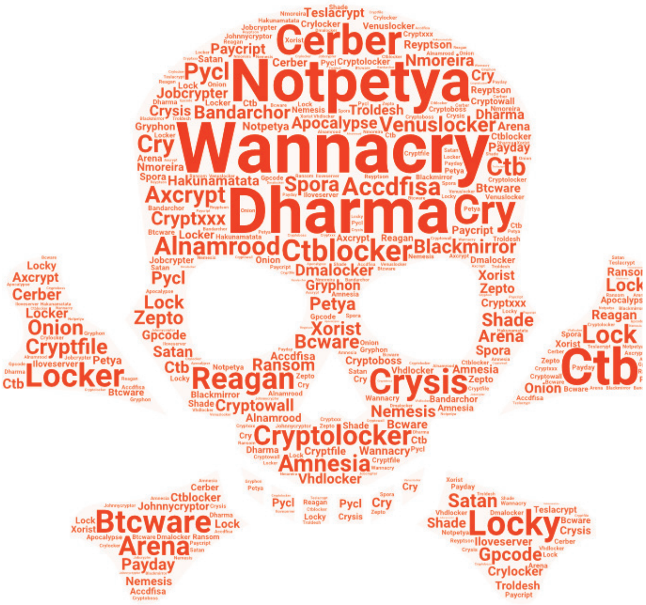
Ransomware dominates reporting across the board

From law enforcement to media and from the security industry to the financial sector[2], ransomware dominated reporting across the board throughout 2017. The WannaCry and NotPetya attacks of mid-2017 were of an unprecedented global scale, affecting an estimated 300 000 victims worldwide, in over 150 countries, with the WannaCry attacks alone estimated to have cost global economies in the region of USD 4 billion[3]. Within the EU, the attacks affected a wide range of key industries and critical infrastructures including health services, telecommunications, transport and manufacturing industries. Later in the year, the Bad Rabbit ransomware hit over 200 victims in Russia and Eastern Europe, again affecting critical infrastructures such as healthcare, transport and financial sectors[4].

These attacks were notable for a variety of reasons. Firstly, according to public reports, their origins are strongly suspected to be the acts of Advanced Persistent Threat (APT) groups associated with nation states and not financially motivated criminals. All three attacks also leveraged one or more of the NSA exploits leaked by the Shadow Brokers group in April 2017[5]. Lastly, all incorporated some self-replicating worm functionality, which accounted for the speed and spread of the infections.

While there continues to be a global coordinated response to these specific attacks, European law enforcement reports ransomware attacks from a wide range of other ransomware families. The most commonly reported ransomware families are Cerber, Cryptolocker, Crysis, Curve-Tor-Bitcoin Locker (CTB-Locker), Dharma and Locky. With the exception of Dharma, for which decryption keys are now available[6], all of these were reported in previous years. Member states reported a wide range of other ransomware families, but in fewer instances and dispersed across Europe.

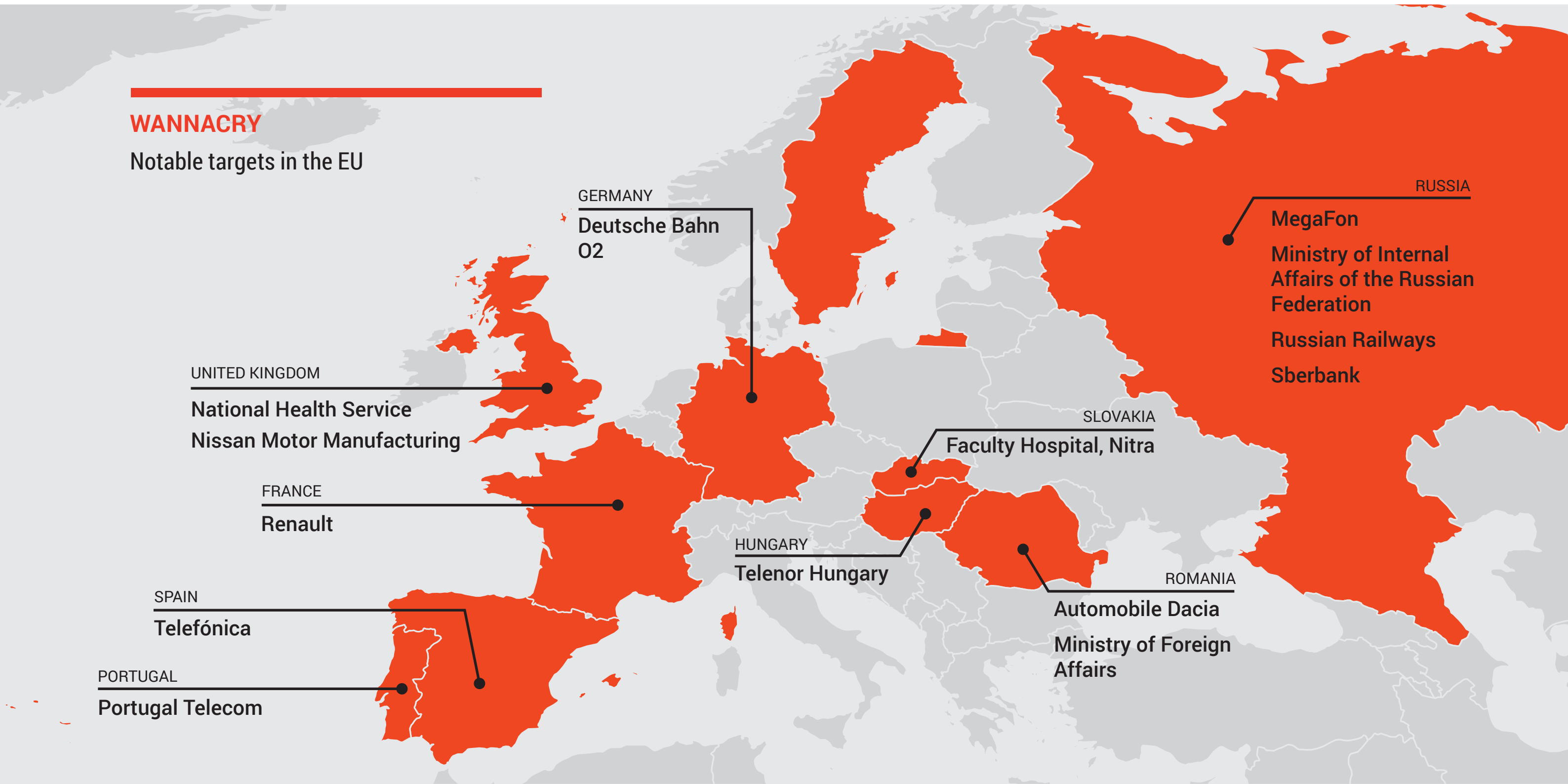
Overall damages arising from ransomware attacks are difficult to calculate, although some estimates suggest a global loss in excess of USD 5 billion in 2017[7]. In comparison, other reporting suggests that over the past two years, 35 unique ransomware strains have earned cybercriminals USD 25 million, with Locky and its many variants accounting for more than 28% of that figure[8]. This highlights the huge disparity between the losses to victims, compared to the actual criminal revenue generated.



In December 2017 Romanian authorities arrested three individuals suspected of infecting computer systems by spreading the CTB-Locker ransomware. Two further suspects from the same criminal group were also arrested in Bucharest in a separate, parallel ransomware investigation linked to the US.

The group spread the malware using spam drafted to look like it was from well-known companies in countries like Italy, the Netherlands and the United Kingdom (UK). Each email had an attachment, often in the form of an archived invoice, which contained a malicious file, which, once opened on a Windows system, would allow the malware to encrypt files on the infected device.

The operation was supported by the Dutch National High-Tech Crime Unit, the National Crime Agency in the UK, the FBI and Europol's EC3 and the Joint Cybercrime Action Taskforce (J-CAT).



Ransomware attacks may move from random to targeted

In some Member States attacks appear to remain largely untargeted, affecting citizens and businesses alike; this is perhaps the result of “scattergun” attacks by those engaging ransomware-as-a-service, or those with affiliate programmes, such as Cerber, which allegedly allows its authors to sustain an income of USD 200 000 per month[9]. Some other Member States report that campaigns are customised or tailored to specific companies or individuals, suggesting a more organised or professional attack.

As we have seen with other cyber-attacks, as criminals become more adept and the tools more sophisticated yet easier to obtain, fewer attacks are directed towards citizens and more towards small businesses and larger targets, where greater potential profits lie.

In March 2018 Polish National Police, in close cooperation with the Belgian Federal Police and Europol, arrested a Polish national, known online as “Armaged0n”. He was suspected of having encrypted several thousands of computers belonging to Polish companies between 2013 and 2018 using ransomware spread via email correspondence pertaining to be from well-known companies, such as telecommunication providers, retailers, banks, etc. Criminals offered a decryption key to the victims in return for a ransom payment between USD 200 and 400. The suspect carried out such online campaigns on average every three to four weeks.

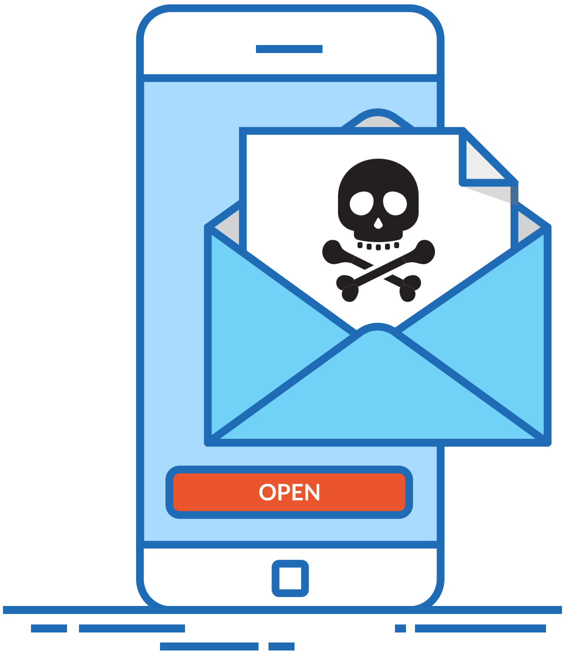
In addition to spreading ransomware, the suspect also infected computer systems with a virus which stole bank account login credentials. The suspect then wired money online to accounts he controlled, subsequently using prepaid payment cards to cash out the profits. The Polish National Police subsequently developed a decryption tool for the ransomware spread by “Armaged0n”.

5 year flashback

In the 2014 IOCTA report, while over half of EU law enforcement had encountered ransomware, this related on the whole to police ransomware, without encryption. Cryptoware was only just emerging with sporadic cases of Cryptolocker. By 2015 cryptoware had become a top emerging threat for EU law enforcement, although non-encrypting police ransomware still accounted for a significant proportion of ransomware cases. By 2016 police ransomware had all but vanished, except for on mobile devices, superseded by a growing variety of cryptoware. By 2017 the number of ransomware families had exploded, their impact significantly overshadowing other malware threats such as banking Trojans. Industry reported that ransomware damages had increased fifteen-fold over the previous two years[10].

Financial malware plays a less prominent role in law enforcement reporting

As ransomware continues to dominate law enforcement efforts, the reported number of cases of banking Trojans and other financial malware remains comparatively low. Mirroring this, industry reporting also contains noticeably less focus on financial malware, in some instances eschewing it altogether. While fewer than one quarter of Member States reported a significant number of cases of financial malware, the financial sector maintains that such attacks are still a substantial threat[11]. Law enforcement reported cases of malware such as Carbanak, Dridex, Emotet, Tinba and Trickbot, although there was a clear geographical bias in terms of which variants were targeting which jurisdiction. For once there was notable overlap between law enforcement and industry observations, with Dridex, Emotet, Tinba and Trickbot also featuring frequently in industry reporting, alongside older malware such as Ramnit (a top threat for British law enforcement in 2016) and various Zeus variants.



Mobile malware absent in law enforcement reporting, but industry reports growing volume

Mobile malware did not feature with any prominence in law enforcement reporting in 2017. Only one Member State reported a small, yet increasing number of cases. This may be explained by some industry reporting which indicates that mobile malware activity is concentrated in Africa, Asia and the USA, with the exception of mobile ransomware which heavily targets North America[12]. On the whole, industry reports that the volume of new mobile malware families has grown significantly throughout in 2017, in particular mobile ransomware[13],[14].

Victims of mobile malware are more likely to approach their provider in relation to problems with their device than to report it to the police.

This contrast in picture between law enforcement and industry may also emphasise the continued lack of awareness within the populace on how to react to an attack on their mobile device, with few victims reporting the attack to the police.

Remote access trojans

There continues to be a general decline in cases involving Remote Access Trojans (RATs), with just over one fifth of Member States reporting cases, compared to one third in the previous report. Those that do, however, highlight the use of RATs primarily to attack networks and companies in both the public and private sector rather than private citizens, for the purpose of data theft, extortion, malware dropping or making unauthorised financial transactions.

In September 2017 an operation led by British law enforcement and supported by Europol's EC3 and over a dozen law enforcement agencies in Europe, led to the disruption in the distribution of the RAT Luminosity Link. The investigation uncovered a network of individuals who supported the distribution and use of the RAT across 78 countries and sold it to more than 8 600 buyers via a website dedicated to hacking and the use of criminal malware.

Once installed upon a victim's computer, a user of the RAT Luminosity Link was free to access and view documents, photographs and other files, record all the keystrokes entered and even activate the webcam on the victim's computer – all of which could be done without the victim's knowledge.

Cryptocurrency miners

Cryptojacking is a relatively new term which refers to any process that uses the processing power or bandwidth of a device to mine cryptocurrencies without the user's permission.

In many cases, this is achieved through a script running within a website that, via the visitor's browser, allows the website to harness the visitors processing power to mine cryptocurrencies during their visit. Typically Monero is mined as it does not share Bitcoin's heavy processor requirements. Brought to light by the CoinHive JavaScript miner, the script was initially intended to allow content providers to generate some income without relying on intrusive advertising. While this activity is not illegal per se, it has since been exploited by financially motivated cybercriminals who hack legitimate websites to cryptojack users visiting those sites, with a number of significant attacks reported in the media in the latter part of 2017[15],[16],[17]. The phenomenon has grown such that by the last quarter of 2017, 2.2% of the top 100 000 sites listed by website-ranking resource Alexa were using cryptomining scripts[18].

True cryptomining malware can cause significant disruption

In addition to this form of cryptomining, there is 'true' cryptomining malware which is delivered as a malicious payload like any other malware. Such malware similarly uses the infected machines processing power to mine cryptocurrencies, although in this case Bitcoin is also mined, albeit often inefficiently due to the increasing processing power required to mine Bitcoins. The impact of this activity is however easier to detect. While law enforcement did not formally report any cases, there were again a number of incidents featured in the media such as the attack which resulted in healthcare systems in Finland grinding to a halt in February 2018[19].

On the whole, cryptomining attacks only featured anecdotally in law enforcement reporting throughout 2017. This is likely due to the fact that it is an emerging threat, but it may also be due to the questionable legality of the activity. In-browser cryptomining is not illegal. Moreover, while cryptomining malware may result in demonstrable criminal profits, the damages to victims (with some exceptions) are hard to quantify and difficult to investigate.

In contrast, industry reporting highlights an explosion in the volume of cryptominers (taking into account both varieties), such that in the latter part of 2017, it overshadowed almost all other malware threats[20],[21],[22]. Other reporting highlights huge cryptomining botnets[23] and even cryptomining malware operating on Supervisory control and data acquisition (SCADA) systems[24].

Infection vectors

Following on from last year's trends, the decline in use of exploit kits (EKs) as a primary infection continues; only a few Member States reported significant numbers of cases involving EKs. Where EK activity is noted, it typically refers to the RIG EK, which remains the dominant EK, albeit at a fraction of its former distribution[25],[26]. Other prominent EKs from 2017, such as Neutrino and Sundown, appear to have all but ceased activity. While earlier in 2017 the RIG EK was primarily delivering ransomware, many industry reports highlight that it has now shifted to delivering cryptomining malware[27],[28], which generates less risk, provides a steadier income and requires less victim engagement that ransomware.

Social engineering overtakes EK use

As highlighted in last year's report, attackers have instead turned to more consistent methods of infection, with email-based attacks such as spam and phishing (including targeted spear phishing) most commonly used to obtain an initial foothold on a victim's device[29]. Several Member States however also report the growing exploitation of RDPs as a means of installing malware. Criminals will scan the internet for specific open ports before attempting to brute force access to the victims RDP. The use of this technique is also stressed in some industry reporting[30].

In November 2017, the FBI, in close cooperation with German law enforcement, Europol's EC3 and J-CAT, Eurojust and private-sector partners, dismantled one of the longest running botnets in existence. The Andromeda botnet (also known as Gamarue) was associated with the distribution of over 80 malware families.

The international action targeted servers and domains which were used to spread the Andromeda malware. Overall, 1 500 domains of the malicious software were subject to sink-holing. During 48 hours of sink-holing, approximately 2 million unique Andromeda victim IP addresses from 223 countries were captured[31].

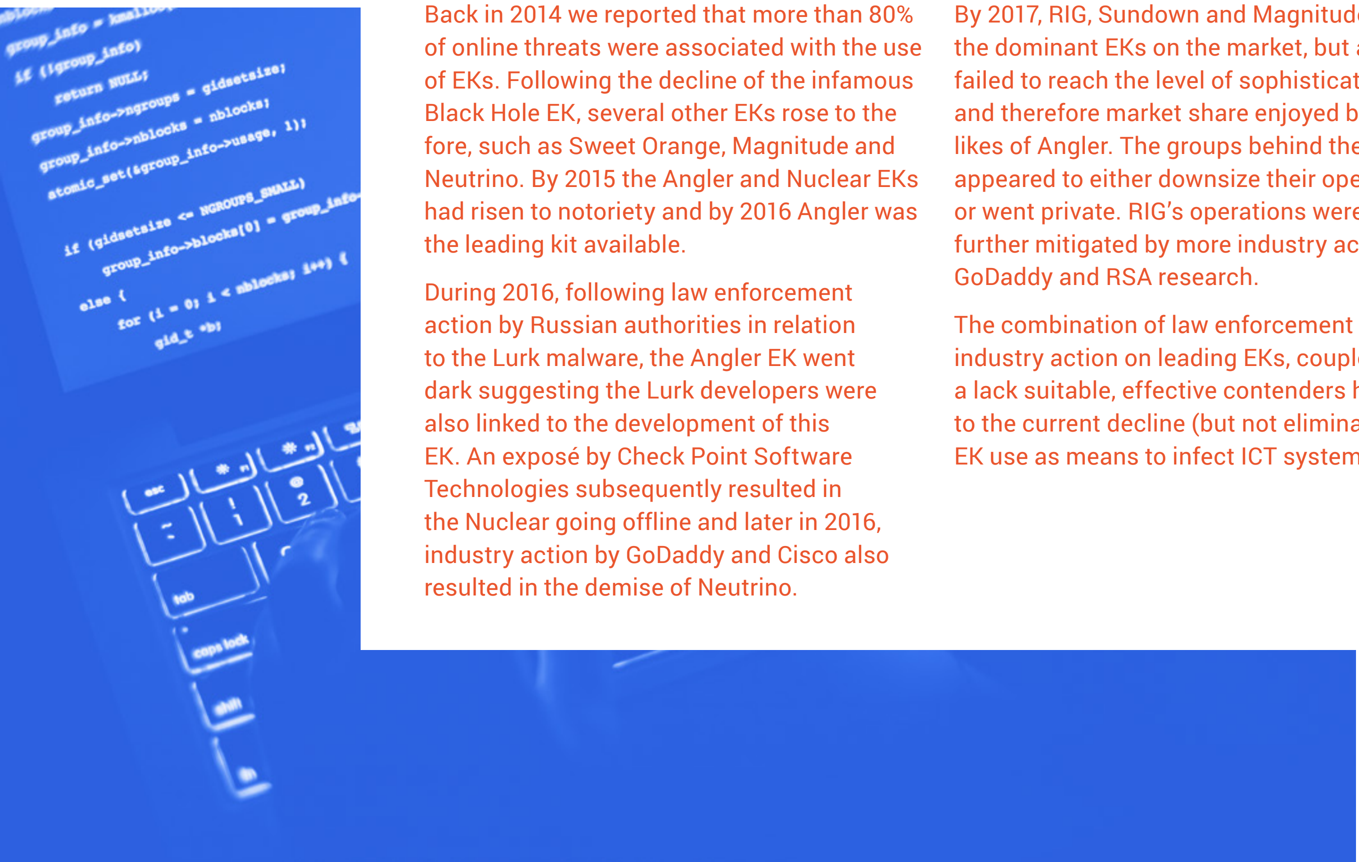
5 year flashback

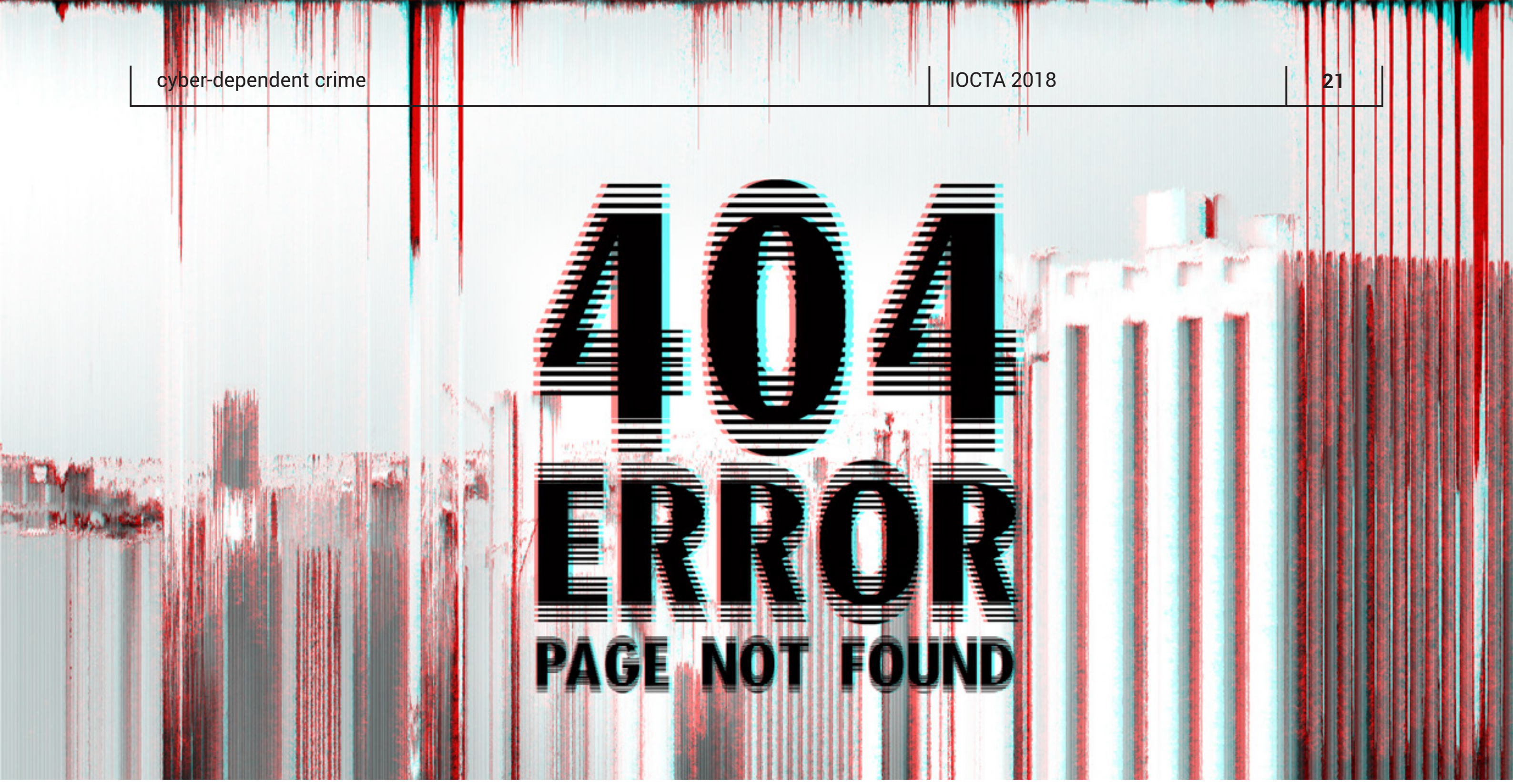
Back in 2014 we reported that more than 80% of online threats were associated with the use of EKs. Following the decline of the infamous Black Hole EK, several other EKs rose to the fore, such as Sweet Orange, Magnitude and Neutrino. By 2015 the Angler and Nuclear EKs had risen to notoriety and by 2016 Angler was the leading kit available.

During 2016, following law enforcement action by Russian authorities in relation to the Lurk malware, the Angler EK went dark suggesting the Lurk developers were also linked to the development of this EK. An exposé by Check Point Software Technologies subsequently resulted in the Nuclear going offline and later in 2016, industry action by GoDaddy and Cisco also resulted in the demise of Neutrino.

By 2017, RIG, Sundown and Magnitude were the dominant EKs on the market, but all failed to reach the level of sophistication and therefore market share enjoyed by the likes of Angler. The groups behind these kits appeared to either downsize their operations or went private. RIG's operations were further mitigated by more industry action by GoDaddy and RSA research.

The combination of law enforcement and industry action on leading EKs, coupled with a lack suitable, effective contenders has led to the current decline (but not elimination) in EK use as means to infect ICT systems.





4.3 / Attacks on critical infrastructure

Earlier we discussed the WannaCry, NotPetya and Bad Rabbit attacks during 2017. While not necessarily directly targeted, victims included several elements of industries from national critical infrastructures, namely those in the health, transport and telecommunications sectors.

One third of Member States reported cases involving attacks on critical infrastructures. Due to the varying nature of these attacks, it was not possible to highlight a particular modus operandi for the cases referred to law enforcement. However, the most frequently reported modus operandi did involve a malware component. Media reporting also highlights the use of DDoS as an attack vector, with DDoS attacks crippling train networks in Sweden as a consequence of an attack on two Swedish Internet Service Providers (ISPs)[32] and shutting down communications on the Finnish Åland Islands after a telecom provider was attacked.

The number of cases dealt with by EU law enforcement continues to be low. There are a number of likely contributing factors to the dearth of law enforcement reports, namely the possible or even probable source of such attacks, which is often suspected to be state-sponsored, condoned or otherwise not financially motivated. If such is the case, most subsequent investigations are likely to be outside of the remit of many law enforcement agencies and instead lying with those dealing with national security. While there are no prominent examples of this from within the EU, within Europe there are many news articles reporting Ukrainian national critical infrastructure being significantly disrupted[33].

> “
>
> Today attackers of ICS/SCADA systems analyse existing systems and try to find vulnerabilities to exploit. Finding new or unpatched vulnerabilities usually requires a thorough understanding of the target system and – in many cases – reconnaissance is tedious work. We anticipate that in future, attackers will strive to compromise the development and engineering phase of industrial systems to embed well-hidden vulnerabilities only known to them. It is therefore important to implement a secure development lifecycle in production systems engineering.
>
> *Dr Edgar Weippl, SBA Research, Austria*

4.4 / Data breaches and network attacks

Data is the lifeblood for almost any industry and consequently is not only a highly valued commodity in the digital underground, but the target of attacks aimed at illegally acquiring, destroying or denying access to that data. Industry reports that personal data is most commonly compromised, followed by payment data and then medical data[34].

This year's reporting highlights a number of ways attackers profit from gaining access to private networks. Over 55% of Member States report investigations into some form of network attack, other than DDoS attacks, which were notably more frequent. Moreover, almost half of these report that network attacks are being reported more frequently.

Network intrusions

When we look at the incidents reported to law enforcement, the most common apparent motive behind such attacks is the illegal acquisition of data, as reported by over one third of Member States. Data acquired in such a way was noted to be used for a number of purposes, depending on the nature of the data. Criminals often use stolen data to extort the victim to prevent its disclosure, particularly where it relates to intellectual property. In other instances, the data is used for the furtherance of other fraudulent activity, such as phishing or, in the case of payment card data, CNP fraud. However, in many cases the ultimate destination of such exfiltrated data is often unknown and difficult to determine.

The largest data breach in history continues to get worse

In each annual report we typically highlight data breaches disclosed that year which have had a significant impact, or are particularly newsworthy due to the scale of the breach. For the second year running, the breach at *Yahoo!* is the top reported data breach. While the breach actually occurred in 2013, as is often the case, the scale of the breach was not discovered until a later date. In the last issue we reported that the breach had affected over one billion customers, already the world's largest ever breach, but during 2017 it was disclosed that the breach actually affected all three billion customers[35].

Another prominent breach was at the credit report service *Equifax*. The breach affected 145.5 million customers, but while most of those were in the USA, it also affected over 15 million customers in the UK. No direct financial information was disclosed in either breach, however in both cases the disclosed data could be used to facilitate other criminal activity. The financial sector underlined data breaches as a key concern, as the data disclosed is a key source of personal information used to mount phishing campaigns on its customers[36].

Law enforcement also reported on intrusions with different motives, namely the perpetrator's desire to gain access to, or control of, internal systems and processes as a means to conduct other criminal activity. This may be access to internal email systems to carry out Business Email Compromise (BEC – also known as CEO fraud). Such access can also, depending on the technical capabilities of the attacker, allow the perpetrator to monitor and ultimately control internal systems, to, for example, facilitate remote ATM cash withdrawals[37]. Business process compromise is also an option once the perpetrator has gained access as they can make payments using internally accessed payment platforms such as SWIFT. Several Member States also report intrusions purely for the purpose of inflicting malicious damage, typically the destruction of business critical data. For some attackers, the victim's data is not the goal, but instead their infrastructure, with access to hacked servers sold on criminal markets.

In March 2018 the leader of the crime gang behind the Carbanak and Cobalt malware attacks targeting over 100 financial institutions worldwide was arrested in Alicante, Spain, after a complex investigation conducted by the Spanish National Police, with the support of Europol, the US FBI, the Romanian, Belarussian and Taiwanese authorities and private cyber security companies.

The gang began their activity in 2013, attacking banks, e-payment systems and financial institutions using malware of their own design, known as Carbanak and Cobalt. The criminal operation struck banks in more than 40 countries and has resulted in cumulative losses of over EUR 1 billion for the financial industry. The Cobalt malware alone allowed criminals to steal up to EUR 10 million per heist. All of these attacks began with a social engineering attack.

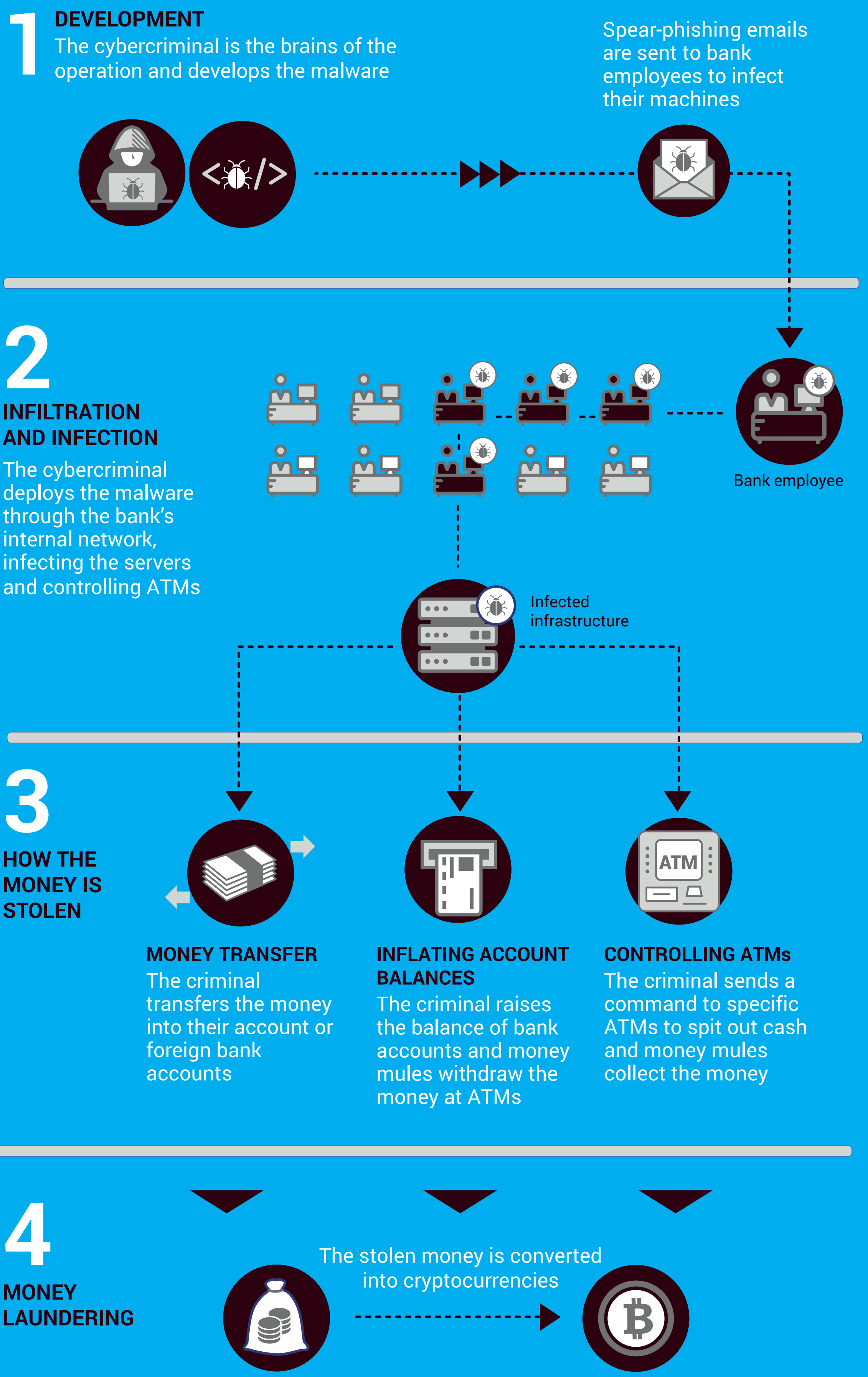
→ info-graphic

According to these reports, external malicious actors carry out 73% of breaches, but 28% also involved internal actors. OCGs carry out 50% of breaches, whereas industry reporting attributes 12% of the breaches to state sponsored actors. Cutting across these actor attributions, industry reporting indicates that 76% of all attacks are financially motivated[38].

Healthcare organisations are now the most targeted sector, accounting for 24% of breaches, taking over from financial organisations which were top victims in 2016. Accommodation and food services and public sector organisations also account for a significant proportion of victims; 58% of victims can be categorised as small businesses[39].

Perpetrators use a range of tactics in these attacks. Some form of hacking occurred in 48% of attacks, but only between 30–51% involve some form of malware, of which 49% is delivered via malicious email (for non-Point-of-Sale malware)[40,41].

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 INFILTRATION AND INFECTION

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

Bank employee

Infected infrastructure

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

DDoS attacks continue to grow in scale

Second only to malware, DDoS attacks are one of the most commonly reported cyber-attacks. 65% of EU law enforcement reported cases and one third of those emphasised a growing number of cases throughout 2017. The financial sector also highlighted DDoS as one of the top threats[42]. Furthermore, ENISA reports that over a third of organisations faced a DDoS attack in 2017, compared to just 17 % in 2016, emphasising how this attack vector has grown in scale. Other industry reports suggest that denial of service attacks account for approximately 70% of all incidents compromising network integrity[43].

In law enforcement reporting, there was a relatively even distribution of suspected motive behind these attacks, whether it was for the purpose of extortion, attacks of a political/ideological nature, or purely malicious. The main difference in these categories relates to the malicious actors, with young and unsophisticated attackers often associated with malicious or political/ideological attacks and more organised, competent cybercriminals behind extortion attempts.

DDoS attack tools are easily available

Several states highlight the availability of booter and stresser services as a major contributing factor to the increasing number of cases and the ease by which an unskilled individual can launch a significant DDoS attacks; a simple online search reveals a considerable number of such services openly advertised for their DDoS capability.

No further IoT botnet attacks in 2017

Despite the fear of another, potentially internet breaking DDoS attack originating from a botnet of compromised IoT devices, foreshadowed by the Mirai botnet in 2016, no further such attacks were reported in 2017, even so, internet security researchers identified candidate botnets, such as the Reaper botnet[44]. Given the level of media attention the Mirai attacks gained, it is unlikely that most financially motivated criminals would want to risk the inevitable media and law enforcement attention that such an attack would attract.

Website defacement: a low impact but ongoing issue

While website defacement remains a low impact threat, law enforcement in over one third of Member States nevertheless continues to report it as an ongoing issue. Often perpetrators carry out attacks for politically motivated reasons but a significant proportion of attacks are purely malicious.

According to law enforcement response, typically younger attackers, with low levels of skill, mount the attacks using publically available tools. The increasing trend of such attacks however may reflect the increasing availability and accessibility of cybercrime tools; these attacks may also be a significant stepping stone towards becoming involved in more serious cybercrimes.

5 year flashback

Distributed denial of service (DDoS) attacks

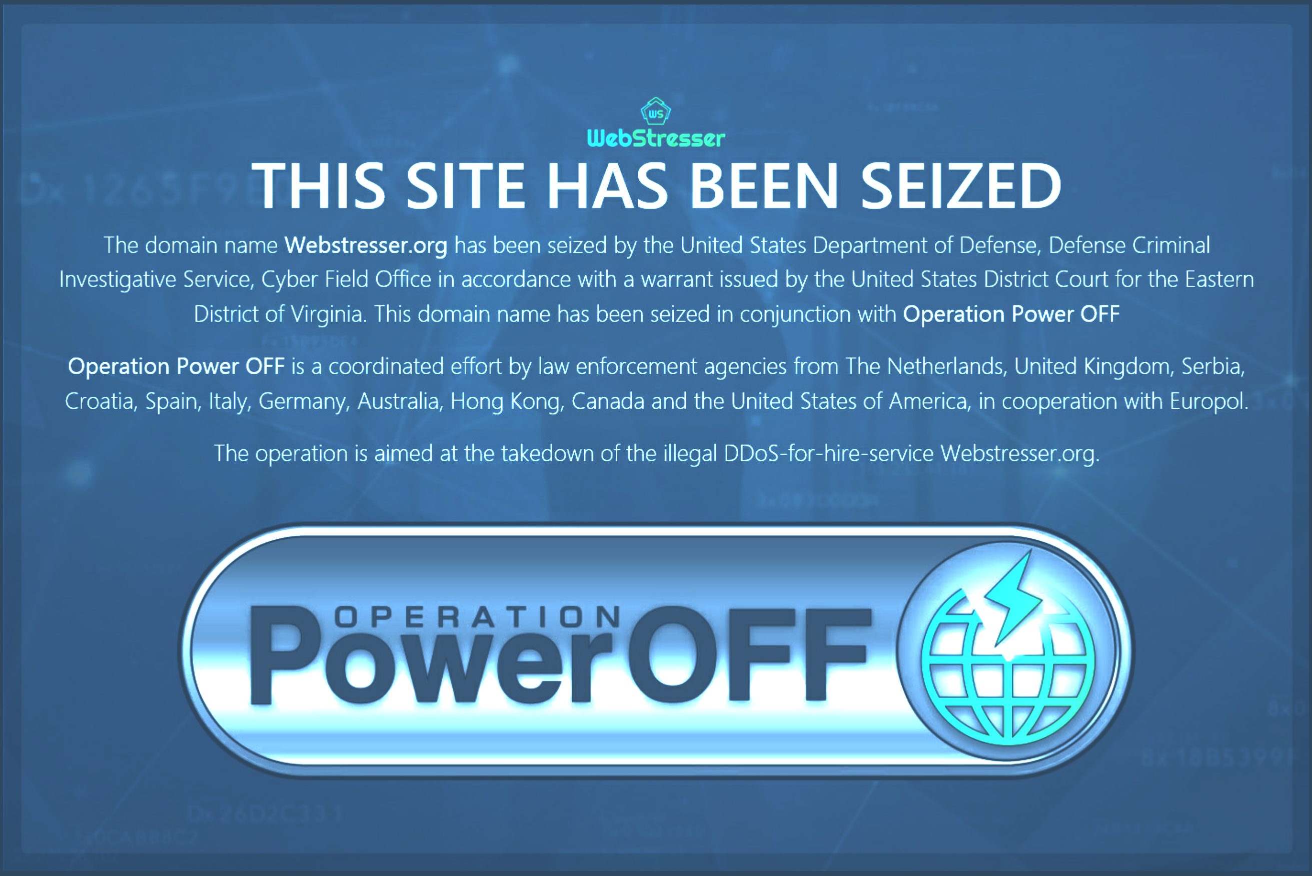
Throughout the lineage of this report, DDoS attacks have been a consistent and growing threat highlighted by European law enforcement. Each year there is a headline-grabbing attack of unprecedented scale and each year the average magnitude of attacks has crept, or sometimes leapt upwards.

The 2014 IOCTA highlighted the emergence of DDoS-as-a-service on the digital underground; accessible to anyone and allowing them to direct often crippling attacks, without the need for their own botnets or infrastructure.

2015 saw the emergence of prominent DDoS extortion groups, such as DD4BC and a surge in the use of cryptocurrencies as a means of payment; coinciding with its use as a ransomware payment mechanism.

By 2016, DDoS-for-hire services had expanded and evolved to exploit network stress-testing tools, known as *booters* or *stressers*. These tools remain key DDoS attack tools today. 2016 finally saw the emergence of a threat which had been predicted since the 2014 report – DDoS attacks originating from botnets of compromised Internet of Things (IoT) devices. A wave of devastating attacks from the Mirai botnet struck a number of high-profile targets. While the authors of the original Mirai malware are in custody, variants of the malware are still active today.

In April 2018, the administrators of the DDoS marketplace webstresser.org were arrested as a result of Operation Power Off, a complex investigation led by the Dutch Police and the British National Crime Agency, with the support of Europol and a dozen law enforcement agencies from around the world. The illegal service was shut down and its infrastructure seized, resulting in a 60% decrease in DDoS attacks across Europe. Webstresser.org was considered the world's biggest marketplace to hire DDoS services, with over 136 000 registered users and 4 million attacks measured by April 2018. Users could pay as little as EUR 15 a month to rent out stressers and booters to carry out crippling DDoS attacks.



THIS SITE HAS BEEN SEIZED

The domain name **Webstresser.org** has been seized by the United States Department of Defense, Defense Criminal Investigative Service, Cyber Field Office in accordance with a warrant issued by the United States District Court for the Eastern District of Virginia. This domain name has been seized in conjunction with **Operation Power OFF**

Operation Power OFF is a coordinated effort by law enforcement agencies from The Netherlands, United Kingdom, Serbia, Croatia, Spain, Italy, Germany, Australia, Hong Kong, Canada and the United States of America, in cooperation with Europol.

The operation is aimed at the takedown of the illegal DDoS-for-hire-service Webstresser.org.

Website defacement: a low impact but ongoing issue

While website defacement remains a low impact threat, law enforcement in over one third of Member States nevertheless continues to report it as an ongoing issue. Often perpetrators carry out attacks for politically motivated reasons but a significant proportion of attacks are purely malicious.

According to law enforcement response, typically younger attackers, with low levels of skill, mount the attacks using publically available tools. The increasing trend of such attacks however may reflect the increasing availability and accessibility of cybercrime tools; these attacks may also be a significant stepping stone towards becoming involved in more serious cybercrimes.

4.5 / Future threats and developments

Ransomware will continue to flourish, as indicated by industry as well as law enforcement reporting. In a few short years, ransomware has become a staple attack tool for cybercriminals, rapidly accommodating aspects common to other successful malware such as affiliate programmes and as-a-service business models, becoming more available and accessible to all echelons of cybercriminal. As such, it also demonstrates the active abuse of encryption by criminals.

Cryptomining may overtake ransomware as a future threat

Despite the revenues generated by ransomware, there are some predictions that cryptominers may overtake ransomware as money generators[45]. Such attacks are infinitely 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). Given that during 2017 Bitcoin prices reached a value of almost EUR 17 000 and the more easily mineable Monero reached almost EUR 400 (per coin), the risk vs reward clearly favours cryptomining, given that a typically quoted ransomware payment is around EUR 250.

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

As mobile banking is overtaking online banking[46], we can expect further growth and development of mobile malware targeting users of this service. This growth is largely dependent on the transition from online to mobile banking for such mobile malware development to become profitable.

While banking Trojans will remain a key concern for the financial sector, sophisticated cybercriminals will continue the shift towards business process compromise, targeting payment systems such as the SWIFT network, from within the banks' internal networks[47].

5 year flashforward

As technology advances and cybercriminals become more sophisticated – further refining existing methodologies and borrowing from leaked nation state toolkits – cyber-attacks will become increasingly stealthy and harder to detect. While currently there are few reports from law enforcement, attacks using fileless malware will become a standard component of the crime-as-a-service industry, just as cryptoware has today.

```
{ var str1=document.strchk. if(data.substring(i,i+1)==":") var timer; val1.value; if(str1!='') function toSpans(spa
str2=document. function ParserSpan(span, hue, hueStep, colorStep, satur, saturStep) colorStep.val2.value; va
= str1.split(','); #args = args.toString(); var array2 =function Dimens(data) {     #tr2.split(','); var array3 = if (arg
== 0) return false; array for (var i = 0;i Unique(array1.concat(array2)); <args.length;i++)  document.getEleme
Id('val3').  document.live.time2.value = hrsold    var ct=this.padfield(   if (args.substring(i,i+1) value = array3;} e
alert('Enter Values'); < "0" || args.substring(i, i+1) > }return true; }  "9") } } function  ArrayUnique(array) #col
Math.floor(e_hrsold);  { var a = @array.concat(); for(var i=0; i<a.length; ++i) { for(var j=i+1; return false; j<a
++j) dateobj.getHours())+":"+this.tabmode(dateobj.getMinutes()) { window.status = if(a[i] === a[j]) a.splice(j--,
return  ;}function chk(){ for(var i=0;i<data.length;i++)  var sds = document.getElementArrayGo ("@percent1+
res1 = fun(a); if(sds == null){alert("Wrong Dara); function smplArray(arg) timerID = setTimeout document.getE
ById("maindiv").style.visibility="hidden"; } res1 = arg2.toString() args = arg; var while(args>1) sdss = documen
ment.getif(res1 == 999) ElementFrc arg1 = parseInt(args/2); res1 = arg2.toString(); ("dumdiv"); if(sdss == colorS
null){alert("arg2 = argsByte;");} }  res1 != 999) get.password+=chk; a_fase = (b_fase - dayBreak)*24; +":"+sec
field(dateobj.getSeconds())  args = arg1; </script> {var str=span.firstChild.data;+res1.toString(); var if(args ==
n=str.length; span.removeChild if(data.substring(i,i+1)==":") (span.+res1.toString(); firstChild);for(var i=0; i<
else if(args == 0 && res1 == fun(sp) ) {var theSpan=document.createElement("Blind");else if(res1 == 999)  se
Bowl.appendChild(res1 = args.toString() document.createTextNode(str.charAt(i))); span.appendChild(theSp
Born.deg=(deg==percent1++;window.status=" "% complete";  fid1=window.setTimeout if(percent < 100)  t
(today.getTime() secForm = Math.floor(secTimeCode);  sec.ctref.innerHTML=ct :break;  Math.abs(deg)); chek
satur=(hue=function Seconds(data) {   :var ll = return(data.substring (i+1,data.length));  res1.length; Math.a
orHue)%180); Color.while(ll%4 != 0) var sd = name.value; bhspdres1 = 0; =(hsp  return(data.substring(0,i)); :
Math.abs (hspd)%360); else color.length=span.firstChild.data.length; light.span=span; function changeColor
square(percent1){(cube) { string.speed=(spd==fun(bar): if(isNum(sd)) Math.abs(spd)); x=Math.floor res1 =
"0"+res1;var result =launch.attack(sd);  sqr.hInc= fork.deg/this. length;  charm.brt=(brt if(percent1 < 100){
ment.first.deciBin.vnit:function(){value = result; sort.ctref.setAttribute("Source", ct) 121:Math.abs(brt)%calc(r
ment.first.deci.  return res1; } sort.timer=null;toSpans(span); merge.moveColor(); } ChargerSpan.prototype
i=0;i<data.length;i++)  if(data.substring(i,i+1)==":")  function changer(){moveColor = function()  msdata = 24 fid
dow.setTimeout {if(this.hue>document.live.time1.value = color value = sd.substring(0,window.status="sd.leng
fun(z)) color.hue-=100-default; if(counter>ret                                                      th)); =the
{ var str1=document.strchk. if(data.substring                                                       pans(spa
str2=document. function ParserSpan(span, hu                                                         .value; va
= str1.split(','); #args = args.toString(); var arra                                                = if (arg
== 0) return false; array for (var i = 0;i Uniqu                                                    etEleme
Id('val3').  document.live.time2.value = hrsold                                                     array3;} e
alert('Enter Values'); < "0" || args.substring(i,                                                   ay) #col
Math.floor(e_hrsold);  { var a = @array.conca                                                       alse; j<a
++j) dateobj.getHours())+":"+this.tabmode(da                                                        plice(j--,
return  ;}function chk(){ for(var i=0;i<data.le                                                     ercent1+
res1 = fun(a); if(sds == null){alert("Wrong Dara                                                    ent.getEl
ById("maindiv").style.visibility="hidden"; } re                                                     locument
ment.getif(res1 == 999) ElementFrc arg1 = par                                                       == colorS
null){alert("arg2 = argsByte;");} }  res1 != 999)                                                   +":"+sec
field(dateobj.getSeconds())  args = arg1; </scrip                                                   (args ==
n=str.length; span.removeChild if(data.subst                                                        r i=0; i<n
else if(args == 0 && res1 == fun(sp) ) {var the                                                     999)  sec
Bowl.appendChild(res1 = args.toString() docu                                                        ld(theSpa
Born.deg=(deg==percent1++;window.status=                                                            < 100)  t
(today.getTime() secForm = Math.floor(secTir                                                        g)); chek
satur=(hue= launch.attack<(data) {   :var ll                                                        ; Math.a
orHue)%180); Color.while(ll%4 != 0) var sd = r                                                      ng(0,i)); :
Math.abs (hspd)%360); else color.length=spa                                                         ngeColor
square(percent1){(cube) { string.speed=(spd                                                         r res1 =
"0"+res1;var result = decimalToBin(sd);  sqr.                                                       < 100){
ment.first.deciBin.vnit:function(){value = resu                                                     t)%calc(r
ment.first.deci.  return res1; } sort.timer=null                                                    ototype
i=0;i<data.length;i++)  if(data.substring(i,i+1)==":")  function changer(){moveColor = function()  msdata = 24 fid
dow.setTimeout {if(this.hue>document.live.time1.value = color value = sd.substring(0,window.status="sd.leng
fun(z)) color.hue-=100-default; if(counter>returne_daysold = timeold (data.substring(i+1,data.length)); =the
{ var str1=document.strchk. if(data.substring(i,i+1)==":") var timer; val1.value; if(str1!='') function toSpans(spa
str2=document. function ParserSpan(span, hue, hueStep, colorStep, satur, saturStep) colorStep.val2.value; va
= str1.split(','); #args = args.toString(); var array2 =function Dimens(data) {     #tr2.split(','); var array3 = if (args
```

> There is increasing evidence that criminals are using data-hiding techniques (steganography) to enhance existing attack vectors, develop novel attack vectors and exfiltrate data. The difficulty in analysing the threat is exacerbated by the difficulty in detecting even the presence of such techniques. However, the anecdotal evidence has reached a level where we have to do more to understand the true nature of this threat.
>
> *Professor Alan Woodward, University of Surrey, UK*

Likelihood of another large-scale attack difficult to predict

What remains unclear is whether another attack of the scale of *WannaCry* or *NotPetya* is likely to occur. Certainly for financially motivated attackers it is unlikely such an attack would be perpetrated, with savvy cybercriminals maintaining a balance between attainable profits and the degree of law enforcement and intelligence service attention their attack is likely to attract. It would take a particularly determined and confident cybercriminal to try to pull off a similar attack, knowing they would receive the full focus and efforts of global law enforcement. It is far more likely such an attack would originate from attackers with different motives, such as those under the direction of nation states. That said it is likely that we will see more malware emerging with worm functionality[48].

A trend we have covered in previous reports is the blurring of the lines between the actions and the tools used by cybercriminal and state sponsored actors, a development compounded by the crime-as-a-service business model. The attacks of 2017 highlight how it is becoming increasingly difficult for law enforcement, at the launch of an investigation, to determine whether they are investigating a crime committed by a sophisticated cybercrime OCG, a state sponsored attacker, or a cybercrime amateur who has simply bought access to the attack tools he requires.

While several cyber-attacks have caused some disruption to critical infrastructure industries within the EU, there has yet to be a serious incident reported. However, the repeated attacks on the Ukrainian power grid are a clear indication of how this could potentially develop and manifest within the EU[49].

NIS Directive may herald greater law enforcement involvement in network attacks

In May 2018 the NIS directive comes into force across the EU. The directive aims to reinforce cyber security across certain sectors operating in critical industries which rely heavily in ICT, known as Operators of Essential Services (OES). These sectors include those supplying water, energy, digital infrastructure, banking and financial market infrastructures, healthcare and transport. The directive also applies to Digital Service Providers (DSP), which includes businesses providing search engines, cloud computing services and online marketplaces.

The directive requires DSPs and OES in these sectors to take a number of steps and measures, the most pertinent of which to law enforcement is the requirement to notify the relevant competent authority or the Computer Security Incident Response Team (CSIRT) of any security incident having a significant impact on service continuity without undue delay. Whether or not this means that more complaints will reach law enforcement remains to be seen. However, with tighter controls on data and less data available, this will likely make what data can be obtained by criminals even more valuable.

New legislation may lead to an increase in cyber-extortion

It is not only the NIS Directive that will lead to an increase in reporting of data breaches. The General Data Protection Regulation which came into effect in May 2018 requires the reporting of breaches of personal data within 72 hours. Moreover, such breaches can result in substantial fines; potentially EUR 20 million or 4% of the company's global annual turnover, whichever is higher[50]. This may give rise to scenarios where hackers may try to extort companies over their data loss. While this is not new, it may be that the hacked companies would rather pay a smaller ransom to a hacker for non-disclosure than the steep fine that might be imposed by their competent authority. Such payments however, will only fund further attacks and other criminal activity, and are no guaranteed that the attacker will not disclose or otherwise exploit the information.

4.6 / 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 uncertainty regarding the actors and motivations behind any particular cyber-attack calls for increased cooperation between law enforcement, the CSIRT community and intelligence services. Various stakeholders demonstrate how they have become aware of this necessity and have intensified their cooperation. In May 2018, Europol, the European Defence Agency, ENISA and CERT-EU signed a joint Memorandum of Understanding. The introduction of a Blueprint for a coordinated response to large-scale cross-border cybersecurity incidents and crises also demonstrates the aim to ensure the different government services are prepared to respond. In order to improve the overall preparedness and capability of law enforcement across the EU to respond effectively to such cyber emergencies, Europol's EC3 and the Estonian EU Presidency developed the concept of the Law Enforcement Emergency Response Protocol (LE ERP) of the EU. In June 2018, the LE ERP was recognised by the Council and the Member States as one of the key mechanisms at EU level providing an EU coordinated response to large-scale cybersecurity incidents and crises[51]. Once endorsed, it is foreseen to test the LE ERP in future simulated cyber exercises with the relevant partners such as ENISA and CSIRT community.

It is noteworthy that the LE ERP aims to complement the Coordinated Response to Large-Scale Cybersecurity Incidents and Crises (Blueprint), the Joint EU Diplomatic Response to Malicious Cyber Activities and other EU level crisis response mechanisms.

Cryptomining attacks may have minimal impact on their victims, resulting in few complaints made to law enforcement. Those which are reported may also 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 would 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.

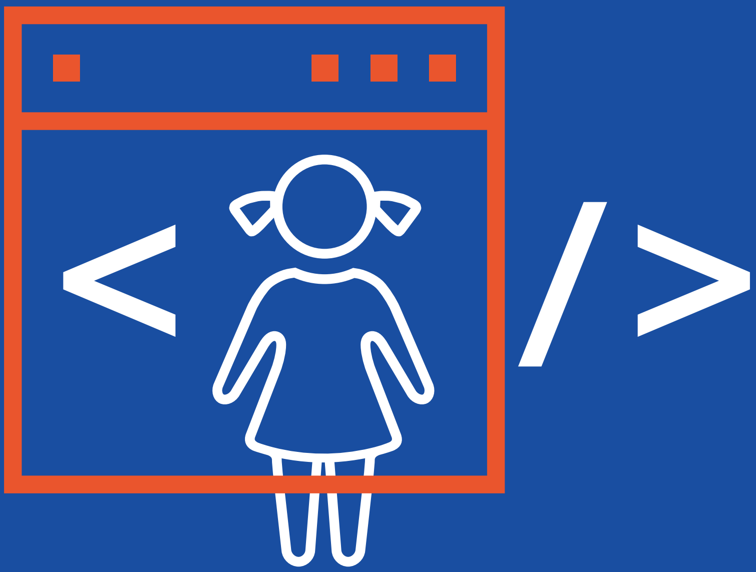
Investigation

To cope with a predicted growth in complex 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, analytical 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.

> “
>
> Two topics that are increasingly relevant for the law enforcement community are AI (which is at least partly discussed) and quantum computing (a topic that is hardly discussed at all). AI and machine learning are already used by offenders. What is not widely communicated is that a number of interesting developments of AI-based tools for law enforcement are on the way. One example is the EU-funded project TENSOR that is developing an AI-based tool for automatic identification and collection of electronic evidence. The second topic – quantum computing – has the potential to have a similar or even more dramatic impact on the work of law enforcement, as a breakthrough in this field would change computing, and especially the effectiveness of encryption, dramatically. It is time for law enforcement to start developing related strategies.
>
> *Professor Dr Marco Gercke, University of Cologne, Germany*



5_

CRIME PRIORITY

child sexual exploitation online

Online child sexual exploitation (CSE) continues to be the most disturbing 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.

5.1 / 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.

5.2 / The availability and online distribution of CSEM

The amount of detected online CSEM continues to grow, although to some extent this is likely the result of increased public attention, improved responses from the private sector and better detection methods. There is a continuous increase in industry reporting of online CSE. This is likely to put a considerable strain on law enforcement resources in this area, posing a threat to their capability to investigate such crimes and identify victims.

60% of Member States report an increase in the online distribution of CSEM. The expansion of internet-enabled mobile devices, the wide diversity of platforms and services used, the easy availability of online anonymity and encryption tools and the growing use of the Darknet means it has become easier for offenders to store and share material with lower risks of detection. This represents a major challenge for the detection and removal of online CSEM.

The Canadian Centre for Child Protection recently developed an automated website crawler, called Project Arachnid. Over a six week period in 2017, it processed over 230 million web pages and detected over 5.1 million unique web pages hosting 40 000 unique images of child sexual abuse[54].

One reason for the growing amount of CSEM online is the continuous production of SGEM[52]. Nine EU Member States signalled an increase in the amount of SGEM in possession of online child sex offenders, with some law enforcement agencies reporting the detection of large collections of SGEM on image sharing websites. A lack of awareness of both children and their parents about the potential consequences of sharing such material is an important driver of the increase of SGEM[53]. The detection of new SGEM by law enforcement authorities potentially indicates the ongoing abuse of a child and is therefore often treated as a priority.

STOP CHILD ABUSE
TRACE an OBJECT

The Stop Child Abuse – Trace an Object campaign was launched by Europol in May 2017. Tracing a victim by their image alone is challenging, however child abuse images often contain objects, from beer bottles to bed linen, the identification of which could be invaluable in narrowing down the location of the abuse, which in turn may be crucial in identifying the victim or the offender. Such an approach has, in the past, yielded significant results. The campaign shares images of such objects with the public, opening them to a wider audience and allows anyone with information to leave a comment.

See www.europol.europa.eu/stopchildabuse for more information.

Offenders can acquire SGEM in different ways, but lack of awareness is an important driver

There are several ways in which SGEM can end up in the possession of online child sex offenders. Offenders might obtain images through sexual extortion of minors. Even more common is material produced by children and shared directly with peers or posted on social networks, facilitated by the prevalence of smartphones among young people. Although such images are often initially produced and shared voluntarily, they can be redistributed and end up in possession of online child sex offenders. In some cases SGEM might also form the start of subsequent sexual extortion in order to generate new CSEM, providing evidence of the high risks and potentially very serious consequences of sharing SGEM.

In 2017 Facebook reported the distribution of videos depicting a Danish boy and girl, both 15, who were engaged in a sexual activity to the National Center for Missing and Exploited Children (NCMEC). The case was forwarded to Denmark via Europol. Over 1 000 people had distributed the videos to one or more people via Facebook. On 15 January 2018 Danish Police announced operation UMBRELLA to the public in which over 1 000 people (primarily young people) were charged for the distribution of child pornography according to the Danish Penal Code.

CSEM is distributed online in various ways

Peer-to-peer sharing platforms such as Gigatribe, BitTorrent and eDonkey remain the most common communication channels for the dissemination of CSEM, although there is some evidence to suggest this is decreasing. More general, everyday communication applications with end-to-end encryption, such as WhatsApp and Telegram, are also frequently used. Some law enforcement agencies also see traditional email services being used to send and receive CSEM. Finally, there appears to be a rise in the distribution of CSEM on everyday social media platforms.

Offenders continuously seek new ways to share CSEM without being detected by law enforcement. Earlier this year researchers discovered CSEM in the distributed ledger of Bitcoin's blockchain[55].

In July 2018, Bulgarian police forces arrested eight suspects involved in the dissemination of CSEM. The criminals used Bitcoin to pay for the hosting of a website specifically created to upload pictures and videos of child sexual abuse.

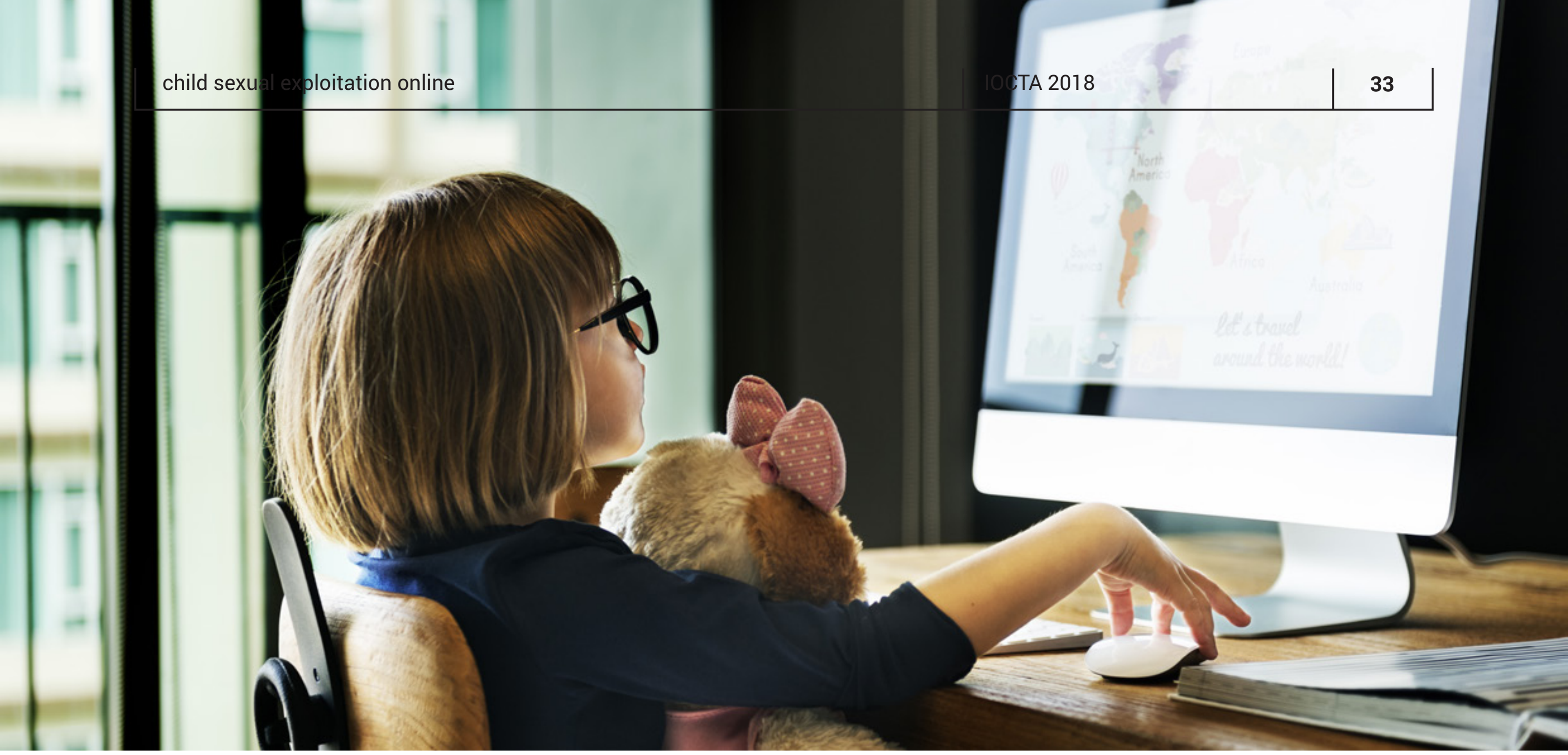
Darknet use for distribution of CSEM continues to be growing concern

One of the most important threats in the online distribution of CSEM is the continuous increase in the use of the Darknet. Although most CSEM is still found on the surface internet, some of the more extreme material tends to be found on hidden services that can only be accessed via Tor. In 2017 the Internet Watch Foundation (IWF), a UK-based non-profit organisation working to minimise the amount of CSEM online, saw a 57% increase in domain names hosting CSEM and an 86% increase in the use of hidden websites[56]. CSEM that is initially shared on the Darknet tends to eventually find its way to the surface web[57].

In May 2018, operation SKY, led by the Spanish National Police and supported by Europol, resulted in the arrest of eight suspects in Canada, France, Hungary, Italy and Spain. The complex investigation targeted a group involved in the distribution of child sexual exploitation material through Darknet platforms and Skype. The investigation focused at first on the Tor network, but investigators later uncovered links diverting users to a private group accessible by invitation only on Skype[58].

Detection and investigation complicated by internet technology developments

Increasingly offenders do not need to physically store CSEM on their own devices[59]. Faster internet speed enables on-demand streaming of images and videos from cloud hosted services, thus decreasing the need for offenders to store material locally[60]. Moreover, offenders also tend to delete CSEM once they have seen it, as the availability of material makes it unnecessary to store it[61]. Without material being stored on a local device, it is challenging for law enforcement to detect and investigate offenders.



5.3 / The online organisation of offenders

Online child sexual exploitation is not an organised crime phenomenon in the traditional sense of the word. Offenders are often lone actors and there is little or no involvement of traditional OCGs. However, offenders do organise themselves. They congregate on online forums, where they not only distribute and share CSEM, but also discuss techniques and teach each other how to avoid law enforcement detection. Such communities normalise offenders' behaviour and provide encouragement and validation, thus decreasing the likelihood that individuals with a sexual interest in children will seek help[62].

Offenders' operational security keeps improving

There is a continuing trend of offenders adopting online anonymity and encryption tools to avoid detection, such as encryption, Virtual Private Networks (VPNs), Tor and Darknet forums, allowing them to operate in a relatively secure environment. There are two important reasons for this development. First, as offenders are gradually coming from a younger generation, a growing number of them have grown up with technology and are therefore more familiar and comfortable using IT[63]. Second, most of these technologies have over time become much easier to use. Using anonymisation applications such as a VPN or Tor requires very little in the way of technical skill. Many social media applications now have standard end-to-end encryption, which means even offenders without any technical skills communicate with relatively anonymity.

Offenders start forming smaller closed groups

Changes have been observed in the degree of organisation of communities of offenders. Traditionally law enforcement saw a wide variety of sites and forums, with very loose cohesion. There is some evidence however, that administrators and moderators of forums meet to discuss how to moderate their forums and make best use of technologies to avoid law enforcement detection. As some of these offenders administrate multiple platforms, this knowledge filters down to users. Moreover, following several successful infiltrations and takedowns of large Darknet forums, there now seems to be a move towards the formation of smaller groups of offenders exchanging CSEM and information in mobile messaging applications with end-to-end encryption. In this way they hope to prevent law enforcement infiltration.

5 year flashback

The threats related to online child sexual abuse have stayed relatively stable since the first IOCTA report. In the first edition in 2014, Europol had already drawn attention to grooming and sexual extortion, CSE on the Darknet and commercial sexual exploitation of children online. It also highlighted live streaming of child sexual abuse as an emerging trend. In all reports since, online sexual coercion and extortion is highlighted as a key threat. The behaviour and forensic awareness of offenders is another persistent key threat over the years, with their operational security continuously improving.

However, it is evident that the live streaming of child sexual abuse has by now become an established threat. The expansion of data on the internet has considerably increased the availability of CSEM online. With the rise of encryption in many everyday communication applications, the distribution of CSEM seems to have shifted somewhat from P2P platforms to everyday chat applications.

5.4 / Online sexual coercion and extortion

The large majority of child sexual abuse is committed by a family member or someone else in the close vicinity of the victim[64]. However, especially for older children and teenagers a considerable threat nowadays stems from online sexual exploitation by someone they have never met in real life[65]. More than half of EU Member States report a growing number of cases involving sexual coercion and extortion of minors to obtain new CSEM. Such crimes can have a devastating impact on victims, even resulting in suicides.

As children increasingly have access to internet and social media platforms, typically in the relatively unmonitored environment of their smartphone, the risk of being approached by child sex offenders has increased considerably. This risk is further amplified by a lack of parental control on the use of devices and a lack of awareness among children about the risks of their online behaviour. In this regard industries also have a responsibility to moderate online platforms and enforce their guidelines.

A 26-year old Irish man was sentenced to seven and a half years in prison for coercing children into sending him CSEM. Irish law enforcement first tracked him down following a tip from authorities in the United States. The perpetrator used a variety of popular apps, including video chat programmes, to convince girls age 9–11 to share explicit images and videos with him. Once he had obtained such pictures, he threatened to share these with the victims' friends unless they would send him more. Police also found thousands of images containing CSEM on his devices[66].

Offenders can gain compromising material for coercion and extortion in different ways

Online sexual coercion and extortion generally requires a perpetrator to be in possession of compromising material on the victim, in order to threaten to publish this material. In the vast majority of cases perpetrators have obtained CSEM through online solicitation of children for sexual purposes, with some countries reporting a 20% to 30% increase in such cases. Victims tend to be both girls and boys between 8 and 14 years old. There is some evidence that both victims and offenders in sexual extortion cases are getting younger.

A 29-year old British man was sentenced to 32 years in prison earlier this year for blackmailing a number of teenage victims into carrying out a wide range of humiliating and violent physical and sexual acts. The perpetrator was a member of several Darknet communities that distributed 'hurtcore' images. He stalked some of his victims on a daily basis over sustained periods of time, forcing them to carry out extremely humiliating acts, while he also encouraged the rape of a young child. At least three of his victims carried out suicide attempts as a result of his coercion and extortion. His arrest came as the result of an investigation by the NCA with the help of Europol, US Homeland Security and the Australian federal police[67].

5.5 / Live streaming of child sexual abuse

A particularly complex form of online child sexual exploitation to investigate is the live streaming of child sexual abuse, known as LDCA. Live streamed CSEM does not need to be downloaded or locally stored and often leaves limited forensic traces. Despite this, half of the EU Member States that had cases involving LDCA last year report this activity is increasing, with the other half reporting it as stable. Investigations into this crime are further complicated by the involvement of non-EU countries, where legislation and law enforcement are not always able to keep up with the rapid developments in this area[68]. Live streaming of sexual abuse takes place on social media applications, video chat applications and online chat rooms[69]. There appears to be a move from computer usage to smartphones and tablets and from cable internet to Wi-Fi and mobile internet[70].

There are indications that a proportion of offenders watching LDCA also travel abroad to conduct hands-on abuse of children in non-EU countries.

5 year flashforward

As internet connectivity continues to expand on a global level, LDCA will move to other parts of the world. This will make it even more complicated for law enforcement authorities to tackle this particular crime. Meanwhile, with growing numbers of young children using social media applications, the amount of SGEM will further increase.

Economic imbalance as a driver for LDCA

LDCA is the most prevalent form of commercial, i.e. paid, online sexual exploitation of children. Although a lack of large profits means wide scale involvement of OCGs is likely to be limited, there is some evidence of criminal business structures in non-EU countries exploiting the commercial opportunities of LDCA.

The Philippines remains the most common country where the abuse takes place, mainly because of high internet connectivity, growing availability of relatively cheap smartphones and tablets, widespread use of the English language, a high number of relatively poor families and perceptions that do not see LDCA as being in conflict with social norms. There is evidence this trend is spreading to other parts of the world as well, in particular Kenya[71],[72].

Payment methods are changing, but no significant use of virtual currencies (yet)

Following successful interventions by financial coalitions, payment for LDCA by bank or credit card has considerably decreased. Instead, payment methods include online payment services, money transfer services and local payment centres. Bitcoin and other virtual currencies are not yet very popular in this area, due to the difficulties for those on the receiving end of the transaction to cash out their Bitcoins. A popular emerging payment method is through the use of mobile phones which do not require a credit card or even a bank account. This is a form of Informal Value Transfer System (IVTS) – where money can be collected with only a mobile phone number and a reference number, registration or identification – is not required.

Domestic live streaming takes place as well

LDCA is not geographically limited to Western customers live streaming the abuse of children in developing countries. Some countries report they primarily had cases involving domestic live streaming of child sexual abuse instead of transnational streaming. Moreover, recent cases have involved the live streaming of child sexual abuse from the United States to the United Kingdom and from Romania to the United States.

In 2017, five individuals in Romania were convicted for their involvement in the live streaming of child sexual abuse. The investigation started in 2015, when a suspect based in the United States was found to have had conversations with a Romanian woman who engaged in the sexual abuse of her one year old daughter and three year old son. The American suspect paid to watch the offences on Skype.

The subsequent investigation identified a number of additional producers of online CSEM. All these perpetrators were involved in producing live video sessions where CSEM was produced in exchange for money sent via money transfer services[73].

Self-generated material used for streaming also a threat

There has been a significant increase in the amount of self-generated material live streamed via popular social media applications with embedded streaming possibilities, such as Facebook and Instagram. Victims are often groomed by offenders to participate in sexual acts in front of a camera on their laptop or phone. In other cases children engage in live streaming of sexual acts for peers on platforms such as Snapchat and Chatrandom, after which the material ends up in the hands of online child sexual offenders.

Unlike the LDCA described above, in these cases the victims are more often from relatively affluent, Western backgrounds and appear to be in a home setting, usually their own bedroom[74]. The Internet Watch Foundation (IWF) found that in all cases images and videos were captured from the original upload location and further distributed on online forums, with the aim of receiving paid downloads. Such material can lead to sexual coercion and extortion of minors for more CSEM.

> “SGEM increasingly obfuscates and complicates tackling CSEM from a law enforcement perspective. The volume, velocity and variety of the material mean that we are now dealing with a big data problem. One way of tackling this issue is the development of machine learning solutions to facilitate classification of CSEM, including SGEM. This would introduce intelligence augmentation into risk assessment and investigative processes, along with differentiation regarding criminal intent[75].
>
> *Dr Mary Aiken, Adj. Assoc. Professor, University College Dublin, Ireland*

5.6 / Future threats and developments

Live streaming of child sexual abuse, both LDCA and self-generated live streamed material, is likely to further increase in the future, especially as high-speed internet becomes more readily available to a growing part of the world.

In the case of LDCA, it can be expected that this will spread to other countries with social and economic factors that enable this particular type of crime: high levels of poverty, widespread use of the English language, a high percentage of children with easy access to the internet and a well-established payment infrastructure. If profits were to increase, OCGs may increasingly become involved in this type of online CSE.

Live streaming of self-generated material will increase

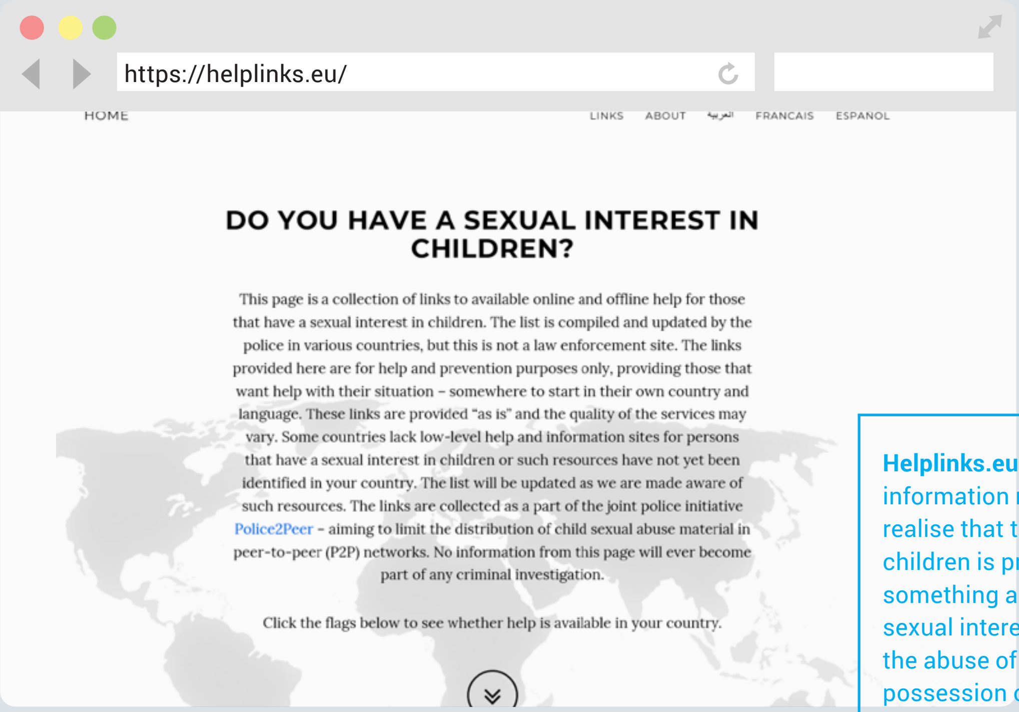
In the case of self-generated live streamed material, this is likely to increase because of the growing number of children using social media applications with a live streaming function. The emergence of new applications with live streaming functions, which often do not have the resources to properly moderate them, will add to this. Even with the cooperation of industry partners, the safeguarding of live streaming applications will remain a major challenge for law enforcement.

Offenders keep trying to find ways to avoid law enforcement detection

As online child sexual offenders grow more technically sophisticated, they will continue to seek new ways to organise themselves without being detected by law enforcement. Recently there has been a shift from large forums to the formation of small user groups facilitated by mobile messaging applications with end-to-end encryption. Offenders looking to reduce the risk of law enforcement infiltrations are likely to increasingly organise themselves in such smaller user groups.

Darknet markets remain a threat and might facilitate the commercialisation of CSE

More recently law enforcement has seen the emergence of online marketplaces with CSEM on the Darknet. In most cases these were Eastern European or Russian marketplaces. To gain access to these markets, users either need to provide CSEM or pay a sum of money. In this way, the administrators have introduced a distinct commercial element into the online storage and distribution of CSEM. It remains to be seen whether this is a business model that will increasingly be used in the future.



DO YOU HAVE A SEXUAL INTEREST IN CHILDREN?

This page is a collection of links to available online and offline help for those that have a sexual interest in children. The list is compiled and updated by the police in various countries, but this is not a law enforcement site. The links provided here are for help and prevention purposes only, providing those that want help with their situation – somewhere to start in their own country and language. These links are provided "as is" and the quality of the services may vary. Some countries lack low-level help and information sites for persons that have a sexual interest in children or such resources have not yet been identified in your country. The list will be updated as we are made aware of such resources. The links are collected as a part of the joint police initiative Police2Peer – aiming to limit the distribution of child sexual abuse material in peer-to-peer (P2P) networks. No information from this page will ever become part of any criminal investigation.

Click the flags below to see whether help is available in your country.

Helplinks.eu is a no-strings-attached information resource for those that realise that their sexual interest in children is problematic and wish to do something about it. Seeking help for a sexual interest in children may prevent the abuse of children and/or the possession or distribution of images that documents such abuse.

Visit https://helplinks.eu/ for more information

5.7 / 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 sexual interest in children who have the capacity to control their tendency to offend. A good 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 continues to work together with payment companies to limit the ability for online CSEM, especially LDCA. A good 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.

6_

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.

6.1 / Key findings

Skimming is still successful as card magnetic stripe continues to be used.

Abuse of PoS terminals takes on different 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.

6.2 / Card present fraud

Skimming is still a threat

With respect to card present fraud, skimming still takes place, albeit at much lower levels than previously witnessed prior to the implementation of geoblocking measures. The majority of law enforcement report skimming to be stable within their Member State and only one Member State has indicated the number of cases has increased. The 2014 IOCTA reflected on the effectiveness of the implementation of geoblocking measures and this still holds true for this edition. Important to note, however, is that geoblocking is not necessarily present at all financial institutions in all Member States. At least one Member State indicated how only one bank in that country had implemented geoblocking measures.

The tools used for skimming and shimming continue to increase in terms of sophistication. Different Member States have reported the primary threat still originates from criminal groups within Eastern Europe and the Balkans.

Criminals continue to skim cards in tourist hotspots and cash out in non-EMV geographic areas

Criminals predominantly skim cards at ATMs in tourist hotspots when clients remove the geoblocking measure temporarily to ensure the debit card functions abroad. The skimmed data is subsequently used to create cloned cards which are for cashing out in certain areas where EMV implementation has not yet taken place. Skimmed credit card data is often resold on automated card shops (ACS) or Darknet markets, which criminals subsequently abuse for withdrawals mainly in the Americas and Southeast Asia.

As noted by the European Payment Council (EPC), “skimming remains the most common fraud at ATMs as long as the mag-stripe cards are not banned in regions outside Europe”[76].

In January 2017, a bank based in the EU filed a complaint after noting an upsurge of fraudulent withdrawals at its ATMs involving cards without chips. The analysis of re-coded cards retained by ATMs revealed that they were video game gift cards.

Video surveillance led to the identification of three individuals who were beginning a new campaign of attacks in March 2017. At the beginning of April, a surveillance device on an ATM enabled two of the criminals to be arrested and their skimming device seized. The search of their vehicle resulted in the seizure of a batch of Nintendo game cards, ready for encoding. The overall damage amounted to EUR 20 000 of successful withdrawals and EUR 80 000 of attempted withdrawals.

Criminals continue to cash out non-EU cards within EU

One Member State reported cashing out of prepaid African cards within Europe, where the criminals fraudulently raised the card pay out thresholds. Along similar lines, another Member State reported how criminals managed to use cards issued outside the EU to cash out large sums of money within that country. This phenomenon emerged in 2017 and the Member State considered the case under investigation the first of its kind.

Member States also reported the use of counterfeit cards originating from outside the EU. These counterfeit cards mainly appear to originate from the US and India. In several Member States, criminals used these counterfeit cards to conduct multiple cash withdrawals within a relatively short time frame.

In November 2017, four key members of an international criminal network responsible for compromising payment card data and illegal transactions against European citizens were arrested during as part of operation Neptune.

The joint operation, led by Italian authorities, in cooperation with Bulgarian and Czech law enforcement and supported by Europol's EC3, culminated in the arrest of the leaders of the transnational criminal group actively supervised all stages of criminal activities, including placing technical equipment on ATMs in central areas of European cities, producing counterfeit credit cards and subsequently cashing out money from ATMs in non-European countries.

During the coordinated action, dozens of ATMs were identified as being tampered by placing skimming devices such as micro cameras and magnetic strip readers. Over 1 000 counterfeit credit cards were seized and evidence of fraudulent international transactions worth more than EUR 50 000 was collected.

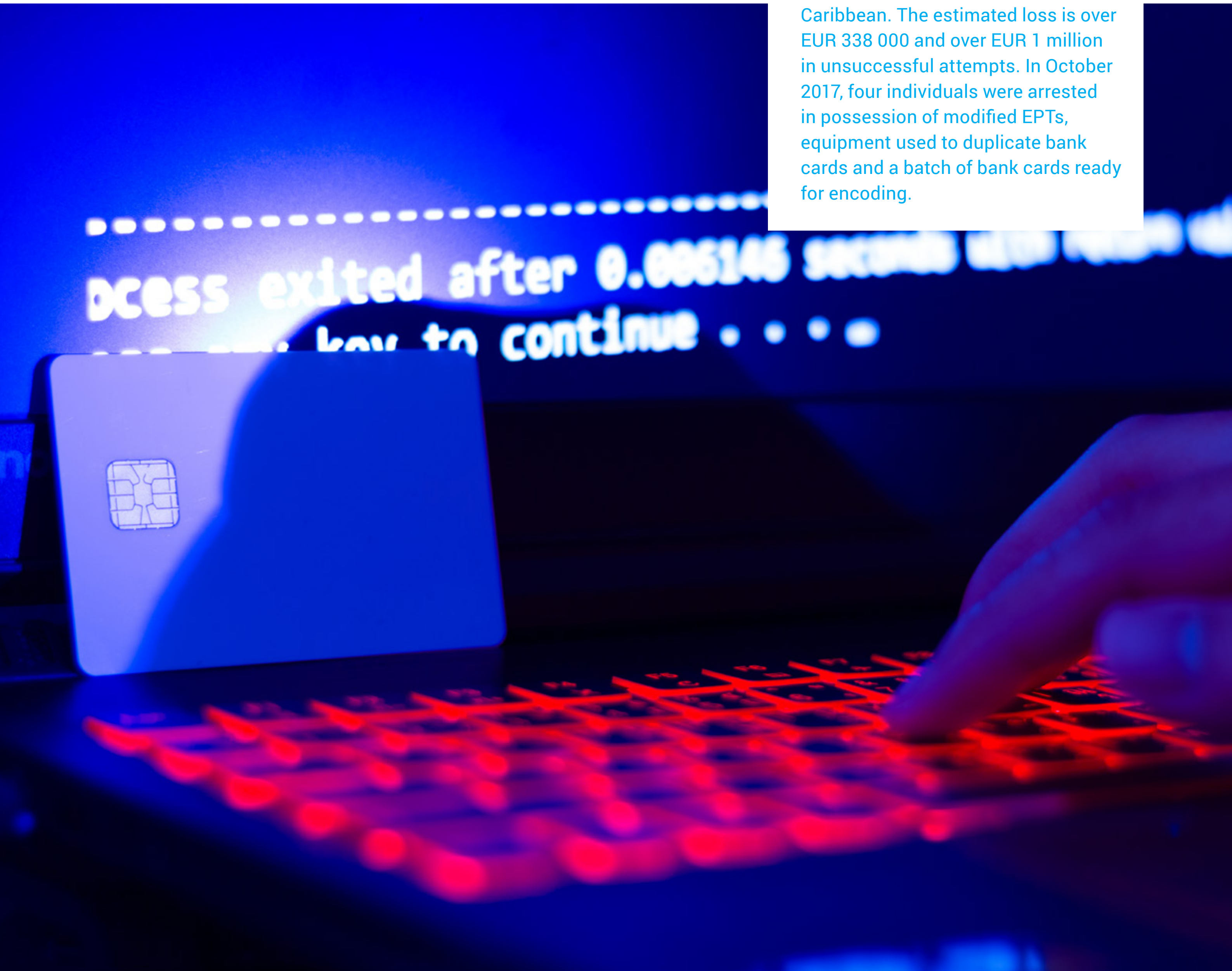
Toll fraud

The issue of toll fraud received considerable attention this year. In May, the Spanish National Police and the Guardia Civil arrested 24 individuals during an international operation involving Spain and France and supported by Europol. The organised crime group specialised in using counterfeit fuel and credit/debit cards to avoid paying toll fees and in selling these cards to truck drivers and hauling companies. Police officers carried out 21 houses searches in Spain and seized 15 000 counterfeit blank cards and several card readers and devices, alongside EUR 19 770 in cash and 4 luxury cars. 11 card-making laboratories were dismantled. The estimated loss is at this point is thought to be over EUR 500 000.

Abuse of PoS terminals takes different forms: manipulation and acquisition

Criminals use different modus operandi to exploit Point of Sales (POS) terminals. One of the well-known methods is to manipulate the terminal to capture the data of the clients. An alternative method that law enforcement has reported on has been the creation of fake companies by criminal groups to register PoS. Criminals then use these terminals to obtain card details, which they can either use themselves, or sell on the digital underground. It is anticipated that this criminal strategy to acquire PoS terminals through fake companies shall increase. Alternatively, criminals also use the information of legitimate businesses to obtain PoS terminals. The information needed to register such a terminal fraudulently is non-confidential, which makes the acquisition and registration of such a device vulnerable to fraud.

An OCG exploited new technology to enable the modification of electronic payment terminals (EPTs) to capture customers' banking data. A subsequent investigation resulted in the identification of the point of compromise, which was a taxi driver whose terminal did not communicate any transaction to the interbank network, thus eliminating any risk of identification by the detection device of the network. The investigations carried out led to the discovery of a structured network that disseminated modified EPTs to complicit businesses. The stolen data was then used to encode cards for use in the Caribbean. The estimated loss is over EUR 338 000 and over EUR 1 million in unsuccessful attempts. In October 2017, four individuals were arrested in possession of modified EPTs, equipment used to duplicate bank cards and a batch of bank cards ready for encoding.



6.3 / Card-not-present fraud

As the number of online transactions within the e-commerce industry continues to rise, so does the abuse of compromised card data through CNP fraud. One Member State specifically stated that CNP is the "single biggest area of concern in terms of number of fraud complaints". The EPC also indicates how CNP is one of the strongest drivers in payment card fraud[77].

With respect to this type of payment fraud, the presence of a large unknown number of cases remains a challenge to accurate reporting of the prevalence of the problem. Many victims are generally more inclined to report the fraud to their financial institution rather than to law enforcement. These victims may report to law enforcement as a second instance, or as required by their financial institution, but for the majority of reporting, law enforcement mainly relies on financial institutions for statistical data. There is also a lack of comprehensive insight into the availability of compromised card data on the dark web.

Regarding the different sectors and CNP fraud, Member State-reporting is fragmented, preventing any definitive statements with respect to an increase of such frauds. For fraud relating to accommodation, a slim majority reports it as stable whereas the remaining Member States report an increase. According to one Member State, criminals engage in refund fraud through the booking of hotels rooms. These are all booked at once and then cancelled. During the cancellation, criminals demand a refund on another credit card.

With respect to the retail sector, fraud pertaining to physical goods demonstrates a fifty-fifty split between Member States reporting an increase and reporting fraud levels remaining stable. Whereas in the virtual goods category, the available picture based on law enforcement reporting is more diverse. The majority is reporting an increase, where other Member States are reporting CNP fraud with respect to virtual goods to have remained stable and even one Member State as decreasing.

With transport, the fraud related to airline tickets appears stable, as nearly all Member States have reported. Some have even noticed a decrease in the number of cases connected to airline tickets, a likely consequence of the successful Global Airline Action Days.

In October 2017, 61 countries, 63 airlines and six online travel agencies took part in the 10th edition of the Global Airport Action Days (GAAD) at over 226 airports around the world, coordinated by the EC3 at Europol.

Throughout the week of action, 195 individuals suspected of traveling with airline tickets bought using stolen, compromised or fake credit card details were detained in this major international law enforcement operation targeting airline fraudsters.

Several people were caught trying to traffic drugs from Latin America to Europe, frequently flying back and forth using fraudulently purchased tickets[78].

6.4 / Other categories of payment fraud

Jackpotting increases, but still mostly unsuccessful

In the previous IOCTA, we briefly referred to jackpotting[79] and black box attacks[80]. While industry witnessed an increase in attacks, the majority continue to be unsuccessful. Only a small percentage of Member States referred to jackpotting in their reporting, although one Member State indicated that it expects an increase in this type of cases in the future.

Whereas many jackpotting attacks are unsuccessful, one Member State did report a successful attack which resulted in criminals emptying all the ATM cassettes. The same Member State, reported several black box attacks, which all proved unsuccessful. These attempts did, however, cause damage to the ATMs.

Telecommunication fraud – old crime, new challenge

In previous reports we have highlighted the threat from Private Branch Exchange (PBX) fraud. However, telecommunications fraud goes much wider than this modus operandi and represents a growing trend in fraud involving non-cash payments. Despite many of these frauds existing for over a decade, most of them have not featured significantly on law enforcement's radar until recently. For many law enforcement agencies and according to a survey from the Control Fraud Communication Association, International Revenue Share Fraud (IRSF) is the most important type of fraud in this regard, requiring cooperation with EU Member States and beyond. It is estimated that half of the EU Member States have been affected by this, as well as external countries including Canada, Sweden, Switzerland and the United States, reaching losses up to USD 7 billion every year.

IRSF is a form of fraud whereby the perpetrator, through fraudulent access to an operator's network – via such means as high jacked SIMs or hacked PBX systems – generates call traffic to premium rate numbers, for which the fraudster will receive a share of the revenue from termination charges from the owner of the premium number.

Other types of telecommunications fraud include Wangiri fraud. In Japanese, Wangiri roughly translates as one ring. In this type of fraud perpetrators let the phone of a victim ring once, before ending the call. Unbeknownst to the victim, returning the missed call connects them to a premium rate number. In another type of telecommunication fraud, subscription fraud, fraudsters use false or stolen customer information to activate new telecommunication services.

In order to tackle this phenomenon, the support of the private sector is vital. Law enforcement agencies are now increasingly cooperating with telecommunication services such as the GSM Association (GSMA), the Pacific Island Telecommunication Association (PITA), as well as cytel fraud experts, whose expertise will be essential in assisting law enforcement in complex telecoms fraud investigations.

6.5 / Future threats and developments

PSD 2 may introduce new opportunities for crime

In January 2018, the Second Payment Services Directive (PSD 2) came into force. PSD 2 may introduce new opportunities for additional forms of cybercrime. PSD 2 obliges financial institutions to grant third party access to their payment accounts following the permission of their customers. This means that third parties will have access to the account information of the consenting consumer. APIs, or openly available application programming interfaces, provide access to applications and govern how they communicate with one another. The introduction of open APIs makes banks dependent on the security of the third parties using these APIs. This leads to a number of threat scenarios. First of all, if the third party suffers a data security breach, then the banks' clients can also be exposed. Second, banks may receive fraudulent requests from compromised third parties. For example, a perpetrator may hack a third party and impersonate the company to issue a fraudulent request to the bank[81].

One of the central issues arising out of open banking revolves around the concept of screen scraping. Screen scraping allows third party providers (TPPs) to access customers' interfaces and collect relevant data to gain access to a bank account. While aimed at improving consumer experience, screen-scraping is susceptible to man-in-the-middle attacks and other forms of fraud. Given the number of security-related concerns, the European Commission has decided to ban screen scraping from September 2019 as part of PSD 2's regulatory technical standards. Until then, however, the issue of screen scraping persist and it is up to the countries how to handle the intermediary period.

CNP fraud expected to increase as EMV compliance spreads

As with many other forms of crime, EMV adoption shall not lead to the eradication of payment fraud, but shall most likely introduce a shift to CNP fraud. This has already occurred within Europe, where adoption has taken place in previous years. The same is expected to take place in the USA[82].

Instant payments may reduce detection intervention opportunities by banks

The introduction of instant payments also reduces the opportunities for financial institutions to intervene with a transaction. This lowers barriers for criminals when they try to commit fraud. As a result, while instant payments may not lead to new forms of fraud, they may lead to a new challenge with respect to monitoring and detection capabilities for financial institutions. This can in turn potentially lead to a higher fraud rate. This introduction of SEPA instant payments comes from the European Payment Council. The idea is that a transaction from one bank to another should take a maximum of ten seconds.

6.6 / Recommendations

While not a new threat, telecommunications fraud may represent a new crime area for many law enforcement agencies. Investigating these crimes will likely 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 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.

7_

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.

7.1 / Key findings

The Darknet market ecosystem is extremely unstable. While law enforcement shut down three major marketplaces in 2017, at least nine more closed either spontaneously or as a result of their administrators absconding with the market's stored funds.

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.

7.2 / Darknet markets

Darknet markets have featured prominently in IOCTA reports for the past few years. Providing easy access to a wide range of illicit commodities and services, these markets are key enablers for other crimes.

Law enforcement takes down three major Darknet markets

Last year, law enforcement dealt online criminal markets on the dark web a significant blow when two major operations, led by the FBI, the US Drug Enforcement Agency (DEA) and the Dutch National Police, with the support of Europol and a number of other law enforcement agency partners, dismantled two of the largest Darknet markets: AlphaBay and Hansa. Until that point, along with the Russian Anonymous Marketplace (RAMP), these three markets had accounted for 87% of all Darknet market activity[83].

AlphaBay was one of the largest criminal marketplaces to date, hosting over 200 000 users and 40 000 vendors. There were over 250 000 listings for illegal drugs and toxic chemicals on AlphaBay and over 100 000 listings for stolen and fraudulent identification documents, counterfeit goods, malware and other computer hacking tools, firearms and fraudulent services. The site was conservatively estimated to have had USD 1 billion pass through its ledgers since it opened its doors in 2014.

RAMP was the second largest Darknet marketplace. Unlike Alphabay and Hansa, RAMP did not use a market interface and instead used a classic forum structure. Moreover, the market was almost exclusively in Russian. The market was also shut down by Russian authorities in July 2017, although its fate was not revealed until September that year.

Hansa was the third largest criminal marketplace on the Dark Web, trading similarly high volumes in illicit drugs and other commodities. It was seized by the Dutch National Police, with the assistance of authorities in Germany and Lithuania. Hansa was covertly run by Dutch law enforcement for approximately one month prior to its take down, allowing them to collect valuable information on high-value targets and delivery addresses.

5 year flashback

The 2014 IOCTA closely followed the takedown of the infamous Silk Road marketplace by the FBI in October 2013. Even though it was dwarfed in size by some of its successors, Silk Road put Darknet markets firmly in the law enforcement and public spotlight and still epitomises this facet of the digital underground. Operation Onymous in late 2014 resulted in the takedown of a further 33 Darknet markets and a significant migration of illicit business to the largest two remaining markets at the time – Agora and Evolution.

This respite was to be short-lived however. In March 2015 Evolution performed an exit scam, taking with it USD 12 million of its members Bitcoins. Later that same year Agora voluntarily closed its doors, allegedly to address a security issue, but never reopened them. The Nucleus market, again one of the largest remaining markets at the time, then shut down in early 2016.

As described in this report, 2017 was a particularly tumultuous year for Darknet markets. The largest three Darknet markets – AlphaBay, Hansa and RAMP – were all taken down by international law enforcement and a series of other markets closed for a variety of reasons.

Vendors migrate to other markets but activity decreases overall

These events had a notable impact on the dark web community. The closure of any market will inevitably lead to the migration of customers and vendors to new or existing markets. Prior to the official announcement of the joint market seizures, Alphabay had been offline for several weeks. This had already resulted in a 25% increase in the number of listings appearing on Hansa, as it presumably absorbed the business from its chief competitor[84]. Three months after Alphabay went offline and following the closure of Hansa and RAMP, several of the remaining markets had similarly displayed considerable growth in the number of listings they advertised. Dream Market, the largest remaining English language market, had grown by 20%, while several of the smaller markets such as Wall Street, TradeRoute and T•Chka/P•int had grown by 290%, 475% and 840% respectively[85]. However, even collectively these markets did not meet the former scale of Alphabay, suggesting an overall decrease in dark web activity. Industry reporting supports this by highlighting that the value of Bitcoin transactions to Darknet markets fell by two thirds in the aftermath of the takedown operations[86].

Darknet markets are plagued by exit scams and closures

Throughout 2017, while the three largest Darknet markets were shut down as a result of law enforcement action, many more closed down either as a result of an exit scam by the administrators, hacks, voluntarily, or for unknown reasons.

Apple market, Outlaw market, Diabolus/SilkRoad3 and Trade Route all closed, taking with them the funds of the vendors and customers which were stored within the market infrastructure (in escrow). In some cases the markets were allegedly hacked and had their wallets stolen and were subsequently forced to close. In most cases though the administrators are believed to have simply abandoned the marketplaces and stolen the funds.

Several other markets, such as Acropolis, Infinite Market, Minerva, Placemarket and Pyramid market, simply closed their doors and shut up shop. Some of these markets were very short-lived; operational for only a few months.

Large market closures leading to more secondary markets

Several Member States suggest that another consequence of these market closures and of the regular DDoS attacks which frequently knock larger markets offline, is the growth in both the number of vendor shops (shops run by a single vendor) and secondary markets, i.e. non-English language markets catering to a particular nationality or language group.

Well-established vendors with high trust levels and reputation are more likely to set up their own hidden service platforms. Some of these vendors can continue doing business solely with clientele established on the now-defunct markets, especially in relation to sales of products that are purchased repetitively, such as drugs.

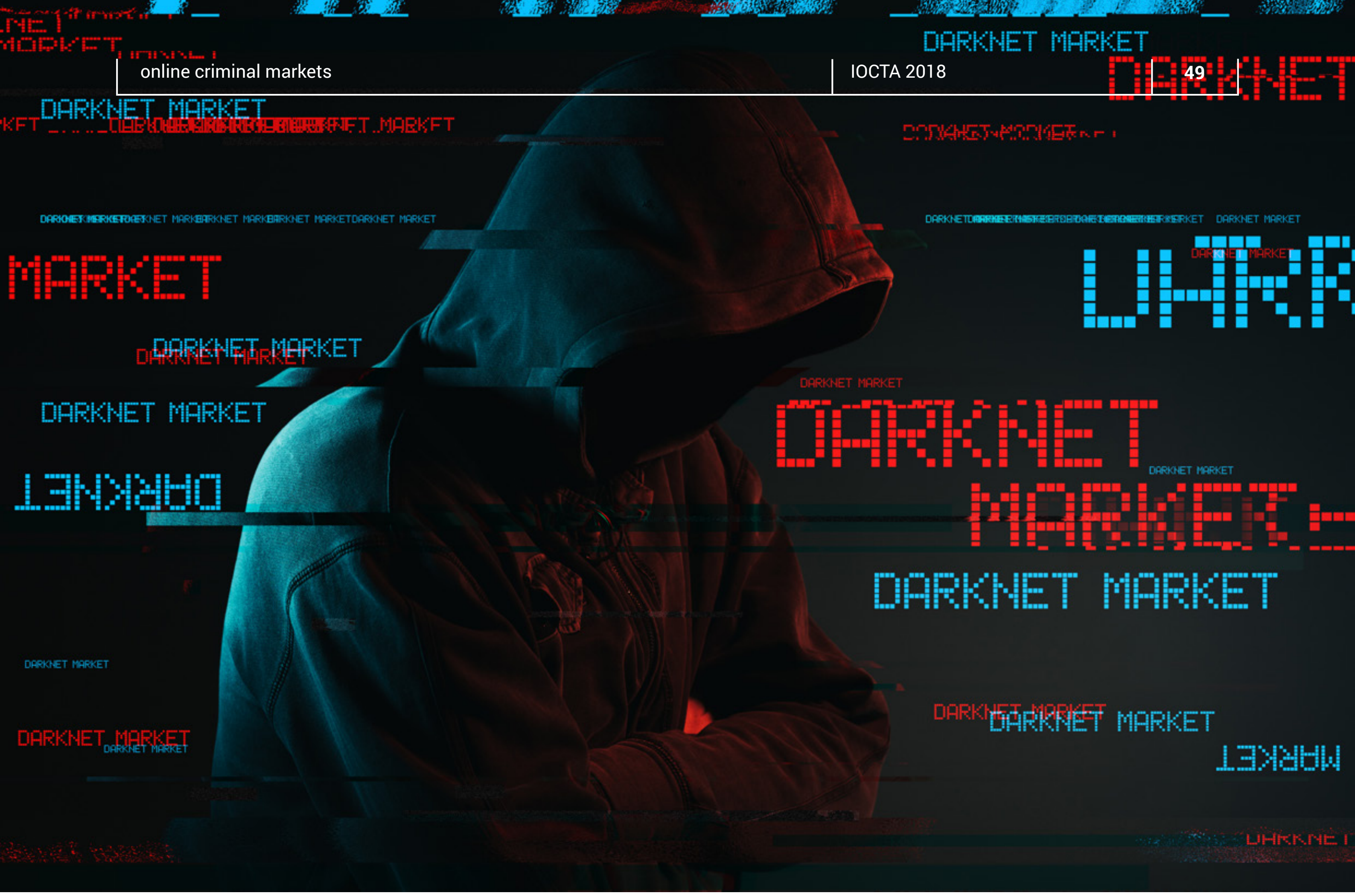
The online trade in drugs continues to dominate Darknet markets

The online trade in drugs continues to epitomise illicit trade on the dark web, accounting for the majority, if not the totality of the listings on many Darknet markets. Drugs are also the focus for the majority of dark web law enforcement investigations. Law enforcement authorities across the EU have noted a significant increase in the number of cases involving the trade in illicit drugs on Darknet markets over the last four years. However, the proportion of illicit drugs traded online remains small compared with the proportion traded through traditional distribution and trafficking networks. It remains to be seen whether this comparatively new channel of supply will supplement or otherwise affect drug demand[87].

According to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol, Germany, the Netherlands and the United Kingdom were the most important countries with regards to the EU-based Darknet drug supply, in terms of sales revenue and volumes[88]. Other research indicates that vendors of certain drugs commodities, such as cannabis and cocaine, are primarily located in a small number of highly active consumer countries. This further suggests that most Darknet market vendors are 'local' retailers serving the 'last mile' for drug trafficking routes[89]. This is supported by other research that Darknet markets are mostly used for mid- or low-volume market sales or sales directly to consumers. Large-volume sales (wholesale) on Darknet markets are relatively uncommon[90].

Darknet markets are of less importance to 'top-tier' cybercriminals

In last year's report we highlighted the marked growth in the volume of tools and services related to cyber-dependent crime on Darknet markets. With the downfall of most of the major markets which followed, this position is harder to clarify and requires further research. Nevertheless, a number of Member States report activity in relation to a variety of cybercrime tools and services including the provision of bullet proof hosting, counter anti-virus (CAV) services, DDoS services and malware.



While the number of cybercrime tools and services on Darknet markets is not insignificant, it has been observed that top-tier cyber criminals, i.e. those operating at the high-end of high risk, do not typically use the dark web. These groups are sufficiently well-established that they have a lesser need to engage with criminals on the comparatively adolescent Darknet markets in order to sell the proceeds of their criminality, instead operating within established criminal communities outside the Darknet.

The trade in counterfeit goods remains largely on the surface web

While Darknet marketplaces offer a range of counterfeit and pirated goods for sale, the majority of illicit trade still occurs on the surface web. The nature of the counterfeit commodity is reflected in which market it is sold. Counterfeit goods such as clothing, pharmaceuticals, electronics, or jewellery, which can be sold either wittingly or unwittingly as counterfeits of genuine articles, will typically be found on the surface web where they can reach the maximum customer base. Counterfeits such as ID documents or money, are unlikely to be found on the surface web and instead will be sold amidst the other clearly illicit commodities on the dark web.

As with other crime types, efforts to curtail the trade of counterfeit or pirated goods on the surface web Internet will likely result in a shift towards the dark web.

Compromised data is a key commodity on Darknet markets

As outlined in chapter 4.4, compromised personal, medical and financial data is a key commodity for the commission of cyber-dependent crime, but even more so for cyber-enabled crime. It plays a crucial role in activities such as frauds, phishing, identity theft and account takeovers. The prominence of data on Darknet

In November 2017, joint investigations by Europol’s Intellectual Property Crime Coordinated Coalition (IPC^3), the US National Intellectual Property Rights Coordination Centre and law enforcement authorities from 27 EU Member States and non-EU parties, facilitated by INTERPOL, seized over 20 520 domain names that were illegally selling counterfeit merchandise online to consumers.

This joint global recurrent operation ‘In Our Sites’ (IOS) was implemented in 2014 and has grown in scale year on year. The eighth edition of this global operation in 2017 saw a wide range of anti-counterfeiting associations and brand owner representatives joining law enforcement authorities participating in this huge worldwide action, to facilitate international cooperation and support the countries involved.

markets reflects this. Data is often the second or third largest category of commodity listed and one of the more common commodities highlighted by law enforcement.

In last year's report, we described the large number of automated credit card shops on the surface web. These are online stores which sell large quantities of compromised payment card data using a fairly standardised automated shopping interface. While a large number of these sites still exist on the surface web, there are a growing number of reports of such sites migrating to the dark web.

Weapons trade is still thriving on the dark web

The availability of firearms and explosives on Darknet markets remains a key concern for law enforcement. While it typically is one of the least common commodities found on Darknet markets, it is the one which represents the greatest potential danger to public safety. Buyer motivation ranges from feelings of insecurity to curiosity, a collecting passion, and preparation for private disputes, to possible planned criminal or terrorist offences.

The current top remaining markets handle weapons sales differently. Some, such as Dream market, simply do not allow weapons sales on the market. Others, such as P•int, do not openly list weapons, but users can find them on the market nonetheless. However, some markets do still openly list weapons. For example, as of June 2018, the Berlusconi Market has over 700 listings under the category of 'weapons', including ammunition, pistols, long-range guns, explosives and hand weapons. This represents approximately 5% of all listing on that particular market. Considering the markedly smaller customer base compared to commodities like drugs, this is a sizeable market.

7.3 / Future threats and developments

In previous years we have suggested that continued successful law enforcement action against markets on Tor will likely push these markets to other decentralised networks such as I2P or Freenet. However, even with all three top markets sensationally being taken offline by police in the space of a few months, the will or desire to migrate from the familiar territory of Tor to another, potentially safer digital environment still does not appear to be there. It therefore seems unlikely that this will come to pass in the foreseeable future.

7.4 / Recommendations

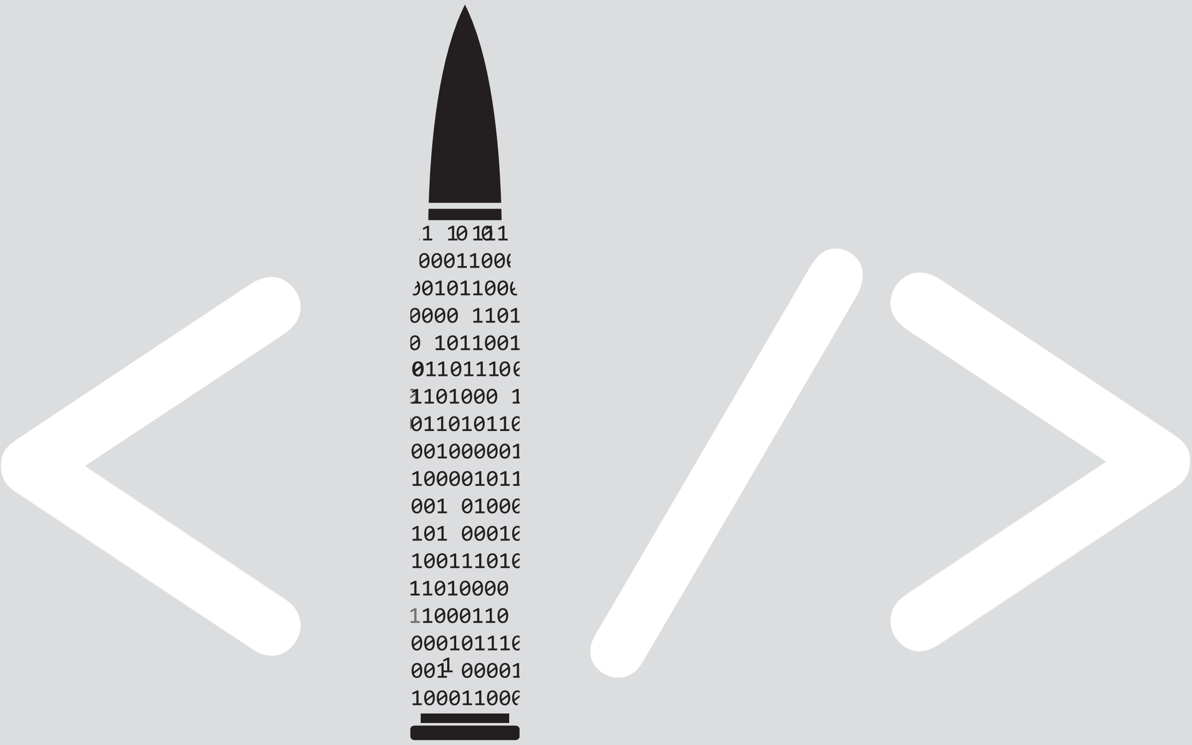
Criminality on the dark web spans multiple areas and involves a wide range of criminal commodities. An effective countermeasure will therefore require a suitably coordinated, cross-cutting response, involving investigators with equally diverse expertise. This will likely require additional capacity building 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.

5 year flashforward

Within the next five years, we can expect to see continued fragmentation of the Darknet market scene. While a number of larger, multi-vendor, multi-commodity markets may survive, there will be an increasing number of vendor shops and smaller secondary markets catering to specific nationalities or language groups. These smaller markets will be less likely to attract the coordinated international law enforcement response that larger markets invite.

Some vendors will abandon web shops altogether and migrate their business to encrypted communications apps, running their shops within private channels/groups[91] and automating the trade process using smart contracts and bots[92]. Industry and media already reports trend in the abuse of apps like Telegram or Discord, despite the provider's efforts to curtail such activity.



8_

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[93].

8.1 / 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.

8.2 / The use of the internet by terrorist groups

Terrorists groups are forced underground

Over the last few years, the take-down campaign carried out by law enforcement in association with OSPs pushed IS sympathisers underground. 2016 saw them migrate from their main hubs on Twitter and Facebook to encrypted messenger platforms such as Threema, Signal and Telegram. Telegram in particular offers a number of options for encrypted communications, including secret chats which cannot be forwarded and have a self-destruct timer. Over 2017 jihadist groups moved increasingly away from the public Telegram channels to the private and closed chat groups for which a link key – available for a short period of time and shared on associated channels – is needed to gain access. The need for increased secrecy also led online sympathisers to revert to blogs and traditional web forums (more adapted for peer-to-peer mentoring) as well as to smaller platforms with less capacity for – or focus on – carrying out disruptive procedures. They have also adventured further into the dark web.

As part of the armed conflict with the Islamic State, law enforcement agencies deployed pro-active cyber operations against the group's online capabilities[94]. On 25 April 2018 EU Member States, Canada and the USA launched a joint action against IS' propaganda machine – principally the Amaq News Agency but also al-Bayan radio, Halumu and Nashir News – with the purpose of severely disrupting their online infrastructure.

Terrorists promote ways to evade detection online

The Islamic State is more technologically sophisticated than its predecessors. It has purposefully reached out to tech-savvy recruits.

IS sympathisers have shared instructional videos offering tips about encryption and discussing the surveillance capabilities of hostile governments. Other tutorials have included advice on how to sign up to Twitter or Facebook without having to register a mobile phone number and how to deactivate GPS tagging when taking or posting a photo.

IS supporters have also been fighting back against the massive closure of IS supporter accounts on various platforms with volunteers building a pool of accounts (al-Ansar Bank or Bank of Supporters) on Facebook, Twitter, Gmail and Instagram. The purpose of al-Ansar Bank is to enable sympathisers to bypass the registration process (thereby ensuring their anonymity) and to retain an online presence when their accounts are shut down.

The IS remains in its infancy in terms of cyber-attack expertise

There has been much concern and speculation over the past few years that terrorists could turn to launching cyber-attacks against critical infrastructure. Yet, while their online propaganda appears technologically advanced and while IS hackers may be knowledgeable in encrypted communication tools, their cyber-attack tools and techniques remain limited. More to the point, they are still purchasing domain hosting services, downloading software and renting botnets for DDoS attacks rather than developing their own cyber weapons. However IS sympathisers do make it a point to stay up-to-date with the latest technological developments.

IS sympathisers have successfully carried out a small number of defacements and low-level hacks (e.g. of a Swedish radio station in November 2017 during which the hacker played an IS recruitment nashid) and in March 2018, IS supporters attempted to come up with a Facebook alternative. Dubbed "Muslim's Network", it was made available in Arabic, English and French. However, the platform was not an in-house development but had been purchased online for a small amount of money. Thus, while terrorist actors are aggregating open-source tools, they have yet to develop their own. With the crime-as-a-service business model of the digital underground however, there may of course be no need for them to do so.

Jihadist networks experiment with cryptocurrencies

Cryptocurrencies represent a source of opportunity for terrorist groups, allowing them to move funds across borders while avoiding the regular banking scrutiny. While the Islamic State saw the benefits of cryptocurrencies as early as 2014, it was not until the end of 2017 that IS sympathisers triggered mass cryptocurrency (Bitcoin and the more anonymous Zcash) donation campaigns in IS affiliated websites as well as in chat environments (e.g. Telegram) to support their cause.

The pro-IS website Akhbar al-Muslimin started calling for Bitcoin donations in November 2017. Initially, the link pointed to an external Bitcoin payment site; this then changed to a page within the website that generated Bitcoin addresses – thereby allowing sympathisers to copy the URLs and donate away from the page. This – alongside embedding malware within the website to mine for cryptocurrencies – shows a certain technical sophistication on the part of the administrators. Furthermore, the system allowed donors to use prepaid credit cards issued by "btc to plastic" service providers instead of their Bitcoin address.

Other IS-affiliated websites, including Dawaalhaq Islamic News Agency and Isdarat also solicited cryptocurrency donations in late 2017. Most of the funding was used to finance online infrastructure and to purchase hosting servers. However, one English-language social media campaign targeting Muslims in the West and dubbed Sadaqah, specifically stated when it was launched in November 2017 that it purported to supply fighters in Syria with weapons and other resources.

Yet despite the clear potential, none of the attacks carried out on European soil appear to have been funded via cryptocurrencies. The use of cryptocurrencies by terrorist groups has only involved low-level transactions – their main funding still stems from conventional banking and money remittance services[95].

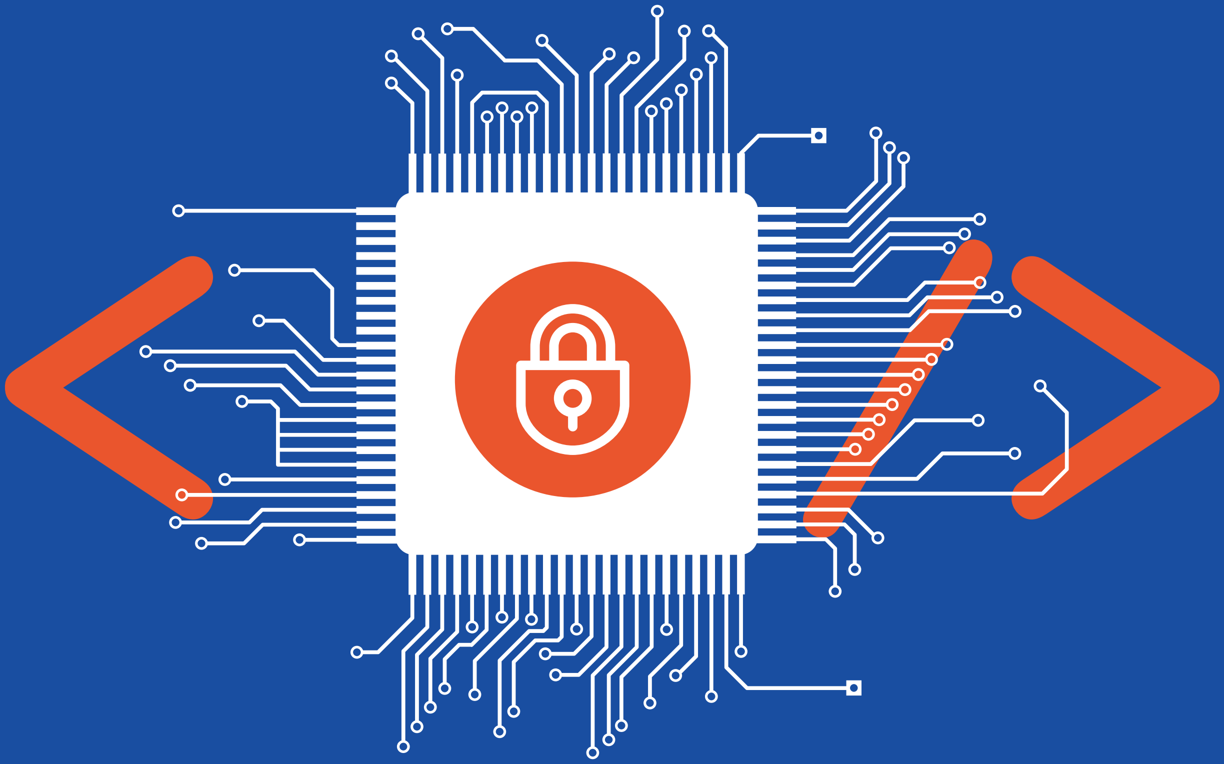
8.3 / Recommendations

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, 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.



9_

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.

9.1 / Key findings

West African fraudsters have adopted emerging fraud techniques, including those with a 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 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 cause harm to 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 remains the predominant cryptocurrency encountered in cybercrime investigations.

9.2 / Social engineering

Year on year, the significance of social engineering within both cyber-dependent and cyber-enabled crime continues to grow. Attacks involving social engineering take many forms. They can be complete attacks in their own right, creating pretext in order to convince victims to divulge information or act abnormally. Such attacks seldom involve any technical measures[96]. Alternatively, they can be a key component of a more complex attack, typically involving victims unwittingly installing malware by opening a malicious email attachment or following a link to a malicious website.

This type of attack occurs cross platform and includes phishing (by email), vishing (by phone) and smishing (by SMS), although many OCGs use them interchangeably.

Phishing remains the primary methodology used within social engineering attacks. In last year's report we indicated that almost 40% of Member States had active investigations into phishing. We also highlighted it as an increasing trend. Phishing was expected to further increase in light of the decline in the use of EKs and the consequent resurgence of other techniques to infect victims with malware. This year almost 75% of Member States reported cases of phishing, with further increases in case numbers expected over the next 12 months. The cases highlighted by law enforcement appear to be an even distribution of technical and pretextual attacks. Some states reported that this activity is occurring on a massive scale, but also indicated that few attempts are successful. This is corroborated by industry reporting, which suggests that only 4% of people targeted by a phishing attempts will click on the bait[97]. However, for technical attacks potentially only one person within an organisation needs to click in order for the attack to succeed.

In March 2018, a two-year long cybercrime investigation between the Romanian National Police and the Italian National Police, with the support of Europol, its J-CAT and Eurojust, led to the arrest of 20 suspects in Romania and Italy over a banking fraud which netted EUR 1 million from hundreds of customers of two major banking institutions. The OCG, comprised largely of Italian nationals, used spear phishing emails impersonating tax authorities to harvest the online banking credentials of their victims.

The highly organised OCG pursued its criminal activity using encrypted chat applications. It established its power by applying intimidating and punitive methods towards affiliates and competitors. The OCG is also suspected of money laundering, drug and human trafficking, prostitution and participation in a criminal organisation.

Social engineering threats were overwhelmingly prominent in reporting from our contributors in the financial sector[98]. Social engineering attacks not only target staff but also their customers. Compromised personal data can be used for account hijacking or identity theft and subsequent bank fraud.

The Anti-Phishing Working Group (APWG) has highlighted an increase in the use of HTTPS encryption protocol by phishing sites, from 5% of sites in 2016 to nearly one third of sites in 2017. The familiar green padlock (or word 'Secure' in the case of Google Chrome), means only that a valid SSL certificate has been obtained for the site and not that the website is either legitimate or even safe. Attackers exploit the potential confusion this creates to legitimise their phishing sites in the eyes of prospective victims[99].

While only 30% of Member States reported cases involving vishing, vishing was a common threat reported within the financial sector[100].

Business email compromise

Business email compromise (BEC) spans both cyber-dependent and cyber enabled crime. Many cases involve technical measures such as malware, whereas some are pure social engineering. This particular aspect of social engineering encapsulates two main forms of attack: CEO fraud whereby attackers impersonate a high-ranking individual within a company in order to initiate fraudulent payments and mandate fraud which aims to mislead employees into making payments meant for legitimate third parties into accounts under criminal control. The UK reports an additional variant – conveyancing fraud, whereby perpetrators purport to represent the other party in a property sale to redirect the funds to accounts they control.

Combined, these methodologies continue to result in significant losses and in some cases even bankruptcy for the affected company. Both also make extensive use of money mules to launder the stolen funds.

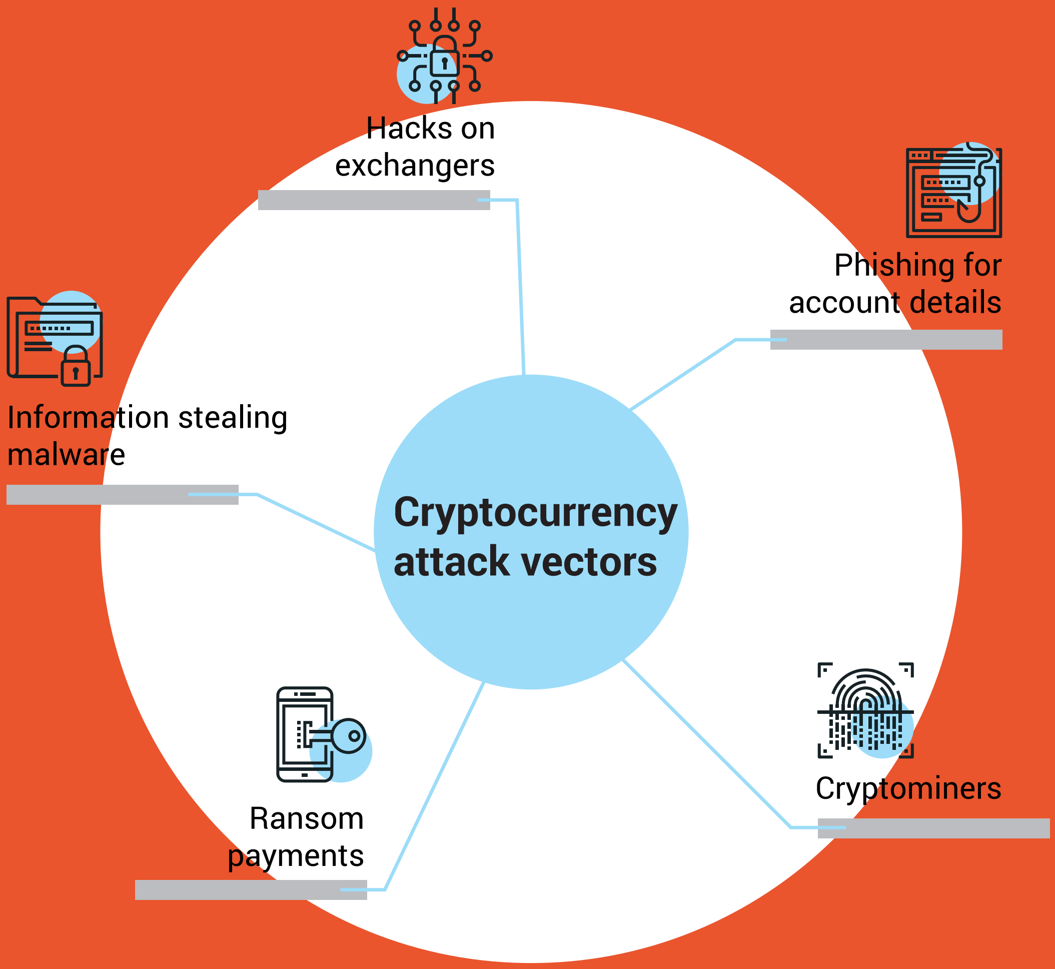
65% of Member States confirmed cases of CEO fraud, with over half of those stating that the crime was increasing year on year. Moreover, the majority of the financial sector contributors to this year's IOCTA also highlighted this as a key threat, targeting both them and their clients. While one Member State highlighted the role of Israeli OCGs, several others quoted the involvement of West African crime groups in perpetrating CEO fraud[102].

Classic scams are still going strong

While some of the aforementioned attacks are comparatively new, social engineering is of course not a new threat. Many frauds and scams have been operating successfully, with little change (or need for it) in their modus operandi since before BEC was even conceived. Technical support scams, (often referred to as Microsoft support scams), advance fee fraud and romance scams still feature prominently in law enforcement reporting, often use multiple platforms and still result in significant financial and emotional damage to their victims.

In February 2018, house searches in France led to the arrests of two individuals suspected of large-scale CEO fraud by the French National Gendarmerie. The criminals belonged to an OCG involved in at least 24 cases of CEO fraud causing EUR 4.6 million worth of loss.

The investigation was launched in June 2016 after two French companies fell victim to CEO fraud, incurring an estimated EUR 1.2 million in losses. The criminal investigation identified around 15 alleged Romanian company managers living in France and Belgium, who opened bank accounts and companies with the sole purpose of orchestrating CEO fraud and Forex scams. Two individuals, who were identified as recruiters and facilitators within the criminal group, were in charge of helping set up companies (such as law firms and notaries) with Romanian bank accounts. The bank accounts were then used to transfer money to Hong Kong by wiring it via different bank accounts in Romania[101].


Cryptocurrency attack vectors
Hacks on exchangers
Phishing for account details
Information stealing malware
Ransom payments
Cryptominers

9.3 / **Criminal finances**

In each previous report we have highlighted the growing role of cryptocurrencies: not only their criminal abuse, facilitating many aspects of cybercrime, but also their adoption as a conventional payment mechanism in the general populace and e-commerce.

A consequence of becoming more mainstream and a recent spike in value, is that cryptocurrency users and facilitators are now subjected to the same attacks aimed at users of traditional financial instruments – attackers now phish for victim's login credentials for their online exchanger accounts, information stealing malware also hunts for victim's electronic wallets and private keys and entities holding stocks of cryptocurrencies, such as exchangers, have become the target for hackers[103].

In 2016 we reported that there were almost 650 individually listed cryptocurrencies. In two years' time this has increased by approximately 250%, to almost 1 600 listed cryptocurrencies[104]. While most of these are more or less unknown, each of the top 25 has a market capacity in excess of USD 1 billion.

The great blockchain robbery

The growing demand for cryptocurrencies, no doubt fuelled by speculators hoping to cash in on the annual price booms, has resulted in a proliferation of exchange services operating globally. Such services not only hold their own float of cryptocurrencies for trading, but often also the funds of customers who have purchased cryptocurrencies and retain their funds within exchange (instead of transferring them to a privately held wallet). Such entities are understandably key targets for financially motivated criminals; a fact made evident by the number of hacks affecting exchangers in the last twelve months. The largest attack hit Japanese exchanger Coincheck, resulting in the loss of over USD 500 000 000 worth of NEM tokens[105]. Another attack on Italian exchanger BitGrail resulted in the loss of USD 195 000 000 worth of Nanos[106]. Notably, neither of these hacks involved Bitcoin.

Not only exchangers are at risk: in December 2017, Slovenian cloud mining service NiceHash was hacked, resulting in the loss of USD 60 000 000 worth of Bitcoins. This highlights how any entity retaining significant amounts of cryptocurrencies will likely be a key target for cybercriminals. Moreover, it is not only the funds these entities hold that are sought after, customer data is also targeted. Such data can be used to further fraud, including phishing customers for their account login credentials and subsequent currency theft. Theft of such data is unlikely to immediately raise the same alarms as a direct currency theft and as with many data breaches may even go undetected.

Bitcoin remains the most commonly used cryptocurrency in cybercrime

The abuse of cryptocurrencies by cybercriminals continues to play a pivotal role in the commission, perpetration and monetisation of cybercrime. They remain the primary payment mechanism for the payment of criminal services, a plethora of goods on Darknet markets and for extortion demands, whether as a result of ransomware, DDoS attacks, or other methods.

Historically Bitcoin enjoyed over 80% of the cryptocurrency market share, but by the start of 2017 this had dropped to less than 35%. However, this is not reflected in cybercrime investigations within the EU, where Bitcoin remains the most commonly encountered cryptocurrency. That said some Member States highlight a small shift towards more privacy orientated currencies such as Monero or Zcash.

While the criminal abuse of cryptocurrencies remains largely within the realm of cybercrime, some Member States reported that they are increasingly encountering their use by non-cyber OCGs.

In April 2018, Operation Tulipan Blanca, conducted by the Spanish Guardia Civil with the support of the Finnish authorities, the US HSI and coordinated by Europol, resulted in the arrest of 11 individuals with a further 137 investigated. Members of the OCG laundered money earned by other OCGs involved in the drug trade. The money launderers realised that cash withdrawals and bank operations were easy to track and changed their laundering methods to use cryptocurrencies. The criminals used a Finnish exchange to convert their illicit proceeds into Bitcoins and then changed the cryptocurrency into Colombian pesos to deposit into Colombian bank accounts. Finnish authorities were able to locate the local Bitcoin exchange and were able to obtain crucial information on the suspects. The investigation shows that the suspects deposited more than EUR 8 million in cash using 174 bank accounts.

Money laundering – it's not all about Bitcoin

Cryptocurrencies inherently offer users several features which facilitate the laundering of criminal proceeds – a decentralised infrastructure and pseudonymous transactions to name two. The more privacy-orientated currencies offer more features, such as coin mixing and stealth addresses.

In previous reports we have highlighted cryptocurrency exchangers as potential sources of investigative leads, as they represent nexuses where criminal crypto-funds cross over into the regulated financial system. These services have since evolved with the emergence of what have become known as swappers, which are semi-automated exchanges which do not require any Know Your Customer (KYC) procedures before they can be accessed. These exchanges allow users to exchange not only to fiat currencies, but also between different cryptocurrencies. We have also seen the arrival of decentralised exchanges, which allow peer-to-peer exchanges and likewise require no KYC to use. Several countries also highlighted the use of online gambling and betting sites to launder funds.

While cryptocurrencies continue to be the mainstay of illicit transactions online, many Member States report a wide range of other payment mechanisms used. The nature of the payment system used may reflect many things, including the nature of the payment (i.e. what it is for) or even the level of sophistication of the criminals involved. The variety of payment mechanisms encountered within cybercrime investigations during the reporting period included the use of centralised virtual currencies, voucher-based payment systems and payment cards. Many Member States reported the use of traditional bank accounts, typically in relation to money mules, or in frauds. The use of prepaid cards was also highlighted, including physically sending the cards to transfer ownership of the funds thereon. However, even card based payments cannot escape the influence of cryptocurrencies, as some Member States report criminals abusing Bitcoin-based credit cards.

Money mules are still going strong

Money mules remain a key component of the laundering of criminal proceeds and a common feature when investigating fraud against individuals and businesses. For the most part, the mule scene remains largely unchanged in terms of methodologies, recruitment and motivations of mules. However, it has been highlighted that cyber money mules have emerged as new actors in frauds and scams. Instead of merely providing bank accounts, these mules additionally use cryptocurrencies and make use of tumblers and mixing services to hide the transactions.

The use of social media accounts to actively recruit people as money mules to facilitate fraud was also noted this year. These accounts post images of fraud activity and offer easy money without mentioning the possible downsides. Some fraudsters operate multiple accounts in different names in order to conduct such recruitment, although some of these accounts are looking to defraud those who respond, rather than work with them to commit fraud.

In May 2018 the Spanish National Police supported by the Spanish Tax Agency, the Bulgarian Judicial Police and Europol dismantled an international poly-criminal group involved in money laundering, home burglaries and drug trafficking. The operation resulted in 14 arrests in Spain and 2 in Bulgaria. Amongst the assets seized by Spanish law enforcement was a virtual wallet containing EUR 220 000 in cryptocurrencies[107].

9.4 / Common challenges for law enforcement

In last year's report we covered a range of challenges for law enforcement, stemming from various technological or legislative developments, such as a loss of location, and issues related to public-private partnerships and legal frameworks. This year, as a result of a number significant of such developments, one of those challenges is especially relevant: the loss of data.

5G technology will inhibit attribution and lawful intercept

5G is the next generation of mobile network. Already in testing in many countries, 5G is expected to be launched worldwide in 2020. 5G is expected to meet the growing demands of our communication needs, in particular considering the growth in IoT technology, by providing faster and more reliable connections for all devices. As an emerging technology, 5G has received and receives a lot of attention with regards to privacy and security. ENISA, for example, published a study on the potential security caveats of 5G in March 2018.

5G poses a number of particular challenges for law enforcement. The ability of 5G technology to download data from multiple sources (such as Wi-Fi, network towers and satellite) simultaneously will make the investigation of communication events increasingly complex. Moreover, with current 4G technology law enforcement is able to use the unique identifier assigned to a device to attribute the device to an individual, but 5G replaces this with a temporary identifier, making attribution challenging.

Given that 5G is expected to carry exponential increases in data, at far higher speeds, with far greater security that ever before, the burden on both communications providers and law enforcement agencies to achieve lawful interception will be unprecedented.

WHOIS goes dark

As mentioned earlier in this report, the EU GDPR entered into effect on 25 May 2018. GDPR was designed to harmonise data privacy laws across Europe in order to better protect EU citizens' data privacy. It imposes obligations on companies that gather, process or hold the personal data of European residents, including constraints and requirements related to data retention, public access to data, international data transfers and data security. National Data Protection Agencies (DPAs) can impose heavy fines for organisations non-compliant with GDPR provisions.

While this has wide implications for law enforcements' ability to access data in general, one of the most debilitating repercussions, for cybercrime investigations in particular, relates to the WHOIS database, which as it stood, was considered non-compliant with the GDPR. On 17 May 2018 the Board of the Internet Corporation for Assigned Names and Numbers (ICANN) adopted a Temporary Specification[108] mandating registries and registrars to redact all personal data from publicly available WHOIS records. This is significantly hampering the ability of investigators across the world to identify and investigate online crime.

From 25 May law enforcement agencies need to initiate formal legal process and mutual legal assistance and get a specific authorisation from a prosecutor or a judge to obtain information on registrants of domain names from registries, registrars and lower-level providers. This comes with a substantial administrative burden as well as long delays which may be much longer than the period for which the data in question is being retained. By the time formal procedures are concluded, the data may therefore no longer exist.

Alternatively, some registries and registrars have started to provide request forms to ask for registrant information. They ask requestor's to provide their name, organisation, email address, which specific domains they want to access. Investigators are also asked to give pertinent details (including the legal basis for the request) and to explain their legitimate interest for access.

None of the access systems above are satisfying law enforcement needs.

Not only do they not scale (in order to map a botnet or an online criminal infrastructure, several thousands of WHOIS queries are necessary), but they also fail to protect the confidentiality of the investigation. In addition, there is no guarantee that registry or registrar operators will not notify their clients that their domain is being investigated.

It is important to highlight that this mainly affects the public WHOIS database related to generic Top Level Domains (gTLDs). While most European country code Top Level Domains (ccTLDs) also now hide certain data fields in response to the requirements of the GDPR, many ccTLDs are subject to national governance mechanisms and were not contractually required by ICANN to provide access to WHOIS data anyway.

The IP WHOIS does not appear to be affected by the requirements of the GDPR as it contains information about the legal entity that holds Internet number resources and the GDPR does not apply to legal entities but only to natural persons.

The law enforcement community is not the only one to use WHOIS routinely for investigations. WHOIS information is used by a variety of private and non-governmental actors to protect consumers, critical infrastructure and intellectual property rights. WHOIS information is used by many large organisations to monitor attacks and to inform cyber security and mitigation activity. Without this information their ability to protect themselves online will be significantly reduced in parallel with law enforcements ability to investigate cybercrime.

9.5 / Future threats and developments

While the use of EKs may be in decline, or at least diminished compared to previous years, it is still on-going and will likely be so as long as there are exploitable vulnerabilities out there. Even with training and awareness raising, human nature cannot so easily be changed; we can therefore expect continued growth in the volume of social engineering attacks on the whole, but more notably as a key component of more complex cyber-attacks.

West African OCGs have a long history with perpetrating social engineering scams. For several years, the significance of West African OCGs in cybercrime has been steadily growing[111],[112] and there are already clear examples of these actors successfully adopting newer social engineering tactics such as BEC, including attacks involving malware. High unemployment rates, combined with more technically capable attackers and a 'trust' environment between fraudsters where tactics and techniques are openly shared, will likely lead to a significant increase in technical and pretextual social engineering attacks from this region.

Africa continues to have the fastest growing internet globally[109],[110]. Within five years, at current expansion rates, it is likely that Africa will match Europe in numbers of internet users. As access to high-speed internet spreads across the continent, it will bring with it access to a global assemblage of victims for increasingly sophisticated and tech-savvy cybercriminals and a more significant role for West African OCGs within the EU.

> Looking forward, emerging technologies such as quantum computing, blockchain, robotics, artificial intelligence and machine learning are both expanding vulnerability surfaces and a domain in which public-private partnerships can flourish. Preparing for the dual (licit and illicit) use of these technologies and designing-in security and accountability mechanisms, as well as resilience to manipulation, will help maximise the benefits of such technologies while minimizing risks to citizens and governments alike.

Francesca Bosco, United Nations Interregional Crime and Justice Research Institute (UNICRI), Italy

With cryptocurrencies gaining greater acceptance within governments, e-commerce and the financial sector, cryptocurrency exchangers, on the whole, are slowly starting to operate in a manner that parallels the regulated financial sector. In many ways they are beginning to resemble banks themselves with regards to how they must manage and account for their customers; an ironic development given the ethos of decentralised economies surrounding cryptocurrencies. Mirroring this, the financial sector is also becoming more open to the concept of cryptocurrencies, as demonstrated by the emergence of Bitcoin futures trading. Proposals with the EU to tax transactions and capital gains with regards to cryptocurrencies, as USA has, may further drive regulation[113],[114].

To counter this, is has been demonstrated that cryptocurrencies supporting smart contracts could potentially be used to create automated, decentralised exchanges, which would require no KYC on the part of the users, thus allowing the users to remain anonymous and the exchange system completely decentralised. As smart contract technology and capability progresses, we can expect to see more of such innovation.

While banks combat the growing trend in business process compromise attacks, exchangers and other cryptocurrency depositories will increasingly be targeted by hackers[115]. Not only are such entities likely perceived as softer targets than corporate banks, but the profits of a successful hack can be comparably profitable and inherently easier to launder.

While Bitcoin remains the currency of choice for the majority of cybercrime enterprises, we anticipate a more pronounced shift towards more privacy orientated currencies. There are a number of drivers for this in addition to greater privacy, such as faster transaction times, lower transaction fees and less price volatility compared to Bitcoin. This shift will be exemplified by an increase in extortion demands and ransomware in these currencies.

We mentioned the use of mixing services and tumblers to facilitate the laundering of cryptocurrencies. However, we anticipate that the use of other coins with greater privacy will slowly replace the need for dedicated mixing services. During 2017, the two largest mixing services, helix - which was part of the Grams dark web search engine – and bitmixer.io, already ceased operating[116], [117].

On 18 June 2018, ICANN published a draft 'Framework Elements for a Unified Access Model for Continued Access to Full WHOIS Data'[118] for Community discussion. The objective is to help build an accreditation and access model for users with a legitimate interest to access differentiated subsets of the non-public registration data – also known as layered access model. However, ICANN is not expected to adopt such model before mid-2019 which will further undermine safety online.

Europol is working together with the European Commission to identify a solution which would ensure continuous access to domain name registration information for the European law enforcement community.

> Smart contracts are great at lowering transactions costs. People no longer need to rely on legal systems to enforce pay-outs after having submitted a digital proof that they have completed their part of a contract. The decentralised nature of the platforms such as Ethereum also means that the contracts cannot be stopped once they have been deployed. This is certainly useful for every economy and more so for economies in countries with unstable or slow legal systems; however, even more so for the economy that cannot rely on the legal system: the underground economy. We think that in the years to come we will see an increase in bribing attacks and fraud that base their attacks on smart contracts to attack other cryptocurrencies.
>
> *Dr Edgar Weippl, SBA Research, Austria*

9.6 / 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 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.

```
h3 {font-size: 20px !important;}
th {font-size: 11px; text-align: left;}
hr {margin: 3px !important; padding: 0px !important; padding-top: 5px !important; border-top: 1px solid #ccc !important;}

#container {margin: auto; width: 850px; padding-top: 90px;}

#info_bar_line1 {font-weight: bold; font-size: 20px; margin: 0; padding: 0; text-align: left;}
#info_bar_line2 {font-size: 14px; margin: 0; text-align: left;}
.info_bar {width: 100%; background-color: #428BCA; position: fixed; padding: 10px 20px; z-index: 10;}
.info_bar p {color: #ffffff !important;}

.hide {display: none;}

.field_information {cursor: pointer; float: left; margin: 1px 0 0 5px;}
.field_information_container {float: left; }
.label {font-size: 82% !important;}
.btn_copy_text {width: 110px;}
#btn_get_first {width: 110px;}

.title {width: 701px !important;}
.description {width:701px !important; height: 73px !important;}

.tag-editor {line-height: 25px !important; height: 225px; padding: 5px 0px !important; border: 1px solid #ccc !important; border-radius: 4px; overflow: auto !important;}
.tag-editor-delete {height: 25px !important;}
.tag-editor-delete i {line-height: 25px !important;}
.tag-editor-spacer {width: 10px !important;}

#btn_settings {-webkit-user-select: none; -khtml-user-select: none; -moz-user-select: none; -o-user-select: none; user-select: none; transition: all 0.5s ease-out 0s;}
#btn_settings:hover {cursor: pointer;transform: rotate(180deg);transition: all 0.5s ease-out 0s;}

#select_theme_container {width: 280px;}
#google_api_key {width: 400px;}
#get_first_n_value {width: 50px;}
.simple_text {text-decoration: none !important;}
.panel-settings {padding: 10px !important;}
.panel-settings-container {margin-bottom: 5px !important;}

#google_translate_api_info {font-size: 10px; margin-left: 35px;}
.checkbox_comment {font-size: 10px;}
.btn-default .badge {margin-left: 3px; border-radius: 5px !important;}
mark {padding: 0 !important;}

#add_and_translate {font-size: 10px;}

.tooltipster-box {background: #fff !important;}
.tooltipster-arrow-background {border-top-color: #fff !important;}
.tooltipster-box {-webkit-box-shadow: 0 1px 4px rgba(0,0,0,.2); box-shadow: 0 1px 4px rgba(0,0,0,.2)}
.tooltipster-arrow{height:10px !important;}
.tooltipster-content {margin: -2px 0px !important; }

#user_language {width: 50px;}
```

```
    <textarea id="description" class="form-control description" style="clear: both;" rows="2" tabindex="2"
    spellcheck="true" lang="en"></textarea>
  </div>
 ▶<div style="float: left; margin-top:25px; margin-left: 5px;"></div>
 </div>
▼<div style="clear: both; padding-top: 8px;">
 ▼<div class="keywords_info_bar">
    <label style="float: left;" for="keywords">Keywords</label>
  ▼<div class="field_information_container" style="padding-top: 5px;">
   ▶<a id="keywords_count_info" class="field_information label label-default" title="Maximum 50 words recommended"
     style="margin-top: -3px;"></a>
     <a id="keywords_log" class="field_information label label-default hide" title="" style="margin-top: -3px;">
     0 deleted</a>
    </div>
  ▶<div style="float: right; padding-top: 7px;"></div>
  </div>
  <div style="clear: both;"></div>
 ▶<textarea id="keywords" class="tag-editor-hidden-src" tabindex="3"></textarea>
 ▼<ul class="tag-editor ui-sortable">
  ▶<li style="width:1px"></li>
  ▼<li class="placeholder">
     <div>Enter keywords or paste via [illegible]</div>
    </li>
  </ul>
 ▶<textarea id="keywords_for_clipboard" style="position: absolute; left: [illegible];"></textarea>
 ▶<div class="btn_keywords_container" style="margin-top: 10px;"></div>
 ▶<div class="has-feedback has-clear" style="clear: both; padding-top: 5px;"></div>
```

10_

the geographic distribution of cybercrime

The following is a brief summary of geographic threats and cybercrime activity throughout 2017 based on law enforcement and industry data.

10.1 / The Americas

The Americas, particularly the USA, continue to be both a key originator of global cyber-attacks and a target for cyber-attacks originating both domestically and from overseas[120].

Industry reporting indicates that the USA and to a lesser extent Canada, is a primary target for global ransomware attacks[121]. The USA is also the top focus for attacks by targeted attack groups and mobile malware[122]. The USA has been the world's second largest host of botnet-forming compromised IoT devices since 2016[123]. Moreover, the APWG identifies both the USA and Canada as top countries for the hosting of phishing sites, with the USA dominating those figures by some margin[124].

Latin America also features heavily in cyber security reporting. Lack of adequate cybercrime legislation has resulted in Brazil being both the number-one target and the leading source of online attacks in Latin America; 54% of cyber-attacks reported in Brazil allegedly originate from within the country[125]. Similar to the USA, Brazil is also a top host of phishing sites[126], with some reporting putting Brazil as one of the world's top ten originators of all cyber-attacks[127].

The profile of Mexico is becoming increasingly prominent, with Mexico suffering from the largest number of cyber-attacks in Latin America after Brazil[128]. Both Brazil and Mexico suffer from malicious URL containing emails, which are coupled with some of the world's highest rates of spam[129].

The primary threat coming from the Americas as a whole, from a law enforcement perspective, relates to various aspects of payment fraud.

10.2 / Europe

The majority of cyber threats affecting Europe continue to emanate from within Europe, either domestically, or from other European countries. The current emphasis on the use of email as an attack vector is clearly demonstrated in some of the trends highlighted by industry. Austria, Germany, Hungary, Italy, Russia, Spain and the UK, had some of the highest global rates of malicious emails containing malware,[130],[131] while Ireland, Norway and Sweden similarly had some of the highest global rates of email containing malicious URLs[132]. Moreover, the Netherlands, Hungary, Portugal and Austria, also suffered from high global rates of phishing emails[133]. In some cases this was exacerbated by some of the world's highest rates of spam[134].

These attacks also account, at least in part for the fact that a significant proportion of global attacks originating from compromised IoT devices stem from a number of Europe countries[135]. Moreover, some EU countries, such as France and Germany are significant global sources of spam[136].

Law enforcement outlined a wide variety of cyber-attacks emanating from other European countries, although there was strong emphasis on various aspects of payment fraud. In this regard, Bulgaria and Romania were highlighted as having a key role.

10.3 / The Middle East and Africa

In previous year's reports we highlighted the growing significance of Africa as a source of both cyber enabled and increasingly cyber-dependent crime. This trend continues with several Member States emphasising the role of West African OCGs in increasingly sophisticated cybercrime. While 'traditional' social engineering scams still epitomise the crimes associated with this region, as outlined in chapter 9.2, social engineering combined with technical attacks involving malware are becoming more commonplace. In addition to payment card fraud, several Member states also highlight the growing role of Africa as a source of CSEM, including LDCA.

A 2017 report by Trend Micro details a burgeoning digital underground active in the Middle East and North Africa[119]. The report highlights that while the scale and scope of products and services does not compare to more mature markets, a wide variety of malware, crime tools and weapons is still available on these markets. Such markets are however, heavily influenced by culture and ideology and consequently operate very differently to the criminal markets European investigators may be familiar with. It is common practice to share code, malware, or instruction manuals for free in a 'spirit of sharing'. The main cyber activity carried out on these fora, is hacktivism and largely limited to website defacement and DDoS attacks. However, it is anticipated that these markets will evolve and mature into more serious attacks, particularly given the already visible influence of the Russian underground.

> Clearly, internet crimes reduce the importance of colocation of victim and offender. However, unless (like Chip and PIN) there are different control mechanisms in different parts of the world, experimentation can take place in one area that can then be tried out in other less protected or target-rich environments.
>
> *Professor Michael Levi, Cardiff University, UK*

10.4 / Asia

Based on industry reporting, cyber-attacks directed towards Asia countries appear to follow a different profile and methodology compared to those commonly encountered in European. While emails loaded with malicious attachments are still noted in several south-east Asian countries[139], the use of malicious URLs to the same effect appears to be very limited[140]. However, higher rates of phishing, particularly again in Southeast Asia, suggests that compromised credentials are still highly valued[141]. China also has one of the world's highest rates of spam[142]. Asia also appears to be one of the primary regions subjected to targeted cyber-attacks. While the US was top for such attacks, seven Asian countries featured within the top ten[143].

As discussed in chapter 4.2, Asia is one of the regions particularly plagued by mobile malware, with several Asian countries featuring in various top ten lists of mobile threats, although that particular threat is concentrated in the US[144]. China is also consistently the home the highest number of botnet-forming IoT devices, by some margin[145].

10.5 / Oceania

As in previous years' reports, while Oceania still suffers from cybercrime internally, it does not often feature in EU investigations. The major cyber-threats reported by the Australian Cyber Security Center (ASCS) mirror those reported by the EU – ransomware, data stealing malware (including the mobile variety), social engineering, DDoS, supply chain attacks and growing levels of state-sponsored activity[137].

Oceania also typically did not feature in industry reporting with the exception of both Australia and New Zealand both being in receipt of significant proportions of emails containing malicious URLs[138].

references

1 Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M., ‘Cyberfraud and the implications for effective risk-based responses: themes from UK research’, Crime, Law and Social Change, Vol. 67(1), 2017, pp. 77–96.

2 Contribution to the 2018 IOCTA: EBF.

3 Beer, J., “WannaCry” ransomware attack losses could reach $4 billion, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/, 2017.

4 Check Point Software Technologies, 2018 Security Report, 2018.

5 Hay Newman, L., The leaked NSA spy tool that hacked the world, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world

6 https://noransom.kaspersky.com/

7 Morgan, S., Global ransomware damage costs predicted to hit $11.5 billion by 2019, https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/, 2017.

8 Spring, T., Google study quantifies ransomware profits, https://threatpost.com/google-study-quantifies-ransomware-revenue/127057/, 2017.

9 Spring, T., Google study quantifies ransomware profits, https://threatpost.com/google-study-quantifies-ransomware-revenue/127057/, 2017.

10 Morgan, S., Global ransomware damage costs predicted to exceed $5 billion in 2017, https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/, 2017.

11 Contribution to the 2018 IOCTA: EBF.

12 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 79.

13 TrendLabs, 2017 Annual Security Roundup: the paradox of cyberthreats, 2018, pp. 30–31.

14 Symantec, Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 79.

15 Greenfield, P., Government websites hit by cryptocurrency mining malware, https://www.theguardian.com/technology/2018/feb/11/government-websites-hit-by-cryptocurrency-mining-malware, 2018.

16 Osborne, C., 500 million PCs are being used for stealth cryptocurrency mining online, https://www.zdnet.com/article/500-million-pcs-are-being-used-for-stealth-cryptocurrency-mining-online/, 2017.

17 Finkle, J. and Hosenball, M., U.S., UK government websites infected with crypto-mining malware: report, https://www.reuters.com/article/us-bitcoin-cyber/u-s-uk-government-websites-infected-with-crypto-mining-malware-report-idUSKBN1FV0VO, 2018.

18 Meshkov, A., Cryptocurrency mining affects over 500 million people. And they have no idea it is happening, https://blog.adguard.com/en/crypto-mining-fever/, 2017.

19 Metropolitan.fi, Bitcoin mining malware grinds healthcare systems to a halt in Finland, https://metropolitan.fi/entry/bitcoin-mining-halts-healthcare-data-system-in-finland, 2018.

20 Check Point Software Technologies, ‘Malware meets crypto-currencies’, 2018 Security Report, 2018, pp. 16.

21 TrendLabs, 2017 Annual Security Roundup: the paradox of cyberthreats, 2018, pp. 16.

22 Contribution to the 2018 IOCTA: ISAG.

23 Khandelwal, S., Cryptocurrency mining malware infected over half-million PCs using NSA exploit, https://thehackernews.com/2018/01/cryptocurrency-mining-malware.html, 2018.

24 Cision, Radiflow reveals first documented cryptocurrency malware attack on a SCADA network, https://www.prnewswire.com/news-releases/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network-300595714.html, 2018.

25 TrendLabs, 2017 Annual Security Roundup: the paradox of cyberthreats, 2018, pp. 30.

26 Cimpanu, C., The rig exploit kit has forsaken ransomware for coinminers, https://www.bleepingcomputer.com/news/security/the-rig-exploit-kit-has-forsaken-ransomware-for-coinminers/, 2018.

27 Cimpanu, C., The rig exploit kit has forsaken ransomware for coinminers, https://www.bleepingcomputer.com/news/security/the-rig-exploit-kit-has-forsaken-ransomware-for-coinminers/, 2018.

28 Segura, J., RIG exploit kit campaign gets deep into crypto craze, https://blog.malwarebytes.com/threat-analysis/2018/01/rig-exploit-kit-campaign-gets-deep-into-crypto-craze/, 2018.

29 Verizon, ‘Ransomware, botnets, and other malware insights’, 2018 Data Breach Investigations Report, 2018, pp. 18.

30 Panda Security, PandaLabs Annual Report 2017, 2017, pp. 18.

31 Europol, Andromeda botnet dismantled in international cyber operation, https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation, 2017.

32 Djurberg, J. A., Bekräftat: ddos-attack bakom tågförseningar [Confirmed: DDOS attack behind train delays], https://computersweden.idg.se/2.2683/1.690504/ddos-bakom-tagforseningar, 2017.

33 Farmer, B., Russia was behind ‘malicious’ cyber-attack on Ukraine, Foreign Office says, https://www.telegraph.co.uk/news/2018/02/15/russia-behind-malicious-cyber-attack-ukraine-foreign-office/, 2018.

34 Verizon, ‘Ransomware, botnets, and other malware insights’, *2018 Data Breach Investigations Report*, 2018, pp. 9.

35 Armerding, T., The 17 biggest data breaches of the 21st century, https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, 2018.

36 Contribution to the 2018 IOCTA: EBF.

37 Contribution to the 2018 IOCTA: EBF

38 Verizon, ‘Ransomware, botnets, and other malware insights’, *2018 Data Breach Investigations Report*, 2018, pp. 5.

39 Verizon, ‘Ransomware, botnets, and other malware insights’, *2018 Data Breach Investigations Report*, 2018, pp. 5.

40 PandaLabs PandaLabs Annual Report 2017, 2017, pp. 6.

41 Verizon, ‘Ransomware, botnets, and other malware insights’, *2018 Data Breach Investigations Report*, 2018, pp. 5.

42 Contribution to the 2018 IOCTA: EBF.

43 Verizon, ‘Ransomware, botnets, and other malware insights’, *2018 Data Breach Investigations Report*, 2018, pp. 8.

44 Check Point Research, A new IoT botnet storm is coming, https://research.checkpoint.com/new-iot-botnet-storm-coming, 2017.

45 Palmer, D., Cryptocurrency mining malware now as lucrative as ransomware for hackers, https://www.zdnet.com/article/cryptocurrency-mining-malware-now-as-lucrative-as-ransomware-for-hackers, 2018.

46 Contribution to the 2018 IOCTA: EBF.

47 Contribution to the 2018 IOCTA: EBF.

48 Contribution to the 2018 IOCTA: ISAG.

49 Greenberg, A., How an entire nation became Russia's test lab for cyberwar, https://www.wired.com/story/russian-hackers-attack-ukraine, 2017.

50 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 83.

51 Draft Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises, 10085/18, 19 June 2018.

52 Explicit material produced by the victim themselves, either willingly, or unwillingly as a result of, for example, sexual extortion.

53 WePROTECT Global Alliance, Global threat assessment 2018, 2018.

54 Cybertip, Groundbreaking tool to remove online child sexual abuse material, https://www.cybertip.ca/app/en/projects-arachnid, 2017.

55 Gibbs, S., Child abuse imagery found within Bitcoin's blockchain, https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content, 2018.

56 Internet Watch Foundation, Annual Report 2017, 2017, pp. 5.

57 Netclean, Netclean Report 2017, 2017.

58 Europol, Eight arrested for distribution of child sexual abuse material through Skype and the darknet, www.europol.europa.eu/newsroom/news/eight-arrested-for-distribution-of-child-sexual-abuse-material-through-skype-and-darknet, 2018.

59 Netclean, Netclean Report 2017, 2017.

60 WePROTECT Global Alliance, Global threat assessment 2018, 2018, pp. 20.

61 Netclean, Netclean Report 2017, 2017.

62 WePROTECT Global Alliance, Global threat assessment 2018, 2018.

63 WePROTECT Global Alliance, Global threat assessment 2018, 2018.

64 Netclean, Netclean Report 2017, 2017.

65 WePROTECT Global Alliance, Global threat assessment 2018, 2018.

66 Traynor, V., Dublin man used social media to sexually exploit young girls, https://www.rte.ie/news/courts/2018/0122/935176-matthew-horan-court/, 2018.

67 Davies, C., 'Sadistic' paedophile Matthew Falder jailed for 32 years, https://www.theguardian.com/technology/2018/feb/19/dark-web-paedophile-matthew-falder-jailed-for-32-years, 2018.

68 WePROTECT Global Alliance, Global threat assessment 2018, 2018.

69 Terre des Hommes, The dark side of the internet for children. Online child sexual exploitation in Kenya – a rapid assessment report, 2018.

70 Terre des Hommes, Children of the webcam. Updated report on webcam child sex tourism, 2016.

71 EFC meeting.

72 Terre des Hommes, The dark side of the internet for children. Online child sexual exploitation in Kenya – a rapid assessment report, 2018.

73 Contribution to the 2018 IOCTA: Romania, SIENA 1172256.

74 Internet Watch Foundation, Trends in online child sexual exploitation: examining the distribution of captures of live-streamed child sexual abuse, 2018.

75 Aiken, M., Forensic cyberpsychology: a content analysis approach to investigating and comprehending the self-production of indecent images by minors, Doctoral dissertation, Middlesex University, 2015.

76 European Payments Council, 2017 Payment Threats and Fraud Trends Report, 2017, pp. 68.

77 European Payments Council, 2017 Payment Threats and Fraud Trends Report, 2017, pp. 6.

78 Europol, 195 individual detained as a result of global crackdown on airline ticket fraud, https://www.europol.europa.eu/newsroom/news/195-individuals-detained-result-of-global-crackdown-airline-ticket-fraud, 2017.

79 ATM jackpotting involves connecting an unauthorised device to an ATM and sending dispense commands so the criminal can withdraw cash without having to use a credit or debit card.

80 Black box attacks require the attacker to physically breach the ATM (by drilling or forging a hole) in order to connect their device.

81 Mennes, F., Open banking APIs under PSD2: how to mitigate risk, https://blog.vasco.com/legal/open-banking-apis-under-psd2-how-to-mitigate-risk/, 2018.

82 Total System Services, European Fraud Trends, 2017.

83 Chainalysis, The changing nature of cryptocrime, 2018, pp. 4.

84 Europol data.

85 Europol data.

86 Chainalysis, The changing nature of cryptocrime, 2018, pp. 4.

87 European Monitoring Centre for Drugs and Addiction and Europol, Drugs and the darknet, 2017, pp 51.

88 European Monitoring Centre for Drugs and Addiction and Europol, op. cit., pp. 33.

89 Dittus, M., Wright, J., Graham, M., Platform Criminalism: The 'last-mile' geography of the darknet market supply chain, in WWW 2018, April 23–27 2018, Lyon, France, 2018.

90 European Monitoring Centre for Drugs and Addiction and Europol, op. cit., pp. 53.

91 Digital Shadows, Seize and desist? The state of cybercrime in the post-AlphaBay and Hansa age, 2018, pp. 10.

92 Dark Web News, Telegram: the app used for the drug trade, http://darkwebnews.com/drugs/drug-trade-app-telegram/, 2018.

93 Callimachi, R., Not 'lone wolves' after all: how ISIS guides world's terror plots from afar, https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html, 2017.

94 Segal, A., Year in review: militaries got more cyber in 2016, https://www.cfr.org/blog/year-review-militaries-got-more-cyber-2016, 2016.

95 Center for a New American Security, Terrorist use of Virtual Currencies: Containing the Potential Threat, 2017.

96 Verizon, ‘Ransomware, botnets, and other malware insights’, 2018 Data Breach Investigations Report, 2018, pp. 11.

97 Verizon, ‘Ransomware, botnets, and other malware insights’, 2018 Data Breach Investigations Report, 2018, pp. 12.

98 Contribution to the 2018 IOCTA: EBF, FSAG.

99 Anti-Phishing Working Group (APWG), Phishing Activity Trends Report 4th Quarter 2017: unifying the global response to cybercrime, 2017, pp. 6.

100 Contribution to the 2018 IOCTA: EBF, FSAG.

101 Europol, Two arrested in France for major CEO fraud, https://www.europol.europa.eu/newsroom/news/two-arrested-in-france-for-major-ceo-fraud, 2018.

102 Contribution to the 2018 IOCTA: Belgium, Denmark, Sweden, United Kingdom.

103 Contribution to the 2018 IOCTA: EBF, FSAG, ISAG

104 https://coinmarketcap.com/

105 Moon, M., Coincheck loses $400 million in massive cryptocurrency heist, https://live.engadget.com/2018/01/27/coincheck-hack/, 2018.

106 Morris, D. Z., Bitgrail cryptocurrency exchange claims $195 million lost to hackers, http://fortune.com/2018/02/11/bitgrail-cryptocurrency-claims-hack/, 2018.

107 Europol, Poly-criminal group involved in money laundering, home burglaries and drug trafficking busted, https://www.europol.europa.eu/newsroom/news/poly-criminal-group-involved-in-money-laundering-home-burglaries-and-drug-trafficking-busted, 2018.

108 ICANN, Temporary specification for gTLD registration data, https://www.icann.org/resources/pages/gtld-registration-data-specs-en, 2018.

109 Hootsuite, We Are Social, Digital in 2018. Essential insights into internet, social media, mobile, and e-commerce use around the world, 2018, pp. 13.

110 Internet World Stats, Internet users in the world by regions – December 31 2017, https://www.internetworldstats.com/stats.htm, 2018.

111 Trend Micro and INTERPOL, Cybercrime in West Africa: poised for an underground market, 2017.

112 Trend Micro, Africa: A New Safe Harbor for Cybercriminals?, 2013.

113 Roberts, J.J., Bitcoin and taxes: what you need to know about cryptocurrency and the IRS, http://fortune.com/2018/01/29/bitcoin-taxes-cryptocurrency-irs/, 2018.

114 Tassev, L., 0 to 50% – time to pay crypto taxes in the European “Union”, https://news.bitcoin.com/0-to-50-time-to-pay-crypto-taxes-in-the-european-union/, 2018.

115 Contribution to the 2018 IOCTA: EBF.

116 Redman, J., One of the Largest Bitcoin Mixing Services Closes its Doors, https://www.bleepingcomputer.com/news/technology/internets-largest-bitcoin-mixer-shuts-down-realizing-bitcoin-is-not-anonymous, 2017

117 Aliens, C., https://www.deepdotweb.com/2017/12/15/darknet-search-engine-grams-shutting, 2017

118 ICANN, Framework elements for unified access model for continued access to full WHOIS fata – for discussion, https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-18jun18-en.pdf, 2018.

119 Trend Micro, Digital souks: a glimpse into the Middle Eastern and north African underground, 2017.

120 ThreatMetrix, Q4 2017 Cybercrime Report, 2018, pp. 14-15.

121 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 61.

122 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 76–79.

123 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 80.

124 Anti-Phishing Working Group (APWG), Phishing Activity Trends Report 4th Quarter 2017: unifying the global response to cybercrime, 2017.

125 McAfee, The economic impact of cybercrime, 2018, pp. 20.

126 Anti-Phishing Working Group (APWG), Phishing Activity Trends Report 4th Quarter 2017: unifying the global response to cybercrime, 2017.

127 ThreatMetrix, Q4 2017 Cybercrime Report, 2018, pp. 14.

128 McAfee, The economic impact of cybercrime, 2018, pp. 22.

129 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 69-74.

130 Demidova, N., Shcherbakova, T., Vergelis, M., Spam and phishing in Q1 2018, https://securelist.com/spam-and-phishing-in-q1-2018/85650, 2018.

131 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 69.

132 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 69.

133 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 72.

134 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 74.

135 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 80.

136 Demidova, N., Shcherbakova, T. and Vergelis, M., Spam and phishing in Q1 2018, https://securelist.com/spam-and-phishing-in-q1-2018/85650, 2018.

137 Australian Cyber Security Centre, 2017 Threat Report, 2018, pp. 15–16.

138 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 69.

139 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 69.

140 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 69.

141 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 72.

142 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 74.

143 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 76.

144 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 79.

145 Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018, pp. 80.

IOCTA
2018

ISBN 978-92-95200-94-4
DOI 10.2813/858843
QL-AL-18-001-EN-N

EUROPOL | EC3
European Cybercrime
Centre

www.europol.europa.eu