INTERNET ORGANISED CRIME THREAT ASSESSMENT

IOCTA 2017

EUROPOL

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2017

This publication and more information on Europol are available online:

www.europol.europa.eu

Twitter: @Europol and @EC3Europol

PHOTO CREDITS

All images © Shutterstock
except pages 6, 20, 26, 33, 35, 36, 44 and 59 © Europol.

ISBN 978-92-95200-80-7
ISSN 2363-1627
DOI 10.2813/55735
QL-AL-17-001-EN-N

IOCTA
2017

CONTENTS

FOREWORD

I am pleased to present the 2017 Internet Organised Crime Threat Assessment (IOCTA), the fourth annual presentation of the cybercrime threat landscape by Europol's European Cybercrime Centre (EC3).

The report provides a predominantly law enforcement focused assessment of the key developments, changes and emerging threats in the field of cybercrime over the last year. It relies on the invaluable contributions of the EU Member States, and our partners in private industry, the financial sector and academia, as well as the expert input of Europol staff.

This year's report highlights how cybercrime continues to grow and evolve, taking new forms and directions, as demonstrated in some of the attacks of unprecedented scale of late 2016 and mid-2017.It further highlights the progressive convergence of cyber and serious and organised crime, supported by a professional underground service economy.

The report also describes some of the key challenges faced by law enforcement in terms of investigation and prosecution of cybercrime, highlighting many cross-cutting issues such as e-evidence challenges, and the need for adequate and harmonised legislation to address the specificities of cybercrime. The report goes on to list a number of key recommendations to address the phenomenon of cybercrime and identifies several priority topics to inform the definition of operational actions for EU law enforcement in the framework of the EU Policy Cycle. These include concrete actions under EC3's three main mandated areas – child sexual exploitation online, cyber-dependent crime, and payment fraud, as well as cross-cutting crime enablers.

As in previous years, the 2017 IOCTA will inform the setting of priorities and help streamline resources within the EU and internationally to respond to cybercrime in an effective and concerted manner. Law enforcement continues to demonstrate that a coordinated, intelligence-led and adaptive approach by competent authorities, involving multiple sectors and partners can result in significant success in preventing cybercrime and mitigating its impact.

Rob Wainwright
Executive Director of Europol

ABBREVIATIONS

ACS	Automated Card Shop
ADSL	Asymmetric Digital Subscriber Line
AIOTI	Alliance for Internet of Things Innovation
APT	Advanced Persistent Threat
APWG	Anti-Phishing Working Group
AQ	al-Qaeda
ATM	automated teller machine
AV	anti-virus
AVC	Automated Vending Card
BEC	Business Email Compromise
CaaS	Crime-as-a-Service
CAM	child abuse material
CEO	chief executive officer
CERT	computer emergency response team
CGN	Carrier-Grade Network Address Translation
CI	critical infrastructure
CJEU	European Court of Justice
CNP	card-not-present
CSE	child sexual exploitation
CSEM	child sexual exploitation material
CSIRT	Computer Security Incident Response Team
CVV	Card Verification Value
DDoS	Distributed Denial of Service
DEA	United States Drug Enforcement Agency
DNS	Domain Name System
DRD	Data Retention Directive
EAST	European Association for Secure Transactions
EBF	European Banking Federation
ECTEG	European Cybercrime Training and Education Group
EC3	European Cybercrime Centre
EIO	European Investigation Order
EMAS	Europol Malware Analysis System
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
EUCTF	European Cybercrime Task Force
EUIPO	European Union Intellectual Property Office
FBI	United States Federal Bureau of Investigation
GAAD	Global Airport Action Day
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communications
HDFS	Hadoop Distributed File System
I2P	Invisible Internet Project
IAP	Internet Access Provider
ICS	Industrial Control Systems
ICSE	Interpol International Child Sexual Exploitation database
ICT	information & communications technology
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
IP	Internet Protocol
IPC3	Intellectual Property Crime Coordinated Coalition
IPR	intellectual property rights
IPv4	Internet Protocol version 4
IRC	Internet Relay Chat
IRU	EU Internet Referral Unit
IS	Islamic State
ISDN	Integrated Services Digital Network
ISP	Internet service provider
IT	information technology
IWF	Internet Watch Foundation
J-CAT	Joint Cybercrime Action Taskforce
KYC	Know Your Customer
LDCA	Live-Distant Child Abuse
LEA	law enforcement agency
MBR	Master Boot Record
MO	modus operandi
MOTO	Mail Order/Telephone Order
mTAN	Mobile Transaction Authentication Number
NAT	Network Address Translation
NCMEC	National Center for Missing and Exploited Children
NFC	Near Field Communication
NGO	non-governmental organisation
NIS	network and information systems
NPS	new psychoactive substances
OCG	organised crime group
OPSEC	operations security
OSINT	open-source intelligence
OTP	one-time pad
P2P	peer to peer, or people to people
PBX	Private Branch Exchange
PIN	personal identification number
PoS	point-of-sale
QKD	Quantum Key Distribution
RAT	Remote Access Trojan
SCADA	supervisory control and data acquisition systems
SCE	sexual coercion and extortion
SEPA	Single Euro Payments Area
SGIM	self-generated indecent material
SGSEM	self-generated sexually explicit material
SIENA	Secure Information Exchange Network Application
SOCTA	Serious and Organised Crime Threat Assessment
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TAN	Transaction Authentication Number
THB	trafficking in human beings
Tor	The Onion Router
UCC	United Cyber Caliphate
URL	uniform resource locator
VIDTF	Victim Identification Task Force
VoIP	Voice-over-Internet Protocol
VPN	virtual private network

EXECUTIVE SUMMARY

The 2017 Internet Organised Crime Threat Assessment (IOCTA) reports how cybercrime continues to grow and evolve. While many aspects of cybercrime are firmly established, other areas of cybercrime have witnessed a striking upsurge in activity, including attacks on an unprecedented scale, as cybercrime continues to take new forms and new directions. A handful of cyber-attacks have caused widespread public concern but only represented a small sample of the wide array of cyber threats now faced.

Because of the similar tools and techniques used, it is sometimes difficult to attribute cyber-attacks to particular groups, for example, financially motivated cybercriminals and Advanced Persistent Threat (APT) groups. Some of the reported cyber-attacks from mid-2017 illustrate this trend. For genuine financially motivated attacks, extortion remains a common tactic, with ransomware and Distributed Denial of Service (DDoS) attacks remaining priorities for EU law enforcement.

Ransomware attacks have eclipsed most other global cybercrime threats, with the first half of 2017 witnessing ransomware attacks on a scale previously unseen following the emergence of self-propagating 'ransomworms', as observed in the WannaCry and Petya/NotPetya cases. Moreover, while information-stealing malware such as banking Trojans remain a key threat, they often have a limited target profile. Ransomware has widened the range of potential malware victims, impacting victims indiscriminately across multiple industries in both the private and public sectors, and highlighting how connectivity and poor digital hygiene and security practices can allow such a threat to quickly spread and expand the attack vector.

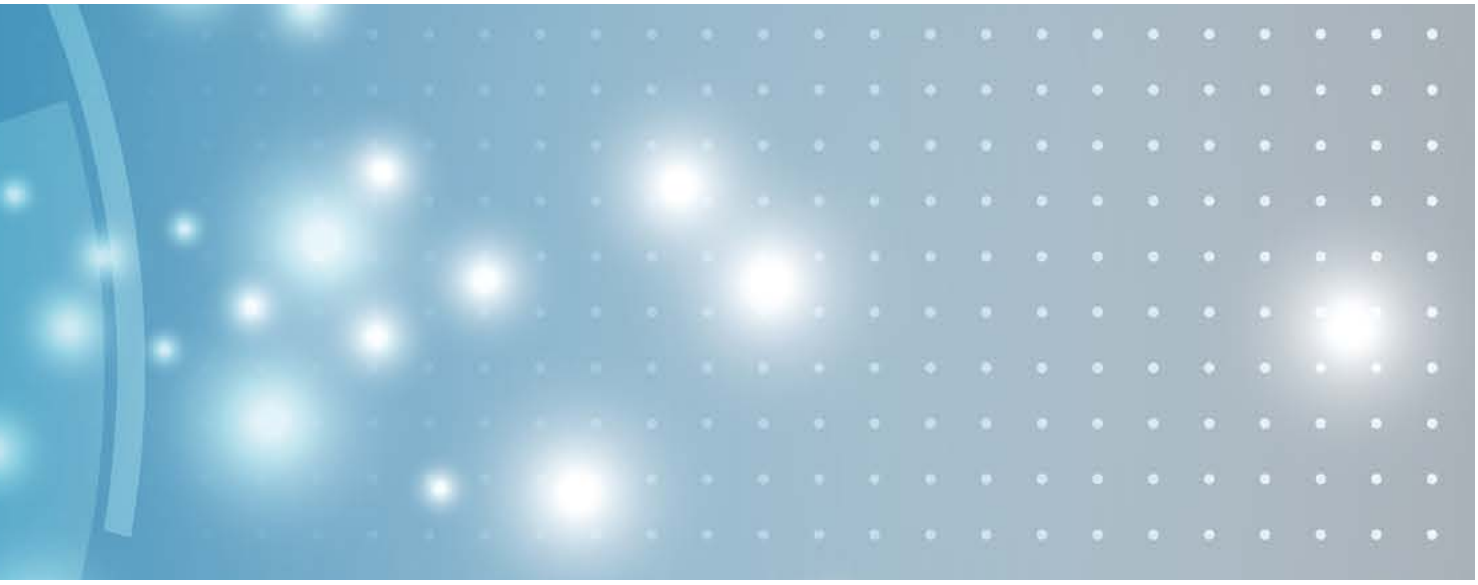
The extent of this threat becomes more apparent when considering attacks on critical infrastructure. Previous reports have focused on worst-case scenarios, such as attacks on systems in power plants and heavy industry. However, it is clear that a greater variety of critical infrastructures are more vulnerable to 'every-day' cyber-attacks, highlighting the need for a coordinated EU law enforcement and cross-sector response to major cyber-attacks on critical infrastructure.

Law enforcement and industry action has led to a decline in the use of exploit kits. This has resulted in a shift towards alternative malware delivery methods, including spam botnets and social engineering. Along with technical attacks, social engineering techniques have become an essential tactic for the commission of many, often complex, cyber-dependent and cyber-facilitated crimes, including payment fraud and online child sexual exploitation.

The success of such attacks is demonstrated by the trend of large-scale data breaches. In a 12-month period, breaches relating to the disclosure of over 2 billion records were reported, all impacting EU citizens to some degree.

Previous reports have highlighted the potential for the abuse of insecure Internet of Things (IoT) devices. By the end of 2016 we had witnessed the first massive attack originating from such devices, as the Mirai malware transformed around 150 000 routers and CCTV cameras into a DDoS botnet. This botnet was responsible for a number of high profile attacks, including one severely disrupting internet infrastructure on the west coast of the United States (US).

The vast majority of child sexual exploitation material (CSEM) is still produced by hands-on offenders. Adding to this, however, is an increasing volume of self-generated explicit material (SGEM), which is either produced innocently, or as a result of the sexual coercion and extortion of minors. Offenders are increasingly using the Darknet to store and share material, and to form closed communities.



Card-not-present (CNP) fraud continues to dominate fraud related to non-cash payments, impacting heavily on the retail sector. Airline ticket fraud continues to have significant impact across the EU and facilitates a wide range of other crime types, from drug trafficking to illegal immigration. Card-present (CP) fraud accounts for a much smaller portion of non-cash payment fraud, yet the number of reported cases has reached record numbers. The US and Southeast Asia are still key locations for cashing-out compromised EU cards. The number of criminal groups specialising in direct, complex attacks on ATMs and banks is also increasing, resulting in dramatic losses for the victims.

A growing amount of illicit trade now has an online component, meaning that cybercrime investigative capabilities are increasingly in demand in all serious organised crime investigations. Darknet markets remain a key crosscutting enabler for other crime areas, providing access to, amongst other things, compromised financial data to commit various types of payment fraud, firearms, counterfeit documents to facilitate fraud, trafficking in human beings, and illegal immigration. Compared to more established Darknet market commodities, such as drugs, the availability of cybercrime tools and services on the Darknet appears to be growing more rapidly.

Cryptocurrencies continue to be exploited by cybercriminals, with Bitcoin being the currency of choice in criminal markets, and as payment for cyber-related extortion attempts, such as from ransomware or a DDoS attack. However, other cryptocurrencies such as Monero, Ethereum and Zcash are gaining popularity within the digital underground.

Law enforcement is witnessing a transition into the use of secure apps and other services by criminals across all crime areas. The majority of the apps used are the everyday brand names popular with the general population.

A combination of legislative and technical factors, which deny law enforcement access to timely and accurate electronic communications data and digital forensic opportunities, such as lack of data retention, the implementation of Carrier-Grade Network Address Translation (CGN), and criminal abuse of encryption, are leading to a loss of both investigative leads and the ability to effectively attribute and prosecute online criminal activity. Such issues require a coordinated and harmonised effort by law enforcement, policy makers, legislators, academia, civil society and training providers to effectively tackle them.

Despite the constant growth and evolution of cybercrime, joint cross-border law enforcement actions in cooperation with the private sector and other relevant EU and international partners against the key cyber threats have resulted in some significant successes, supported by effective prevention and disruption activities.

It is clear that continued, close cooperation with the private sector is essential to combat cybercrime in an agile, pro-active and coordinated manner with a comprehensive and up-to-date information posture at its heart. This report also highlights how adequate training of the public and employees to recognise and react appropriately to social engineering would have a significant impact on a wide range of cyber-attacks.

KEY FINDINGS

CYBER-DEPENDENT CRIME

- Ransomware continues be one of the most prominent malware threats in terms of the variety and range of its victims and the damage done.
- A decline in the exploit kit market has pushed malware developers to rely more on other infection methods, including spam botnets and social engineering.
- While sophisticated cyber-attacks against European critical infrastructures are a real threat, attacks using commonly available cybercrime tools such as booters/stressers appear to be much more likely, and easier to achieve.
- Following the success of the Mirai malware and its subsequent availability, we will see an increasing number of large-scale DDoS attacks originating from a variety of insecure Internet of Things (IoT) devices.
- Inadequate IT security for internet-facing entities will continue to result in sensitive data being unlawfully accessed, exfiltrated and disclosed every year, with major breaches expected frequently.

PAYMENT FRAUD

- Due to the slow rollout of EMV in the US, the US remains one of the key destinations for cashing out counterfeit EU payment cards, along with Southeast Asia.
- Several sectors, such as the airline and accommodation industries, are targeted by CNP fraudsters as the services they provide can be used for the facilitation of other crimes, including trafficking in human beings (THB) or drugs, and illegal immigration.
- The lack of EU-wide criminalisation of the possession of stolen/compromised sensitive online payment credentials causes significant investigative challenges in this area.
- Direct attacks on bank networks to manipulate card balances, take control of ATMs or directly transfer funds, known as payment process compromise, represents one of the serious emerging threats in this area.

CHILD SEXUAL EXPLOITATION ONLINE

- Coercion and sexual extortion are increasingly being used to victimise children. Offenders use these methods to obtain further child abuse material, for financial gain or to get physical access to the victim.
- While peer-to-peer (P2P) networks continue to remain a key platform for the sharing and distribution of CSEM, everyday communication and social media applications are increasingly being used for the same purpose.
- Online offender communities operating from within the Darknet remain a primary concern, providing an environment for offenders to legitimise their behaviour, and to share both access to CSEM and operations security (OPSEC) knowledge. The largest and most prolific offenders and communities identified by law enforcement had a significant presence on the Darknet.

ONLINE CRIMINAL MARKETS

- Darknet markets are a key cross-cutting enabler for other crime areas, providing access to, amongst other things, compromised payment data to commit various types of payment fraud, and fraudulent documents to facilitate fraud, trafficking in human beings and illegal immigration.
- While an unprecedented number of users make use of Tor and similar anonymising networks, the Darknet is not yet the mainstream platform for the distribution of illicit goods, but is rapidly growing its own specific customer base in the areas of illicit drugs, weapons and child sexual exploitation material (CSEM).

THE CONVERGENCE OF CYBER AND TERRORISM

- While terrorists continue to use mainly internet and online communication apps for communication, coordination, propaganda and knowledge-sharing purposes, their capabilities to launch cyber-attacks appear to remain limited.
- Most terrorist activity concerns the open internet; however there is a share of terrorist exchange in the Darknet too. This concerns mostly fundraising campaigns, the use of illicit markets and advertisement of propaganda hosted on mainstream social media.

CROSS-CUTTING CRIME FACTORS

- Social engineering techniques are an essential tactic for the commission of many, often complex, cyber-dependent and cyber-facilitated crimes, but one which can be countered with adequate training.
- While Bitcoin remains a key facilitator for cybercrime, other cryptocurrencies such as Monero, Ethereum and Zcash are also gaining popularity within the digital underground.
- The ease with which new bank accounts can be opened in some countries, particularly online accounts, is facilitating the laundering of illicit funds by money mules.
- Criminal forums and online communication platforms still remain a key environment for cybercriminals, providing meeting places and marketplaces, and allowing access to the skills and expertise of other members of the cybercrime community.
- Law enforcement is witnessing a transition into the use of secure apps and other services by criminals across all crime areas. The majority of the apps used are the everyday brand names popular with the general populace.
- A combination of legislative and technical factors which deny law enforcement access to timely and accurate electronic communications data and digital forensic opportunities, such as lack of data retention, the implementation of CGN, and encryption, are leading to a loss of both investigative leads and the ability to effectively attribute and prosecute online criminal activity.

RECOMMENDATIONS

CYBER-DEPENDENT CRIME

Law enforcement must continue to focus on the actors developing and providing the cybercrime attack tools and services responsible for the key threats identified in this report: developers of ransomware, banking Trojans and other malware, and suppliers of DDoS attack tools, counter-anti-virus services and botnets.

Law enforcement and the private sector must continue to work together on threat analysis and prevention initiatives such as the No More Ransom project[1], to raise awareness and provide advice and free decryption tools to victims of ransomware.

It is clear that many sectors of critical infrastructure are vulnerable to everyday, highly disruptive cyber-attacks. These sectors must be better educated, prepared and equipped to deal with these attacks, leveraging EU and national efforts and resources, in particular the NIS directive and the General Data Protection Regulation (GDPR).

The international law enforcement community must continue to build trusted relationships with CSIRT/CERT communities, and public and private partners, including the improved exchange of relevant information, so that it is adequately prepared to provide a fast and coordinated response in the case of a global cyber-attack affecting critical infrastructures.

Law enforcement should continue to share malware samples with Europol to allow for analysis and cross-matching, and the subsequent linking of cases, using the existing secure information exchange channels like SIENA and the Europol Malware Analysis Solution (EMAS).

In light of the recent turmoil in the exploit kit ecosystem, malware developers are increasingly relying on social engineering, spam botnets, and other infection methods. Hence, law enforcement response strategies and prevention and awareness campaigns must adapt to these changes. Educating employees and the public to recognise and respond accordingly to social engineering attempts would prevent many cyber-dependent attacks.

Educators, parents and law enforcement should actively engage in and promote initiatives in cooperation with other relevant partners such as industry, which channel young people interested in coding into positive activities, and to deter them from potentially following a path into cybercrime.

CHILD SEXUAL EXPLOITATION ONLINE

EU Member States should ensure that any investigative tool or measure used for combating serious and/or organised crime is also made available and used to full effect in investigating online child sexual exploitation (CSE)[2]. It should also be con-

sidered that prosecutions under organised crime statutes should be pursued for dealing with the key individuals creating, supporting and driving communities related to CSE crimes.

Further research within European law enforcement and beyond is required to identify the involvement of organised crime groups (OCGs) in financially motivated sexual extortion of children, and form a coordinated response to this threat.

Crime recording and analysis systems in the Member States should be upgraded to better reflect and capture the different types of online sexual crime being reported by or associated with child victims. This is particularly true for online sexual coercion and extortion but applies to other types of CSEM-related crime also.

Europol should enable and coordinate the targeting, by Member States and partners, of key individuals creating, supporting and driving communities focused on child sexual abuse and exploitation and promoting operational security to their members.

The strategic and political commitments made by Member States through frameworks such as EMPACT and the WeProtect Global Alliance should be matched by the allocation of sufficient resources in the Member States.

Member States should strongly consider cooperating through Europol with agencies and bodies including the European Financial Coalition and other regional Financial Coalitions to tackle the abuse of legitimate payment systems enabling child sexual abuse and exploitation.

Law enforcement agencies (LEAs) in the Member States should continue exploring through Europol how online resources, including electronic service providers, can help in diverting offenders from offending behaviour, to resources that will help them cope with their sexual attraction to children.

Education is the best defence that can be provided to minors. It is therefore essential that the momentum for joint, high-quality and multi-lingual EU-wide prevention and awareness activity is maintained so that strong and effective messages can reach those that need them. Integration in education, and the education of parents is also essential. In addition every opportunity must be made available to enable victims to report abuse.

PAYMENT FRAUD

Law enforcement and the private sector should continue developing initiatives based on mutual cooperation and information sharing to combat payment fraud, including card-not-present fraud, building upon successful models like the Global Airline Action Days and e-Commerce Action weeks.

Law enforcement should keep up to date with emerging payment methods and engage with providers at an early stage to ensure that the channels are there in the event that criminals target their payment system for abuse. Robust Know-Your-Customer (KYC) and due diligence practices in the banking sector and in relation to alternative payment systems are essential for the prevention and mitigation of the monetisation of cybercrime as well as money laundering.

Further research is required to ascertain the extent to which payment card fraud is used to directly or indirectly fund or facilitate other areas of organised crime such as THB, illegal immigration or drug trafficking.

Payment fraud is characterised by a high volume of low value crime incidents, the full scope of which cannot be envisioned by local reporting and the investigation of individual single illegal transactions. A more coordinated and intelligence-led approach to combatting payment fraud is required throughout the EU.

Law enforcement should continue to build enhanced cooperation with LEAs in regions outside the EU where the cash-out of compromised EU cards occurs.

ONLINE CRIMINAL MARKETS

Law enforcement needs to develop a globally coordinated strategic overview of the threat presented by the Darknet, and monitor and understand emerging threats and relevant developments. Such analysis would allow for future coordination of global action to destabilise and close down criminal marketplaces.

While the expertise for investigating crime on the Darknet often resides within cybercrime units, only a limited proportion of the criminality thereon relates to cyber-dependent crime. It is therefore essential that investigators responsible for all crime areas represented on Darknet markets have the knowledge, expertise and tools required to effectively investigate and act in this environment.

Law enforcement must continue to cooperate and collaborate, and share tools, expertise and intelligence, in order to coordinate the global law enforcement response against the trade of illegal commodities through the Darknet.

THE CONVERGENCE OF CYBER AND TERRORISM

A robust answer to the jihadist cyber and online threats requires coordination of effort among the multitude of stakeholders in the law enforcement and intelligence communities, as well as the private sector and academia, ensuring attribution of jihadist acts in cyberspace.

Law enforcement must continue to engage with and support online service providers such as social media companies in initiatives to devise common strategies to fight their abuse by terrorist groups.

CROSS-CUTTING CRIME FACTORS

Innovation, in terms of the pro-active and adaptive approaches and counter strategies employed, and collaboration, in terms of the involvement of all relevant partners, should be at the core of any response to tackling cybercrime.

There is a need to continue to develop coordinated action at EU level and beyond to respond to cybercrime at scale, building on and learning from successful operations.

Law enforcement must continue to develop, share and propagate knowledge on how to recognise, track, trace, seize and store cryptocurrencies. Existing training on investigating cryptocurrencies should be shared and promoted within the law enforcement community.

Law enforcement should engage early with the private sector, academia and developers to seek solutions to investigating those emerging cryptocurrencies which boast additional security measures designed to hamper lawful investigation.

Private sector partners and law enforcement should continue cooperating to target mule networks which are an essential element of the criminal ecosystem, following successful models such as the European Money Mule Actions (EMMA).

Where not already present, Member States should consider implementing more efficient fraud reporting mechanisms. Online reporting channels are particularly suitable for such high volume crimes, and allow victims to report the crime without the need to contact local police.

While the implementation of the European Investigation Order (EIO) is expected to simplify cooperation between judicial authorities and expediting investigations, existing legal frameworks and operational processes need to be further harmonised and streamlined for dealing with cross-border e-evidence. Such measures, as well as the parallel EU policy processes on encryption, data retention and internet governance challenges, should thoroughly consider the specific law enforcement needs and strive for practical and proportionate solutions to empower innovative, efficient and effective approaches to conducting lawful cybercrime investigations. The growing prevalence and sophistication of cybercrime requires dedicated legislation that more specifically enables law enforcement presence and action in an online environment.

Member States should continue to support and expand their engagement with Europol in the development of pan-European awareness and prevention campaigns with a view to increasing baseline cybersecurity protection and further improving digital hygiene. This includes security-by-design and privacy-by-design principles such as the use of encryption to safeguard sensitive data.

As human beings are the direct targets of social engineering which is often the starting point of a cyber-attack, the investment in combating it must also be in the employees and members of the public that are likely to be potential victims. Training and education are crucial to allow prospective victims to identify and respond accordingly to social engineering attacks.

INTRODUCTION

AIM

The Internet Organised Crime Threat Assessment (IOCTA) is produced by the European Cybercrime Centre (EC3) at Europol. It 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 2017 IOCTA will contribute to the setting of priorities for the 2018 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 2017 IOCTA focuses the trends and developments pertinent to the above-mentioned priority crime areas. In addition to this, the report will discuss other cross-cutting factors which 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 2017 IOCTA was drafted by a team of Europol strategic analysts drawing predominantly on contributions from Member States, the European Union Cybercrime Taskforce (EUCTF), Europol's Analysis Projects Cyborg, Terminal and Twins, as well as the Cyber Intelligence team and SOCTA team, via structured surveys, interviews and moderated workshops. This has been enhanced with open source research and input from the private sector, including EC3's Advisory Groups, Eurojust, ENISA, CERT-EU, the EBF and the CSIRT community. These contributions have been essential to the production of the report.

ACKNOWLEDGEMENTS

Europol would like to extend thanks to all partners who contributed to this report, and extend a special thanks to Prof. Marco Gercke, Prof. Michael Levi and Prof. Alan Woodward of the IOCTA Advisory Board for their contributions and insight.

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 these crimes could not be committed[3]. It includes such activity as the creation and spread of malware, hacking to steal sensitive personal or industry data and denial of service attacks to cause financial and/or reputational damage.

KEY FINDINGS

- Ransomware continues be one of the most prominent malware threats in terms of the variety and range of its victims and the damage done.
- A decline in the exploit kit market has pushed malware developers to rely on other infection methods, including spam botnets and social engineering.
- While sophisticated cyber-attacks against European critical infrastructures are a real threat, attacks using commonly available cybercrime tools appear to be much more likely, and easier to achieve.
- Following the success of the Mirai malware and its subsequent availability, we will see an increasing number of large-scale DDoS attacks originating from a variety of insecure IoT devices.
- Inadequate IT security for internet-facing entities will continue to result in sensitive data being unlawfully accessed, exfiltrated and disclosed every year, with major breaches expected frequently.

KEY THREAT – MALWARE

The primary targets for the majority of cyber-dependent crimes are vulnerable software products, insecure, internet-connected devices or networks, and the users and data behind them. As such, the development and propagation of malware typically sits at the core of cyber-dependent crime. Malware can be coded or repurposed to perform almost any function; however, the two dominant malware threats encountered by EU law enforcement continue to be ransomware and information stealers.

INFORMATION STEALERS

The information stealing malware landscape remains dominated by established malware 'brands' and enhanced/rebooted versions of older malware variants. For the second year running, despite a brief hiatus, *Dridex* appears to be one of the leading Trojans. It continues to target financial institutions, with the UK accounting for the majority of infections[4]. Part of *Dridex's* success is due to its distribution method – massive spam campaigns which run from Monday to Friday at a high rate[5].

Similarly, after a period of inactivity following law enforcement action in 2015[6], the *Ramnit* banking Trojan resurfaced in 2016 in a campaign which also focused on major UK banks.[7,8,9] Other banking Trojans which we have discussed in previous reports, such as *Tinba* and *GameOverZeus*, are still active[10] but did not feature significantly in law enforcement reporting this year.

While information stealing malware clearly remains a persistent and significant threat, it does not feature heavily in this year's law enforcement reporting, highlighting how it has been overshadowed by other threats.

There will always be profit to be made from information stealing malware such as banking Trojans. However, such attacks are not only more limited in their scope, but require significantly more effort on the part of the attacker. They often require custom-made web injects to tailor attacks to specific banks or other target websites. Attackers must then not only harvest the data but monetise it, either by selling it or, if it is financial data, cashing out compromised accounts or payment cards, which may require employing third parties (such as money mules) to help launder the proceeds.

RANSOMWARE

Comparatively, ransomware is easier to monetise. Beyond the initial infection, all the attacker has to do is collect the ransom payment, and by using pseudonymous currencies such as Bitcoin, the subsequent laundering and monetisation is considerably simpler. Furthermore, the nature of the attack means that ransomware can inherently target a much more diverse range of targets – essentially anyone with data to protect – with little requirement for adaption. Victims are atypical from the usual financial targets, and include entities such as hospitals, law enforcement agencies, and government departments and services. While the public also continues to be targeted, small to medium enterprises, who often lack the resources to fully safeguard their data and networks, are also key targets.

The success and the demand for ransomware resulted in an explosion in the number of ransomware families throughout 2016, with some reports highlighting an increase of 750% from 2015[11]. The business model for ransomware has also evolved. Developers of early iterations of ransomware produced it for their own use, but now variants such as *Satan*[12] or *Shark*[13] are run as affiliate programs, providing ransomware-as-a-service in exchange for a share of the criminal proceeds.

The surge in ransomware is also reflected in this year's reporting, with almost every Member State reporting a growing number of cases. Throughout 2016, the emerging threats highlighted in the previous year's report, *Locky* and *Cerber*, were the most prominent ransomwares. A number of other ransomwares, including CTB-Locker, *Cryptowall*, *Crysis, Teslacrypt, Torrentlocker*[14] and *Zepto* were also reported, but these appear to be localised to specific countries.

On 12 May 2017 however, all other ransomware activity was eclipsed by a global ransomware attack of unprecedented scale. While reports vary, the *WannaCry* ransomware is believed to have rapidly infected up to 300 000 victims in over 150 countries, including a number of high-profile targets such as the UK's National Health Service, Spanish telecommunication company *Telefónica*, and logistics company *Fed-Ex*.

There were a number of key factors in the success of the *WannaCry* attack. Firstly, unlike most ransomware, *WannaCry* used the self-propagating functionality of a worm to spread infections. Secondly, and of greater concern, the worm made use of a Windows SMB (Server Message Block) exploit dubbed 'EternalBlue' to infect machines. EternalBlue is one of the exploits allegedly leaked by the NSA and acquired by the *ShadowBrokers* group. The *ShadowBrokers* publicly leaked the code for the exploit in April 2017, one month after Microsoft released a patch for it. One month later the *WannaCry* attack occurred.

While the scope and scale of the *WannaCry* attack was considerable, and the anxiety generated was socially significant, if *WannaCry* truly was as an attempt at extortion, it was a negligible financial success, with less than 1 percent of the victims paying the ransom.

In the month following the *WannaCry* outbreak, another global ransomware attack was launched, utilising some of the same exploits used by *WannaCry.* The updated version of the *Petya* ransomware, dubbed *ExPetr* or *NotPetya*, reportedly hit more than 20 000 victim machines in more than 60 countries. Victims were mainly in Europe, but also in Asia, North and South America and Australia; however, more than 70% of the total infections were in the Ukraine.[15] Moreover, reports indicated that more than 50% of the businesses targeted were industrial companies. Some opinions suggest that the attack was staged to appear as another ransomware attack but it appears to have been designed as a 'wiper', whose sole purpose is to destroy data.

In July 2016, the Dutch National Police, Europol, Intel Security and Kaspersky Lab joined forces to launch the No More Ransom project which aims to provide advice and free decryption tools for victims of ransomware. The initiative has now expanded to include more than 100 partners in law enforcement and private industry, is available in 26 languages, has 54 decryption tools and has helped over 29 000 victims decrypt their files for free, depriving criminals of an estimated EUR 8 million in ransoms. [16,17]

MOBILE MALWARE

Only a few countries reported cases involving mobile malware in 2016, although those that did reported that the threat was increasing. While law enforcement may continue to promote awareness campaigns on mobile malware,[18] this is likely to continue to be an area that remains under-reported. However, with the growth in mobile ransomware this may change.

Even so, industry continues to report a significant year-on-year increase in mobile malware, although Europe as a whole appears to suffer lower infection rates, with infections concentrated in Asia.[19] The vast majority of mobile malware also remains restricted to devices running the Android OS.

The dominant mobile malware type is overlay malware, of which *GM bot* is the original and most successful. The malware displays fake overlays on the mobile device when a user tries to use an application. The overlay can capture victims' banking credentials and confidential data. The malware can also intercept SMS messages and can therefore circumvent two-factor authentication, steal mobile transaction authentication number (mTAN) tokens, and initiate remote money transactions. One of the latest examples of overlay malware, *Faketoken*, is capable of running overlay attacks on over 2000 financial applications, and can also encrypt files and perform ransomware attacks.[20]

OTHER MALWARE THREATS – EXPLOIT KITS

2016 saw a number of significant developments with regards to the operation and use of exploit kits as a malware delivery mechanism. In April 2016, the *Nuclear* exploit kit, which was previously considered as one of the most active kits, ceased activity.[21] The arrest of suspects linked to the *Lurk* malware by Russian law enforcement in June 2016 coincided with the demise of the *Angler* exploit kit, which had established itself as the market leader since 2015 and the most sophisticated kit following the demise of the *Blackhole* exploit kit. In the resulting instability in the exploit kit ecosystem, *Neutrino* exploit kit temporarily became the predominant kit. However, it allegedly shut down operations in September 2016 following industry action by Cisco and GoDaddy,[22] and is subsequently believed to have transitioned into private mode around October 2016.

Following this, the remaining exploit kits such as *RIG*, *Sundown*, and *Magnitude*, along with a number of other kits such as *Terror* and *Stegano*, failed to reach the level of sophistication of Angler and have been unable to sustain a stable market lead position. In addition to the recycling of old vulnerabilities, some of them appear to have either downsized their operations or gone private, limiting the use and distribution to smaller campaigns. Another notable development took place in May 2017, when *RIG's* operations were further mitigated following industry-led action by RSA Research and GoDaddy.[23]

Although these developments have made exploit kits less likely to attract the attention of either law enforcement or industry action as top priority,[24] these tools still pose a threat and should be monitored, as the ecosystem had previously demonstrated its ability to adapt.

OTHER MALWARE THREATS – REMOTE ACCESS TROJANS (RATs)

In the 2016 IOCTA we reported a general decline in law enforcement investigations into Remote Access Trojans (RATs). In this year's report however, almost one third of Member States reported cases involving RATs. While the RATs reported include some 'branded' variants, there are reports of increasing numbers of custom-made RATs which are harder to identify.

In April 2017, a joint investigation by Spanish and British law enforcement authorities, coordinated by Europol and its Joint Cybercrime Action Taskforce (J-CAT), resulted in the dismantling of an international cybercrime group involved in the design, development and selling of sophisticated software tools. The tools were used worldwide for the distribution of Remote Access Trojans and key loggers.[25]

OTHER MALWARE THREATS – COUNTER ANTIVIRUS (CAV) SERVICES

CAV services are a key enabler for the deployment of malware. CAV services allow developers to upload a malware sample to test it against a wide range of commercial antivirus tools and software to determine whether it is identified as malicious. Such services are often coupled with encryption services which can run a series of encrypt routines to help obfuscate the malware. Several Member States report cases involving CAV services.

In June 2017, EC3 and the J-CAT, together with the law enforcement authorities from Cyprus, Italy, the Netherlands, Norway and the United Kingdom, executed a coordinated action against the international top customers of a particular CAV service, which led to 6 arrests and 36 suspects being interviewed, along with 20 house searches and multiple data carriers and other equipment being seized.[26] *The operation was led by Germany, and was a follow-up to the 2016 large-scale operational action against the administrator of the service and the German users.*

INDUSTRY vs LAW ENFORCEMENT PERSPECTIVE

As highlighted in the 2016 IOCTA, when assessing malware threats, law enforcement sees quite a different picture compared to the internet security industry. A simple explanation for this is that 'payload' malware such as ransomware or a banking Trojan, which has a direct and visible impact on the victim, is more likely to be reported to the police and result in an investigation; malware operating 'invisibly' in the background, such as a dropper or exploit kit, is not likely to be so. The internet security industry however, has much greater visibility into such threats. What is more, if they are able to detect and mitigate them, they may not even see the payload.

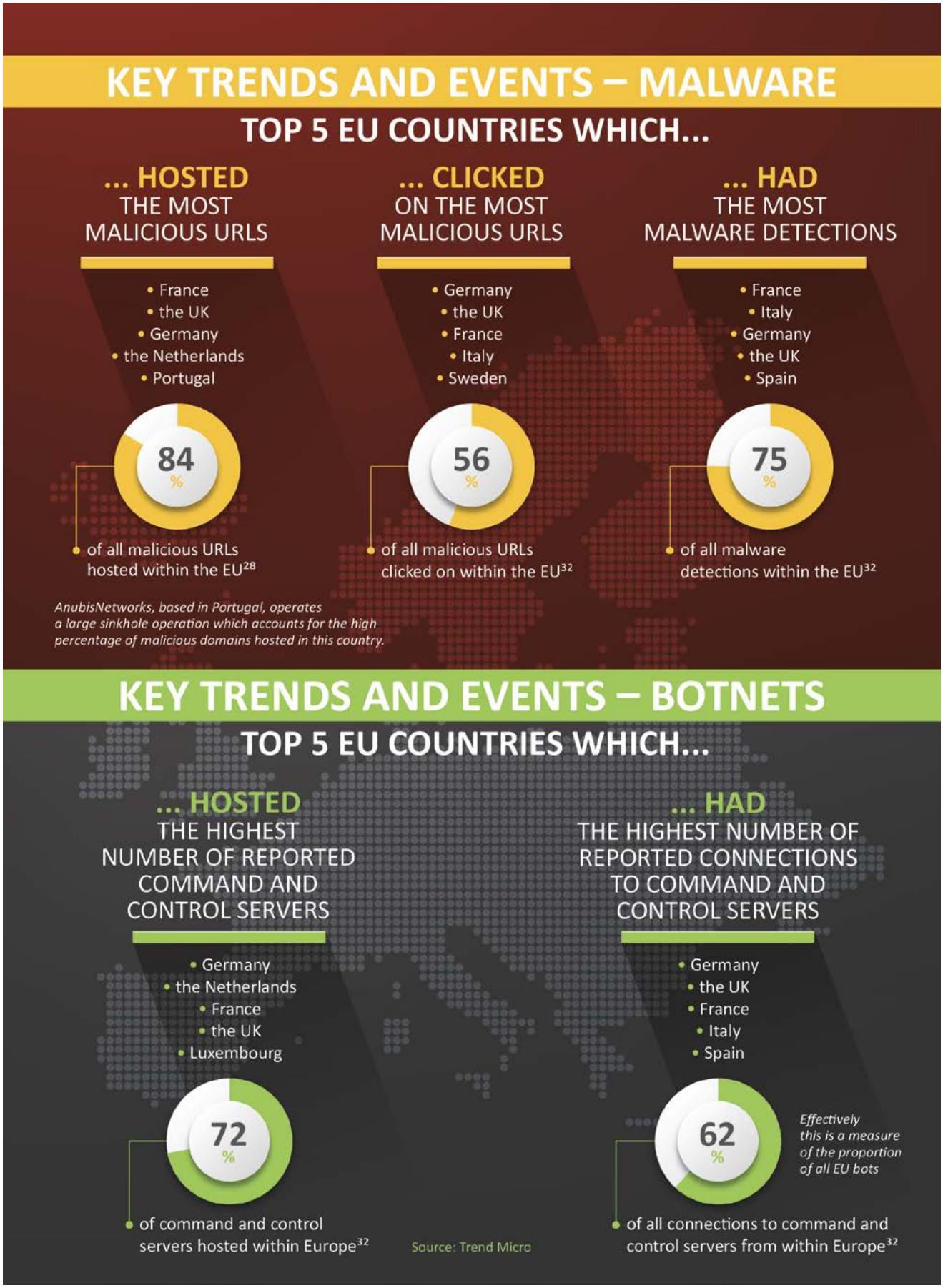
The following table identifies the top 5 (with #1 being the worst) malware threats for each EU Member State as determined by the number of attempts to access the internet from infected systems. This data reflects the total activity over 2016, and typically refers to networks belonging to *enterprise, government or academia,* but not *private citizens*.[27]

EU MALWARE MATRIX

Malware	AT	BE	BG	CY	CZ	DE	DK	EE	ES	FI	FR	GR	HR	HU
Adwind			2											
Angler EK											3			
Bedep											4			
Bladabindi														
Brontok														
Cerber			5											
Conficker		1	3	1	1	2		3	1		1	3	1	1
Cryptoload														
Cryptowall	4			3	2	3	3	2		5	2			2
Cutwail				2										
Delf														4
Dnschanger							1					1		
Dorkbot														
HackerDefender	3	2			5		5	5				4		
Hancitor														
Hummingbad														
JBossjmx								1						
Kazy														
Kometaur								4						
Ldpinch	2													
Locky	5	5			4					3	5	5	5	3
Matsnu						5								
NetSky														
Nivdort									4					
Ponmocup		3	1	4			4						4	
RookieUA														
Sdld						1								
Shmandaler														
Tinba									3	4			3	
Upatre									2					
Ursnif			4											
Vupdavecon														
Wysotot									5					
Zeroaccess							2			1		2		
Zeus	1	4		5	3	4				2			2	5

Source: Check Point Software Technologies

Malware	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Adwind														
Angler EK				5										
Bedep				4										
Bladabindi					3									
Brontok									3					
Cerber	4			3							3			
Conficker			1	1	2		1	3	1	1	2	2	1	1
Cryptoload											1			
Cryptowall	5					2		5	4			4	2	2
Cutwail														
Delf														
Dnschanger							4							
Dorkbot			5											
HackerDefender		3						4				3	5	5
Hancitor					5	5								
Hummingbad			2											
JBossjmx		2						1				1		
Kazy											5			
Kometaur														
Ldpinch						3								
Locky		5	4		1		2						3	3
Matsnu														
NetSky														
Nivdort														
Ponmocup		1		2						5			4	4
RookieUA	1						5							
Sdld														
Shmandaler		4												
Tinba						4				4	4			
Upatre														
Ursnif							3							
Vupdavecon	3													
Wysotot									2					
Zeroaccess										2		5		
Zeus	2		3		4	1		2	5	3				


KEY TRENDS AND EVENTS – MALWARE
TOP 5 EU COUNTRIES WHICH...
... HOSTED THE MOST MALICIOUS URLS
• France
• the UK
• Germany
• the Netherlands
• Portugal
84 %
of all malicious URLs hosted within the EU[28]
... CLICKED ON THE MOST MALICIOUS URLS
• Germany
• the UK
• France
• Italy
• Sweden
56 %
of all malicious URLs clicked on within the EU[32]
... HAD THE MOST MALWARE DETECTIONS
• France
• Italy
• Germany
• the UK
• Spain
75 %
of all malware detections within the EU[32]
AnubisNetworks, based in Portugal, operates a large sinkhole operation which accounts for the high percentage of malicious domains hosted in this country.
KEY TRENDS AND EVENTS – BOTNETS
TOP 5 EU COUNTRIES WHICH...
... HOSTED THE HIGHEST NUMBER OF REPORTED COMMAND AND CONTROL SERVERS
• Germany
• the Netherlands
• France
• the UK
• Luxembourg
72 %
of command and control servers hosted within Europe[32]
Source: Trend Micro
... HAD THE HIGHEST NUMBER OF REPORTED CONNECTIONS TO COMMAND AND CONTROL SERVERS
• Germany
• the UK
• France
• Italy
• Spain
62 %
Effectively this is a measure of the proportion of all EU bots
of all connections to command and control servers from within Europe[32]

KEY THREAT – ATTACKS ON CRITICAL INFRASTRUCTURE

Critical infrastructure is defined as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'. [29]

When discussing (cyber-physical) attacks on critical infrastructure, there is often a focus on the worst case scenario – sophisticated state-sponsored or condoned attacks on vulnerabilities in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems in the likes of power plants and heavy industry. While these threats are undoubtedly real, such attacks are rarely, if ever, reported to law enforcement, instead more likely falling into the territory of national security. There are however far more common and more likely attack vectors and targets which do not require attackers to penetrate such isolated networks, using for instance booters/stressers to launch a DDoS attack.

In last year's report we highlighted everyday malware and zero-day exploits as a key threat. The *WannaCry* attack of May 2017 is a prime example of this, crippling hospitals in the UK, and disrupting rail networks in Germany and the Russian Federation, telecommunications companies in Spain and Portugal, petrochemical companies in China and Brazil, and automotive supply chain industries in Japan. Whether WannaCry can be properly classified as 'everyday' malware is a different question.

In previous reports we have highlighted a growing number of ransomware attacks against hospitals, law enforcement agencies and transportation companies, causing severe disruptions.

The most commonly reported (to law enforcement) attacks against critical infrastructures in the EU were DDoS attacks, with over 20% of countries reporting cases. In September 2016, the website of security researcher Brian Krebs was knocked offline by 'an extremely large and unusual' DDoS attack, which originated from a botnet consisting of an estimated 150 000 IoT devices (such as routers and security cameras) infected with the *Mirai* malware. In October 2016, the Mirai botnet was used to launch an attack on Dyn's Managed DNS infrastructure, severely affecting internet access for the US's west coast for approximately 2 hours. A different variant of the same malware also hit 900 000 Deutsche Telekom users in November 2016, highlighting how telecommunications is one of the most targeted sectors, along with finance. For telecommunications, according to ENISA's Annual Incidents Report, most incidents reported in 2016 involved mobile internet and mobile telephony connections,[32] while the longest lasting incidents were caused for the first time by malware.[33]

While DDoS is often a tool for extortion, the lack of communication from the attackers may suggest that these attacks were of an ideological nature. Although European law enforcement recorded an increasing number of these attacks last year, they also note that they only had moderate, short-lived impact.

Most, if not all, public-facing critical infrastructure sectors rely extensively on computer systems for many aspects of their industry. Each of these is potentially vulnerable to some form of cyber-attack. It is reported that aviation systems are subject to an average of 1000 such attacks each month.[34] Other reports highlight that the frequency with which industrial systems connect to the internet varies considerably and so, logically, does their risk of infection; on average, one-in-five industrial computers is attacked every month.[35]

The second most reported threat in this area is that of Advanced Persistent Threat (APT)-style attacks. It seems probable that there is a built-in selection bias, insofar as those that come to the notice of authorities are more likely than average to be severe. While less than 20% of Member States report cases involving APTs, those that do report that these are high impact attacks, and that they are almost universally becoming more prevalent each year, a view echoed by internet security experts. Again, the financial sector was a key target, alongside government departments/agencies. As with other network attacks, attackers seem to rely heavily on social engineering tactics such as spear-phishing to convince individuals within the target company to breach or circumvent their own IT security measures.

KEY THREAT – DATA BREACHES AND NETWORK ATTACKS

In today's society it is unlikely that there are any public or private sector entities left that do not have some overt or even unknowing connection to the internet. Coupled with the easy availability of crimeware and tools on underground forums, attacks on public and private networks have almost become daily occurrences, while every month there are high profile data breaches. There are several key aspects to these attacks.

DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS

DDoS attacks remain a constant concern for European law enforcement. The most common motivation for reported attacks was extortion, accounting for over one third of attacks. Collectively, attacks that were purely malicious, or those conducted for seemingly political/ideological reasons, accounted for almost half of reported attacks. Such attacks are naturally distressing or problematic for the victims, and while they often have a limited duration they may cause some reputational or financial damage. DDoS attacks are generally only newsworthy due to some aspect related to the size or source of the attacks, or the nature of target rather than actual damage caused. Depending on the motivation for the attack, being 'newsworthy' is likely to be one of the attacker's goals.

DDoS attacks from botnets consisting of IoT devices such as the aforementioned Mirai botnet have been predicted in previous reports for several years now but the attacks against Krebs's web site, Dyn and Deutsche Telekom are the first reported instances.

For financially motivated extortion attempts, attacks are typically directed at medium-sized or large enterprises, with payment almost exclusively demanded in Bitcoins. Such attacks often target specific victims to coincide with specific events or occasions when they are likely to be doing more business; florists during St Valentine's day or online gambling sites around large sporting events, for example.

In some countries, the legacy of DDoS groups such as the Armada Collective continues, with some attackers still posing as the now defunct criminal group. They rely on the group's reputation to scare potential victims into paying, when in reality they likely lack any significant DDoS capability.

Other DDoS groups similarly launch small attacks resulting in some service disruption, followed by threats of a more substantial attack if a ransom is not paid. Even if payment is not made however, there is often no subsequent attack, suggesting that the groups' actual DDoS capability is negligible. Such 'try-your-luck' attacks are likely to become more prevalent due to the increasing accessibility of DDoS tools (such as booters and stressers) and DDoS-for-hire services on both the open web and in the Darknet. Some reports show that a 5-minute attack on a large online retailer can cost as little as USD 5, while simultaneously costing the business considerably more.[36] This disparity between the costs of attacks and the costs of both prevention and reparation is alarming.

In December 2016, Europol and law enforcement authorities from Australia, Belgium, France, Hungary, Lithuania, the Netherlands, Norway, Portugal, Romania, Spain, Sweden, the United Kingdom and the United States carried out a coordinated action targeting users of Distributed Denial of Service (DDoS) cyber-attack tools, leading to 34 arrests and 101 suspects interviewed and cautioned.

The individuals arrested were suspected of paying for stresser and booter services to maliciously deploy software to launch DDoS attacks. The tools used were part of a criminal 'DDoS for hire' facility for which hackers can pay and aim it at targets of their choosing.

PRIVATE BRANCH EXCHANGE (PBX) FRAUD

In some countries it has been estimated that by 2025, all telecommunications will have foregone traditional ISDN lines to be replaced by IP-based exchanges and networks.[37] This shift has already begun with a growing number of businesses switching to low cost IP-based exchanges. This, however, has created new opportunities for cybercriminals who are able to exploit unpatched and vulnerable networks in order to route premium rate or special service calls through these exchanges. This activity leads to often substantial costs to the company involved, and considerable profit for the criminal groups running the premium phone lines.

PBX fraud is a growing problem, accounting for over 20% of all reported telecommunications fraud.[38] European law enforcement not only continues to report a growing number of cases but it was one of the most commonly reported specific modus operandi in relation to network intrusions.

NETWORK INTRUSIONS

There is one common purpose of the majority of network attacks reported to European law enforcement – the unlawful acquisition of data, with an equal split between the acquisition of financial data and the acquisition of other data, including personal data or intellectual property.

Some other Member States highlight network intrusions as an enabling attack vector for other cyber-dependent criminality, including the deployment of specific malware such as Remote Access Trojans or ransomware. A third MO, which will be discussed later in this report, is payment process compromise, which are intrusions into bank networks in order to either directly transfer funds or to remotely command ATMs to dispense cash.

Those attacks targeting sources of financial data will typically target sources of credit card data that can subsequently be used for card-not-present (CNP) fraud. Such data, when exfiltrated in bulk, will often find its way onto criminal automated card shops, which will also be discussed later in this report. Industry reporting suggests that 73% of breaches are financially motivated.[39]

2016 saw a number of online open source databases attacked by hackers. Users of unprotected or insufficiently protected MongoDB, ElasticSearch and Hadoop Distributed File System (HDFS) servers could be found using the Shodan search engine for internet-connected devices. The total volume of users affected by this is unclear, but as an example the insecure HDFS servers were estimated to expose over 5 Petabytes (PB) of data.[40] Attacks on these databases either maliciously deleted data, or backed up the data first and then attempted to extort the data owner into paying for its return. Many of these attacks were confused however as multiple attackers, mirroring the original MO, attempted to extort the same victims, making it unclear for the victims who actually had their data.

The table opposite highlights some of the high profile data breaches which either relate to European organisations or would have significant impact on European citizens, and which were assessed to be of Critical[41] severity or greater. The severity is based on a number of factors including the number of records disclosed, the nature of the data disclosed, the source of the breach and the nature of the breached company's business.

The table lists only the breaches occuring in the second half of 2016 and the first half of2017 when **more than 100 000** records were disclosed.

Data Breaches Affecting Europe[42]

Organisation	Industry	State	Source of Breach	Records Compromised	Data Compromised
Yahoo!	Internet		Malicious outsider	1 500 000 000	Name Email address Phone number Date of birth (DoB) Password data Security question data
Friend Finder Network Inc	Adult		Malicious insider	412 214 295	Email address Password data
National Health Service	Healthcare		Accidental loss	26 000 000	Confidential patient data
Zomato	Other		Malicious outsider	17 000 000	Email address Password data
fashionfantasygame.com	Other (social media)		Malicious outsider	2 400 000	Email address
Aerticket	Transport (Airline)		Malicious outsider	1 500 000	Name Postal address Credit card data Flight details DoB
Supercell	Other (software)		Malicious outsider	> 1 000 000	Username Password Email address IP address
Brazzers	Adult		Malicious outsider	790 724	Username Email address Password data
Capgemini	Other		Accidental loss	780 000	Name Email address Phone number Work history Password data
BankGiro Loterij, Postcode Loterij, VriendenLoterij	Other		Accidental loss	450 000	Name Address Email address Bank account DoB
Netia	Telecoms		Malicious outsider	342 000	Name Address IP address Email address Phone number User agent data
PayAsUGym	Other (Fitness)		Malicious outsider	300 000	Name Address Email address Contact details
Erasmus University	Education		Malicious outsider	270 000	Name Postal address Medical data Bank account Credit card data

Similar to last year, one of the largest breaches in 2016 was the breach of an 'adult' website. However, this year's breach of various adult sites which are part of the Friend Finder Network, which includes AdultFriendFinder (which was also breached in 2015), is 10 times the size of last year's breach. While mainly email addresses were leaked, this still creates significant potential for fraud and extortion, particularly as the list included many official email addresses.[43]

WEBSITE DEFACEMENT

While a low priority for most countries, the defacement of websites remains a common criminal complaint. Ordinarily the work of hacktivists targeting government or corporate websites, or 'script kiddies' showing off their new skills, website defacement is typically a short-lived, low impact attack aimed at making a personal or political statement.

ATTACKS ON THE ELECTORAL PROCESS

During and subsequent to the 2016 US presidential elections, there were numerous allegations that external actors were able, through cyber-attacks, to interfere or influence the democratic process. These allegations were typically levelled at Russian hacking groups.

With several EU Member States due to hold key elections during 2017 and 2018[II], there is considerable speculation that there will be external interference with the process, for instance in the form of DDoS attacks against campaigns websites or online electoral services. In some cases, there are suggestions that it has already begun.[44]

In many countries, the vote still relies on a paper ballot, not only for security purposes, but also to allay fears that electronic voting could potentially de-anonymise the voter.

FUTURE THREATS AND DEVELOPMENTS

Even before the *WannaCry* outbreak, ransomware was already set to take centre stage in terms of malware threats in this year's report. The scale and broad surface of the *WannaCry* attack was unprecedented, with few countries unaffected. One unintended positive aspect of this is something of a global awakening, raising awareness of the threat worldwide and creating an opportunity for IT security issues to be taken more seriously by businesses and organisations, including the need for improved patch and vulnerability management.

Cyber insurance is a growing industry, and within Europe cyber insurance premiums are likely rise to EUR 8.9 billion by 2020 from about EUR 3 billion today.[45] There is a danger of cyber insurance encouraging complacency, with those relying on it to cover potential losses instead of investing in preventative measures. However, there is a real potential for a positive impact where such insurance creates financial incentives for the adoption of due diligence and cybersecurity measures, for instance by offering discounts on premiums.

Another key development seen in both the *WannaCry* and *Petya/NotPetya* attacks was the inclusion of the self-propagating or 'worm' functionality within the malware, creating what some are referring to as a 'ransomworm'. While this was not the first time this has been done,[46] it is the most successful example of its implementation, and a tactic we are likely to see repeated in future threats.

Banking Trojans did not feature heavily in law enforcement reporting this year, however their development and innovation does not cease. As reported in previous years there is little in the way of completely novel malware, as developers instead focus on rebooted variants such as the *Zeus* variant *Panda*, or *Dyre* variant *Trickbot*, or hybrid malware which combines aspects of other successful variants, such as *Goznym* which borrows from both the *Gozi* banking Trojan and the *Nymaim* downloader.[47]

While not new, 'fileless' malware is another malware threat that is likely to become more prominent in the near future. Fileless infections are those that do not involve malicious files being downloaded or written to the system's disk, thereby circumventing many traditional anti-virus programs. Such infections instead reside either within the infected systems' memory, within the Windows registry or operate as a rootkit, and use Windows operating system applications, such as Powershell or Windows Management Instrumentation, to run.[48] While fileless malware did not feature in law enforcement reporting for this year's IOCTA, perhaps due to its nature, there are a growing number of known cases throughout Europe.

The disastrous year for exploit kits has seen malware developers seek alternate infection vectors. Many of the leading malware threats highlighted this year, such as *Dridex* and *Locky*, previously relied on exploit kits for their distribution, but have now resorted to alternative malware delivery mechanisms such as spam botnets and social engineeri ng. The different infection vectors and malware distribution tactics observed during the *WannaCry* and *Petya/NotPetya* attacks are also indicative of this trend. From a criminal perspective, the reliance on a third

[II] For instance, federal elections are planned in Germany in September 2017. In 2018, presidential elections are planned in the Czech Republic, Finland and Ireland and parliamentary elections are planned e.g. in Hungary and Malta.

party product such as an exploit kit for distribution represents an additional point of failure for any malware campaign.

We previously predicted the inevitability of insecure IoT devices becoming tools for conducting DDoS attacks, a prediction which came to fruition this year with the DDoS attacks of unprecedented scale originating from the *Mirai* botnet. The *Mirai* source code was publically released shortly after; as we have seen with previous source code releases, such as Zeus and *Carberp*, it is likely that it will be rapidly adopted and adapted by the cybercrime community. There are therefore two likely outcomes to this event. The first is that we will inevitably see new variants of *Mirai* appearing on criminal markets, or appearing in the wild under control of private developers, and further waves of DDoS attacks originating either from these variants or *Mirai* itself. The variety of IoT devices affected by this type of malware will also undoubtedly increase.[49] The second, on a more hopeful note, is that it may, like the *WannaCry* attack, act as a catalyst for developers of IoT devices to include better security-by-design. This will however do little to reduce the threat from the millions, if not billions, of devices already out there and vulnerable to this sort of exploitation. It will also be interesting to see what impact this will have on the DDoS-as-a-service business model using booters and stressers. In this context, Europe's IoT policy and concrete initiatives such as the Alliance for Internet of Things Innovation (AIOTI) and strategies aiming at advancing the IoT in Europe, looking specifically also at security, liability, privacy and data protection as well as labelling and certification, will play a key role in addressing these challenges.

Sophisticated attacks against European critical infrastructure are a real threat. However, attacks, both direct and indirect, against critical infrastructures using commonly available cyber-attack tools such as booters/stressers appear to be much more likely, and easier to achieve. While these attacks may not be as damaging as taking down a power-grid, they can still cause severe disruption to key utilities and services.

The Network Information Security (NIS) directive that calls for cybersecure solutions in critical sectors will require identified operators in these sectors to take appropriate and proportionate measures to manage the risks posed to the security of their networks and information systems, including the need to notify significant incidents. As such, the NIS directive is expected to have a strong and positive impact on the cybersecurity of European critical infrastructure.

Probably one of the most significant future threats which will affect all areas of cyber-dependent crime relates to the likely disclosure of further hacking tools and exploits by the *ShadowBrokers* group. In May 2017, the group announced its new monthly subscription model, 'TheShadowBrokers Data Dump of the Month', with the first data set of exploits reportedly sent out to subscribers in June.The package allegedly includes web browser, router and handset exploits and tools, exploits for Windows 10, compromised network data from SWIFT providers and Central

banks and compromised network data.[50] Previous attempts to auction off such tools were apparently unsuccessful, resulting in the group leaking the exploits instead. However, the success of *WannaCry* may improve their future chances of finding successful buyers. Should the sale prove ineffective once again, it is likely that another leak will follow. Given that it took less than one month from the leak of the *EternalBlue* exploit to its use in the WannaCry attack, it is likely that another cyber-attack of significant magnitude can be expected within a similar timeframe from the next release. While the vendors of the vulnerable products can issue patches, as with the *WannaCry* attacks, it is likely they there will be huge numbers of unpatched machines, although *WannaCry* should have convinced many of both the benefits of patching and of the necessity to log and update old software that can make their entire systems vulnerable.

RECOMMENDATIONS

Law enforcement must continue to focus on the actors developing and providing the cybercrime attack tools responsible for the key threats identified in this report: developers of ransomware, banking Trojans and other malware, and suppliers of DDoS attack tools, counter-anti-virus services and botnets.

Law enforcement and the private sector must continue to work together on threat analysis and prevention initiatives such as the No More Ransom project to raise awareness and provide advice and free decryption tools to victims of ransomware.[51]

It is clear that many sectors of critical infrastructure, those that are often overlooked in typical reporting such as hospitals, transport networks, telecommunications and even law enforcement, are vulnerable to every-day, highly disruptive cyber-attacks. These sectors must be better educated, prepared and equipped to deal with these attacks, leveraging EU and national efforts and resources, in particular the NIS directive and the General Data Protection Regulation (GDPR).

The international law enforcement community must build trust relationships with CSIRT/CERT communities, and public and private industry, so that it is adequately prepared to provide a fast and coordinated response in the case of a global cyber-attack affecting critical infrastructures.

Law enforcement should continue to share malware samples to allow for analysis and cross-matching, and the subsequent linking of cases, using the existing secure information exchange channels like SIENA and the Europol Malware Analysis Solution (EMAS).

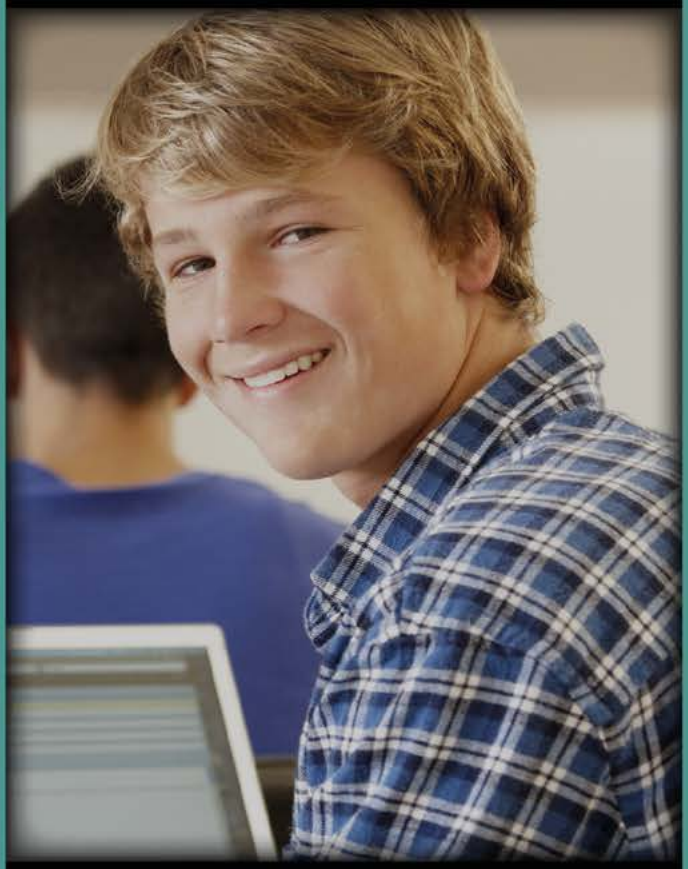
As exploit kits become less available, and malware developers move to rely further on social engineering, spam botnets, and other infection methods, law enforcement response strategies and prevention and awareness campaigns must adapt to these changes. Educating employees and the public to recognise and respond accordingly to social engineering attempts would prevent many cyber-dependent attacks.

PBX and VoIP systems often come with default passwords and security settings. Users of such systems should consider implementing the necessary security measures such as using strong passwords and disabling unused services and protocols.

Educators, parents and law enforcement should actively engage in and promote initiatives which channel young people interested in coding into positive activities, and to deter them from potentially following a path into cybercrime.[52] In December 2016, Europol launched a dedicated campaign to raise awareness of the associated risks and consequences, as well as offering advice for teachers in multiple languages.

SO, WHAT'S IT GONNA BE?

CYBERSECURITY EXPERT



STATUS

Health
Dexterity
Stamina
Happiness

CASH TOTAL

Skills in coding, gaming, computer programming and anything IT-related are in high demand by the public and private sectors. There are many careers and professional opportunities available.

CYBERCRIMINAL

STATUS

Health
Dexterity
Stamina
Happiness

CASH TOTAL

Young people getting involved with cybercrime could face:

- A visit and a warning from police
- Being arrested, a penalty or fine
- Prison, for serious offences
- Their computer seized and no access to internet
- Criminal records which can affect their education, future career prospects and travelling overseas options.

EUROPOL
EC3 | European Cybercrime Centre

#Up2U

Created by Europol

CRIME PRIORITY: CHILD SEXUAL EXPLOITATION ONLINE

Online child sexual exploitation epitomises one of the worst aspects of cybercrime. The hands-on abuse of vulnerable minors occurs very much in the real world, but it is captured, shared, distributed, encouraged and even directed over the internet. Unlike other areas of cybercrime, the primary focus for investigators working in this area is shifting from being offender centric to victim centric.

KEY FINDINGS

- Coercion and sexual extortion are increasingly being used to victimise children. Offenders use these methods to obtain further child abuse material, for financial gain or to get physical access to the victims.
- While peer-to-peer (P2P) networks continue to remain a key platform for the sharing and distribution of CSEM, reports indicate that every-day communication and social media applications are increasingly being used for the same purpose.
- Online offender communities operating from within the Darknet remain a primary concern, providing an environment for offenders to legitimise their behaviour, and to share both access to CSEM and OPSEC knowledge. The largest and most prolific offenders and communities identified by law enforcement had a significant presence on the Darknet.

KEY THREAT – SEXUAL COERCION AND EXTORTION (SCE) OF MINORS

As the internet becomes more accessible and available to younger generations, so do the tools and services for socialising and communicating online. Today children increasingly have access to the social media and messaging platforms which were undoubtedly designed and largely intended for adult use. As a consequence, social media sites are a key environment for online perpetrators to find, contact and groom potential victims. There is no one platform abused in this way; offenders will use whichever one suits them based on their language or location, whether it is popular social media sites or even some online dating sites.

For minors as well as adults, internet access is increasingly accomplished via mobile devices, which not only provide access to the social portals typically accessed via browsers on home computers, but also a continuously expanding range of social media, chat, and media sharing apps. These provide additional channels by which offenders can contact potential victims, in an environment where parents may have less visibility or control over their children's activities.

In order to initiate contact with a child, offenders use fake profiles representing either other minors or celebrities, and will often be in contact with large numbers of potential victims at the same time. Offenders will typically maintain multiple profiles across multiple social media platforms, allowing them to target different victims with an appropriate fake persona. Some offenders still use their own profiles or those of an adult depending on their modus operandus, preferences and the platform they are using.

Once online contact has been made between an offender and a potential victim, offenders are much more likely to attempt to obtain sexually explicit material from them, rather than aspiring to arrange an actual meeting. The offender will groom the victim, encouraging them to send compromising images or videos. Once these are in the possession of the offender, the offender will aggressively coerce or extort the victim, typically threatening to share the images with family, friends, or other peers, or post them publically on the internet unless their demands are met. Such offenders can be extremely persistent, maintaining their threats for months or, in some cases years. Predominantly the offender seeks to obtain increasingly sexual and explicit material from the victim; this may be images, or in some cases the offender may demand the victim display themselves live via the internet. While most offenders simply seek to obtain CSEM from their victims, the threat of coercing a minor into meeting for hands-on abuse still exists.

In a smaller number of cases a financial payment is demanded. There is evidence that this activity is increasingly carried out by organised crime groups running their operation akin to a call centre; targeting, manipulating and extorting their victims in an industrialised, systematic way in order to extract money from them.

Almost 70% of European countries report cases involving the sexual coercion and/or extortion of minors, with more than half indicating that this is a growing phenomenon. While sexual extortion is not exclusive to minors, some reports indicate that over 70% of sexual extortion cases brought to the attention of law enforcement involve only minors. Moreover, once a victim has conceded to an ultimatum, they are more likely to be subjected to continuing, repeated demands by the offender. The motivation of the offender often differs depending on the victim. When targeting another adult, the motive is typically financial; when the victim is a minor the offender more often seeks control over the victim.

In June 2017 Europol's EC3 launched its 'Say NO' campaign.[54] The campaign aims to help potential victims recognise prospective attempts to coerce or extort them, provides online advice, and highlights the importance of refusing the demands of the attacker, seeking help, and reporting the crime to the competent national authorities.

KEY THREAT – THE AVAILABILITY OF CSEM

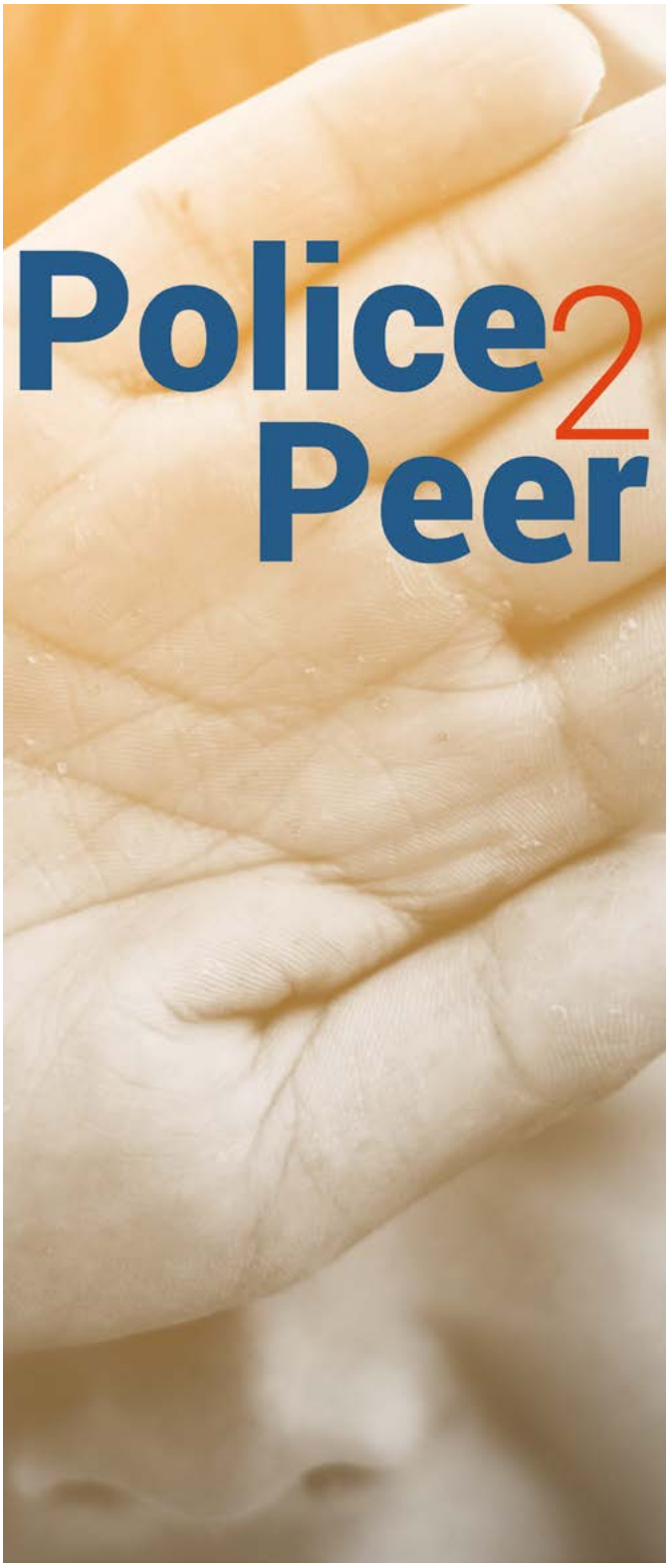
While the volume of CSEM produced via sexual coercion may be growing, it is still assessed to be grossly overshadowed by the volume produced by hands-on abusers. Moreover, the nature of the material produced by hands-on abusers is, by definition, of a much more serious nature. The trend of increasingly younger victims, including babies and toddlers, and increasing levels of violence continues.[55]

The dominance of peer-to-peer (P2P) networks for the sharing and distribution of CSEM remains unchanged from previous years. One country alone initiated over 700 new cases stemming from P2P networks; mostly from private groups on networks such as Gigatribe, but also from a significant number of public depositories such as eDonkey or Bit Torrent. In March 2017, European law enforcement launched the *Police2Peer* initiative to reach offenders operating on these networks.[56] Law enforcement record video messages, name them and other files that are empty or contain image warnings so that they appear to be CSEM, and make them available on file sharing networks. Anyone downloading and viewing these files will receive a message by the police informing them that their activities are neither safe, invisible nor untraceable, and urging them to seek help.

A perhaps more worrying trend than continued P2P use is the growing complacent use of conventional, every-day communication and social media applications for the same purpose. The growing number of apps incorporating media sharing which also provide end-to-end encryption provides offenders with a wide range of easily accessible, popular and ostensibly safe tools by which they can share child abuse material. Almost all commonly used mobile messaging or communications applications feature repeatedly in law enforcement investigations. To a lesser extent webhosting and traditional email services are also used to distribute CSEM. Most offenders will combine the use of multiple platforms to gather and share, or attempt to generate, CSEM.[57]

In April 2017, Europol and INTERPOL provided support to the Spanish National Police with Operation Tantalio, a complex investigation targeting the distribution of CSEM through Darknet platforms and invitation-only WhatsApp groups.

The joint action in Europe, against more than 30 suspects across five countries, was coordinated by Europol, with more than 100 targets focused on through INTERPOL in 13 countries across Central and South America. Altogether 18 different law enforcement agencies worldwide launched coordinated legal activities aimed at tackling this interconnected criminal network. The operation resulted in the arrest of 39 suspects in Europe and South America.[58]



While some countries maintain that the majority of CSEM is still found on the open/surface web, several European countries continue to report an increased use of the Darknet by offenders to store and share material, and to form closed communities where offenders can discuss their sexual predilections with like-minded individuals and legitimise their behaviour. In

February 2017, hacking group Anonymous hacked Freedom Hosting II, a hosting provider which hosted 10 000 Darknet web pages. In a public message left by the hackers, they indicated that 50% of the content related to CSEM.[59]

Data from INTERPOL's International Child Sexual Exploitation (ICSE) image database highlights that the majority of victims in CSEM appear to originate from Europe and North America. It also recognises a growth in the volume of new CSEM coming from South America and Russia as well as a rapid rise in the amount of new material originating from China.[60]

The phenomenon of self-generated indecent material (SGIM) also referred to as self-generated sexually explicit material (SGSEM), which was highlighted in previous year's reports, continues to grow with over 60% of European law enforcement agencies indicating an increase in the number of cases involving SGSEM. This is partly attributable to the growing number of sexual extortion cases in which such material is generated. SGIM is images or videos which minors have produced themselves; either voluntarily or as a result of coercion. However, even material produced voluntarily, perhaps to be shared with partners, friends or even on social media, can end up in the hands of offenders. As an example, in a 2012 study by the Internet Watch Foundation (IWF) which assessed images believed to be SGSEM, 88% of those images were found on websites other than that where they were originally published.[61] This highlights the activity of offenders actively searching for, and collecting such images to add to their collections, the loss of control an individual has once such an image is shared, and the lack of awareness minors have as to what can happen when they produce such material.

The discovery of SGSEM by an offender, or other media which suggests a minor is already extrovert or comfortable posting material about them, can act as a catalyst for the subsequent targeting, manipulation and coercion of the producer of that material.

Some countries highlight the continuing activities of 'fake' modelling agencies or photo studios run by offenders to influence minors into producing SGSEM.

KEY THREAT – COMMERCIAL SEXUAL EXPLOITATION OF CHILDREN

The majority of CSEM is produced by hands-on offenders not only to satisfy their own sexual appetite, but also to share and trade with other offenders. The commoditisation of this material continues to be a powerful means of reinforcing offenders' status in their communities. However, there is another aspect of CSEM production – that for financial gain.

While on the whole this does not appear to be a growing industry, some European countries do report an expansion of the Crime-as-a-Service business model, which supports other areas of cybercrime, into CSEM-*as-a-Service* – the production of CSEM on demand. This can include demands to produce sexual abuse material using different age groups, genders, or containing particular abuse acts or actions.

The full extent to which pay-per-view CSEM material is available and distributed is not fully understood, and requires further research. One aspect of the commercial distribution of CSEM

that is more widely investigated however is that of live-distant child abuse (LDCA), or the live streaming of child abuse.

LDCA is the live broadcast of video footage of a child being sexually abused, where the actions of the hands-on offender are directed by the viewer or viewers who are observing remotely.

There is no shortage of applications for streaming live video feeds. Some of the applications used for contacting victims or sharing material can also be used for this purpose, including many well-known and widely used applications, which often provide end-to-end encryption. Some countries also report the use of online conference facilities.

While cryptocurrencies such as Bitcoin may be used between offenders involved in the commercial distribution of CSEM, these currencies are less accessible to those performing the hands-on abuse in LDCA. Consequently, payment tends to rely on more centralised or traditional means such as online payment service providers, or money service bureaux.

With comparatively wealthy Westerners as the main 'customers' for this type of activity, the financial incentives for a poor family in Southeast Asia or Africa who are prepared to subject children (even their own) to this can be considerable, while for the consumer the costs are negligible.

Investigation of these cases can be additionally problematic due to the environments in which the abuse occurs. In the Philippines for example, there is free public wi-fi widely available even in poor neighbourhoods, making location via IP data very difficult. Moreover, the crowded and often temporary neighbourhood constructions in poor districts make physical location equally difficult.

While most countries report that growth of this activity is stable, one third still report an increase in the number of cases.

KEY THREAT – BEHAVIOUR OF OFFENDERS

The operational security (OPSEC) of CSE offenders differs little from that of cybercriminals. The use of VPNs, proxies and other anonymising solutions is commonplace if not standard practice. Where public wi-fi or the unprotected wi-fi signal of a neighbour is available, these are also exploited.

Encryption is widely used to safeguard communications and stores of child abuse material, potentially frustrating investigations and forensic analysis. Offenders also continue to form communities and forums on the Darknet where they not only share CSEM and benefit from a high level of anonymity, but learn and share OPSEC.

While these developments are neither new nor unexpected, over two thirds of European countries report that the general level of OPSEC among offenders is improving, and over half report that this causes significant impact on their investigations.

FUTURE THREATS AND DEVELOPMENTS

A key challenge for law enforcement, and one which continues to grow each year, is the volume of material to analyse for any

one investigation. Some reports suggest that a 'normal' case has between 1-3 terabytes of material to analyse, including 1-10 million images and thousands of hours of video footage, although there are claims of some cases as large as 100TB, with over 100 million images and thousands of hours of video material.[62] It is clear that using traditional, manual methods of analysis for these numbers are not sustainable. Several tech companies are making great leaps in developing solutions for image recognition, using novel and advanced methods that would likely be of considerable benefit should they be applied to the analysis of CSEM. It is therefore necessary that such solutions are available to law enforcement. This requires effective public-private partnerships and strong cooperation with industry and academia.

In January 2017 Europol's EC3 hosted its third Victim Identification Task Force (VIDTF). The VIDTF 3 saw 25 experts in victim identification from 16 countries and 22 agencies coming together to identify victims of child sexual abuse and exploitation using advanced techniques, software and their knowledge and expertise. As a result, victims of this damaging crime were located living in several countries in the EU and beyond.[63]

The 'Stop Child Abuse - Trace an Object' campaign[64] was launched by Europol in May 2017. Tracing a victim by their image alone is challenging, however child abuse images are often seeded with 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.

The Darknet will continue to become increasingly relevant in terms of the types of offenders operating there and the more extreme nature of the activities they are engaging in; creating a key environment for offenders to legitimise their behaviour, and to share both access to CSEM and OPSEC knowledge. Due to network speeds and storage limitations the majority of shared access

to CSEM takes place through links posted on Darknet forums to file hosting sites on the clearnet. As a result, the majority of CSEM will likely continue to be hosted on the surface web, in such file hosting sites, on P2P networks and in cyberlockers.

There will continue to be steady growth in not only the number and availability of mobile applications which can be used to chat, meet and share media, and the devices to access them on, but also in the access to these by minors. While this will create greater opportunity for offenders, it is slowly being countered by the growing momentum of coordinated EU-wide prevention and awareness campaigns aimed at educating minors on how to stay safe online. There is a requirement for these initiatives to be incorporated into classroom education, which we could then expect to lead to a decline in the number of minors falling victim to extortion and coercion or other online solicitations.

While it is expected that minors will become better equipped to stay safe online, the same can unfortunately be said for offenders. Communication and storage applications and devices increasingly come with encryption by default, which, along with data protection and privacy issues, means that law enforcement can increasingly be denied access to the relevant data it needs to locate and identify offenders and to secure evidence.

RECOMMENDATIONS

Member States should ensure that any investigative tool or measure used for combating serious and/or organised crime is also made available and used to full effect in investigating online CSE.[65] It should also be considered that prosecutions under organised crime statutes should be pursued for dealing with the key individuals creating, supporting and driving communities related to CSE crimes.

Further research within European law enforcement and beyond is required to identify the involvement of OCGs in the financially motivated sexual extortion of children and to form a coordinated response to this threat.

Crime recording and analysis systems in the Member States should be upgraded to better reflect and capture the different types of online sexual crimes being reported by or associated with child victims. This is particularly true for online sexual coercion and extortion but also applies to other types of CSEM related crime.

Europol should enable and coordinate the targeting, by Member States and partners, of key individuals creating, supporting and driving communities focused on child sexual abuse and exploitation and promoting operational security to their members.

The strategic and political commitments made by Member States through frameworks such as EMPACT and the WeProtect Global Alliance should be matched by the allocation of sufficient resources in the Member States.

Member States should strongly consider cooperating through Europol with agencies and bodies including the European Financial Coalition and other regional Financial Coalitions to tackle the increasing abuse of legitimate payment systems enabling child sexual abuse and exploitation.

Law enforcement agencies in the Member States should continue exploring through Europol how online resources, including electronic service providers, can help in diverting offenders from offending behaviour to resources that will help them cope with their sexual attraction to children.

Education is the best defence that can be provided to minors. It is therefore essential that the momentum for joint, EU-wide prevention and awareness activity is maintained so that strong and effective messages can reach those that need it. Integration in education, and the education of parents is also essential. In addition every opportunity must be made available to enable victims to report abuse. This will require the right legislation, environment, culture, reporting mechanisms and support network to be available.

CRIME PRIORITY: PAYMENT FRAUD

Fraud involving non-cash payments is an ever-present threat. Many aspects of this crime area are highly organised, highly specialised, and constantly evolving to adapt to both industry measures to combat it, and new payment technologies. This crime priority is divided into two, relatively distinct crime areas: card-not-present (CNP) fraud, which occurs largely online, and card-present fraud, which typically occurs at retail outlets and ATMs.

KEY FINDINGS

- The slow EMV implementation in certain regions continues to facilitate the cashing out of counterfeit EU payment cards abroad with the US and Southeast Asia remaining key destinations. Several sectors, such as the airline and accommodation industry, are targeted by CNP fraudsters as the services they provide can be used for the facilitation of other crimes, including trafficking in human beings (THB) or drugs, and illegal immigration.
- The lack of EU-wide criminalisation of the possession of stolen/compromised sensitive online payment credentials causes significant investigative challenges in this area.
- While the number of attempted black box attacks on ATMs is rising significantly, many attackers were unsuccessful.
- Direct attacks on bank networks to manipulate card balances, take control of ATMs or directly transfer funds, known as payment process compromise, represents one of the serious emerging threats in this area.

KEY THREAT – CARD-NOT-PRESENT FRAUD

The fraudulent use of compromised card data to make purchases online continues to plague the e-commerce industry. While law enforcement has some visibility with regards to the scale of the problem, it is very difficult to measure. The 'dark' figure for this crime area is assessed to be very high.

The retail sector is predictably one where law enforcement is most active, with growing numbers of cases in over half of European countries. This aspect of CNP is perhaps more 'accessible' compared to fraud in other sectors, carrying the least risk as it typically involves little or no direct interaction with the merchant or the physical presence of the offender to take advantage of the fraud.

Airline ticket fraud continues to have a high impact and priority across Europe. However, the number of cases across Europe appears to be stabilising. This may be attributable in part to the success of Europol's Global Airport Action Days which target airline fraudsters. Fraud relating to other transport industries, such as bus or train tickets, feature much less in European law enforcement cases, but follow the same modus operandi; tickets are typically purchased then resold to third parties on ridesharing, auction or purpose-made websites.

In June 2017, 153 individuals were detained following the sixth Global Airport Action Days (GAAD). These are major international law enforcement operations targeting airline fraudsters. The individuals are suspected of flying using airline tickets purchased with stolen, compromised or fake credit card details. Between 6 and 8 June 2017, 64 countries, 84 airlines and eight online travel agencies worked jointly with law enforcement officers to carry out operational actions in 230 airports across the world. During the actions, new modi operandi were identified as being used by organised crime networks to gain access to transit areas in airports in order to facilitate illegal immigration and drug trafficking.

Member States which report cases of fraud relating to accommodation (e.g. hotels booked using compromised cards) largely indicate that it is on the increase. Offenders using cards for this purpose often do not use the accommodation themselves, but instead sell/rent it onto third parties who are perhaps unaware that it has been fraudulently obtained. In some cases offenders are using rented accommodation as temporary drop addresses to receive goods purchased using compromised cards. Law enforcement identifies both individuals and OCGs involved in this type of activity. Where OCGs are involved, this crime is often linked to other crimes such as trafficking in human beings (THB) or drugs, and illegal immigration – crimes where temporary accommodation is required to facilitate the crime.

While each industry is targeted individually, online portals which combine multiple aspects of a journey, including flights, accommodation, car hire and other transport, are also key targets, as offenders can obtain tickets and bookings for several services in one purchase.

In addition to making purchases of goods and services, law enforcement in several European countries report the continued use of online gambling sites to directly launder the funds from compromised payment cards.

In March 2017, the Cypriot Police, with the support of Europol, the US Secret Service and the Investigative Committee of the Republic of Belarus, disrupted an organised criminal group that affected more than 130 000 payment card holders from 29 countries. Financial losses, including those for EU citizens, totalled EUR 8 million.

The criminal network established several fake online shops and a shell software company in order to make illicit cred it card transactions. Criminals connected to a legitimate online payment service and pretended to process multiple international transactions. They then transferred all the assets to a bank account in Cyprus. Due to many low-value transactions linked with internet services, the criminals were able to operate without detection for several months.[66]

AUTOMATED CARD SHOPS (ACS)

Compromised card data is traded on a variety of online platforms. However, a key source for offenders to purchase such data is automated card shops (ACS), sometimes referred to as automated vending cards (AVCs). These are automated click-and-buy websites where buyers can search for cards based a variety of search factors such as issuer, bank identification number (BIN), country, or even ZIP/postal code. Payment for cards is accepted almost exclusively in Bitcoins.

A recent study by Europol's EC3 identified more than 400 such websites, and assessed that this was merely a fragment of the total number. The example shown below displays the ACS which was part of the AlphaBay market operating on the Tor network. Like the main marketplace, the AlphaBay ACS is a multi-vendor site, with over 280 listed vendors selling card data. As of April 2017, the site was selling almost 330 000 cards, with over 55 000 cards from the EU. With the average loss per card of approximately EUR 350, this one ACS represents over EUR 115 million of potential fraud.

As a 'reputable', established marketplace, with a functional feedback system, it is highly probably that the vendors and card data displayed on the AlphaBay ACS were genuine. However, the research identified that a large number of ACS sites are scam sites, profiting from prospective carders paying to bypass pay-gates to access non-existent markets.

KEY THREAT – CARD-PRESENT FRAUD

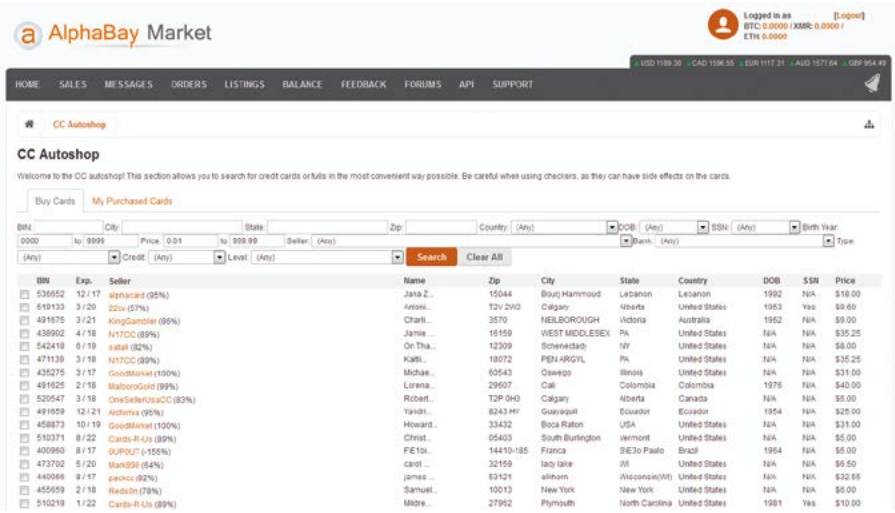
Card-present fraud requires an offender to present a physical card at an ATM, point-of-sale (POS) or other terminal. This crime has two stages: obtaining or producing a card, and the use of the card. The cards used are either lost or stolen genuine cards, or counterfeit cards.

A 2013 report highlighted that lost or stolen cards accounted for 43% of the value of fraud at ATMs and POS terminals. Furthermore, such fraud also typically takes place at the domestic level, which allows offenders to ignore industry security measures such as geoblocking.[67] Stolen cards, other than those acquired by theft, can be obtained via social engineering with the offenders often claiming to represent card issuers to obtain debit cards and PINs.

Counterfeit cards require the data from a genuine card. This is usually acquired using skimming devices fitted into the card slots of ATMs or other payment terminals coupled with micro-cameras to capture the customer's PIN. Alternatively such data can be captured by skimming malware installed on compromised ATMs or POS devices. Some Member States also indicate instances of collusion between merchants and OCGs in compromising particular POS devices. It is not only merchant POS devices that are compromised. Law enforcement is increasingly encountering skimming devices, including deep insert devices, in other, stationary, unmanned POS terminals, such as ticket machines in cinemas and train stations. Unlike fraud using lost or stolen cards, fraud using counterfeit cards is typically committed outside the Single Euro Payments Area (SEPA).[68]

Several Member States highlight the continuing prevalence of Bulgarian and Romanian OCGs in skimming activity.

The equipment required to conduct skimming is easily obtainable from the internet, often originating from Balkans regions or China, however some components or materials (like white plastic) are often available legally domestically. In previous reports we have highlighted the use of 3D printers to produce skimming devices and equipment (such as ATM panels). Developments in 3D printing technology have seen many consumer 3D printers hit the markets making it easier for criminals to acquire the technology they need to make custom components. Some OCGs have partly industrialised their processes, using workshops to produce counterfeit cards.



As more and more EU ATMs have become EMV compliant, the number of 'high-tech' attacks, such as skimming, has correspondingly declined. As a likely consequence, the number of low-tech incidents, such as card or cash trapping has increased.[68] However, only a few European countries reported incidences of such activity, suggesting that this activity may be localised to specific OCGs in specific countries.

A number of Member States also report cases of 'shimming'. Similar to skimming, this involves the insertion of a device into the card slot of an ATM or POS terminal. Like deep insert skimming devices, these are often invisible externally and can therefore remain undetected for long periods. Unlike skimming devices however, these either can additionally or exclusively read the data from the EMV chip. Some devices can then transmit the data wirelessly, without the need for the device to be removed. Depending on how the card is created, this data can be used to make counterfeit magnetic strip cards. The data cannot be used to replicate the chip however. Should the tools and capabilities to make shimming devices improve and become more widely available, it is likely that instances of shimming will increase.

While some European countries report high and increasing numbers of cases of device-based skimming, on aggregate skimming continues to decline throughout Europe.

Cases involving software skimming were only highlighted in three European countries. This activity appears to be carried out by OCGs different to those carrying out device-based skimming. Some countries report that travelling Eastern European groups controlled by Russian cybercrime gangs are amongst those involved in this activity.

CASHING OUT

The monetising of counterfeit EU cards occurs largely outside of the SEPA area. The destinations for compromised EU cards remain largely unchanged year on year with countries in South America and south-east Asia being key hotspots. Due to the slow rollout of EMV in the US as highlighted in previous year's reports, the US still also remains a key cash-out destination for counterfeit EU cards. As of November 2016, EMV adoption in the US was still only at 38%.[70]

Outside of the usual destinations, some Member States also highlight several Caribbean islands as locations where counterfeit EU cards are cashed-out. Furthermore, some European countries bordering the EU, such as the Ukraine, also record a growth in the amount of EU cards cashed-out in their jurisdictions.

While there are some technical skills involved in the various aspects of skimming, when true cyber skills are deployed, attacks upon ATMs can be of a much greater scale in terms of losses. ATM 'jackpotting' involves the connection of an unauthorised device which sends dispense commands directly to the ATM cash dispenser in order to 'cash-out' the ATM, without having to use a credit or debit card.[71] *Black box* attacks require the attacker to physically breach the ATM (by drilling or melting a hole) in order to connect their device. The European Association for Secure Transactions (EAST) reports a 287% increase in this type of attack from 2015-2016, although many attacks were unsuccessful.[72]

In May 2017, 27 individuals linked to ATM 'black box' attacks were arrested across Europe following the efforts of a number of EU Member States and Norway, supported by Europol's EC3 and the Joint Cybercrime Action Taskforce (J-CAT).

Perpetrators responsible for these attacks were identified in a number of countries between 2016 and 2017. Arrests were made in Czech Republic, Estonia, France, the Netherlands, Romania, Spain and Norway.[73]

A more effective method, of which there are a growing number of examples, is to either hack into a bank's systems to remotely infect ATMs in order to trigger them to dispense cash, or to access a card issuer's authorisation system to manipulate card balances, withdrawal limits and other factors, effectively allowing unlimited withdrawals at ATMs using debit cards under control of the OCGs. Using the latter technique, one European country reported OCGs able to withdraw up to EUR 200 000 per card. Europol also notes the increasing use of pre-paid cards in these schemes.

In 2014-2015, the Carbanak OCG infiltrated bank computer systems in up to 100 financial institutions around the world. Once they had access to the ATM network, part of their attack strategy included remotely commanding ATMs to dispense cash. The entire campaign resulted in over USD 1 billion in losses. More recently the Cobalt OCG has remotely infected ATMs with malware in more than dozen countries across Europe to do the same. This includes ATMs belonging to banks in Armenia, Belarus, Bulgaria, Estonia, Georgia, Kyrgyzstan, Moldova, the Netherlands, Poland, Romania, Russian, Spain, and the United Kingdom.[74]

FUEL CARD FRAUD

A number of European countries highlight that compromised cards are not only used to make fraudulent purchases or cash withdrawals from ATMs. Many international logistics companies use fuel cards to allow their transport drivers to refuel en route. There is no requirement for these cards to be EMV compliant; they are therefore more vulnerable to being copied, counterfeited and used by OCGs to fraudulently refuel vehicles under their control. Such activity often goes undetected as many fuel pumps are automated and high usage is normal.

FUTURE THREATS AND DEVELOPMENTS

The technology and the means to exploit payment cards has been around for long enough that, while the phenomenon is becoming increasingly global, there is little to be expected in terms of new threats. While OCGs will develop new devices and techniques to gather and use compromised card data, the fundamental crime remains the same.

In cyber-dependent crime, instead of attack methods becoming increasingly sophisticated, attackers are increasingly resorting to 'old school' methods to reach their targets, such as social engineering or infected email attachments. The same trend is occurring in payment fraud as criminals revisit old, low-tech modus operandi such as cash traps, while industry perhaps focuses on trying to combat more sophisticated threats.

In previous years reports we have highlighted the potential for criminals to compromise and abuse NFC payment cards. The use of contactless payments continues to increase across Europe with 1-in-5 card payments processed by Visa now being contactless. Consumers in Poland, Spain and the UK are among the top users of contactless payments.[75] In the UK, 32% of total purchases are contactless[76], with 72% of debit cards issued now contactless.[77] However, there is little indication that NFC cards are being abused by criminals or that they are being compromised and counterfeited as EMV or magnetic strip cards are. Where there are indications of fraudulent NFC payments, these instead relate to mobile apps such as Apple Pay, Samsung Pay or Android Pay, which have had compromised card data loaded onto them and subsequently used to make fraudulent purchases.

As industry releases new payment technologies, criminals will continue to test and experiment to find ways to exploit them for criminal gain. While criminals may enjoy some period of gain while they exploit these weaknesses, the payment industry will similarly continue to work to seal off these opportunities as they are identified. There is also ongoing work by the European Commission to review the Council Frame Decisions on Combating Fraud and Counterfeiting of Non-cash Means of Payment with a view to possibly extending the scope to take account of newer forms of crime and counterfeiting in financial instruments, as well as the associated investigative challenges.[78]

In November 2016, Europol's EC3, together with the Joint Cybercrime Action Taskforce (J-CAT), Eurojust and the European Banking Federation coordinated the second European Money Mule Action week, which culminated in the arrest of 178 individuals. Law enforcement agencies and judicial authorities from Bulgaria, Croatia, France, Germany, Greece, Hungary, Italy, Latvia, Moldova, the Netherlands, Poland, Portugal, Romania, Spain, United Kingdom, Ukraine, the United States FBI and Secret Service, participated in the international operation. The successful operation was further supported by 106 banks and private-sector partners.

RECOMMENDATIONS

Law enforcement and the private sector should continue devel-

oping initiatives based on mutual cooperation and information sharing to combat payment fraud, based on successful models like the Global Airline Action Days and e-Commerce Action weeks.

Law enforcement should keep up to date with emerging payment methods and engage with providers at an early stage to ensure that the channels are there in the event that criminals target their payment system for abuse. Robust Know-Your-Customer (KYC) and due diligence practices in the banking sector and in relation to alternative payment systems are essential for the prevention and mitigation of the monetisation of cybercrime as well as money laundering.

Further research is required to ascertain the extent to which payment card fraud is used to directly or indirectly fund or facilitate other areas of organised crime such as THB, illegal immigration or drug trafficking.

In order to deny their use by criminals and prevent further fraud, law enforcement should share details of compromised payment cards with the appropriate card issuers at the earliest opportunity in order to allow them to take appropriate action.

Payment fraud is characterised by a high volume of low value crime incidents, the full scope of which cannot be envisioned by local reporting and the investigation of individual single illegal transactions. A more coordinated and intelligence-led approach to combatting payment fraud is required throughout the EU and beyond.

Law enforcement should continue to build enhanced cooperation with LEAs in regions outside the EU where the cashing-out of compromised EU cards occurs.

CRIME PRIORITY: ONLINE CRIMINAL MARKETS

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

KEY FINDINGS

- Darknet markets are a key crosscutting enabler for other crime areas, providing access to, amongst other things, compromised financial data to commit various types of payment fraud, and fraudulent documents to facilitate fraud, trafficking in human beings and illegal immigration.
- While an unprecedented number of users make use of Tor the Darknet is not yet the mainstream platform for the distribution of illicit goods, but is rapidly growing its own specific customer base in the areas of illicit drugs, weapons and CSEM.
- Compared to more established Darknet market commodities, such as drugs, the availability of cybercrime tools and services on the Darknet appears to be growing relatively faster.

KEY THREAT – DARKNET MARKETS

While there is also a significant volume of trade in illicit goods on the surface web, any overt sales, not restricted to closed criminal markets, are often limited to stolen, fraudulently obtained or counterfeit goods, all of which can be sold under the pretence of being legitimate. Law enforcement, domain registrars and hosting providers would be able to rapidly respond to anything of a clearly illegal nature sold on a website using regular hosting.

This has driven the sale of illicit goods to dedicated criminal websites and markets hosted on anonymising networks such as Tor, I2P and Freenet, although such activity appears to be mainly concentrated on the Tor network. This transition is clearly demonstrated, for example, by the sale of gun parts or de-activated firearms which is legal in certain jurisdictions and thus available on the surface web. Once the firearms have been assembled or re-activated they are illegal and will then be traded on the Darknet. Similarly, new psychoactive substances (NPS) are at first not regulated, and can be sold on the surface web, but as soon as they become regulated or banned, sales will migrate to the Darknet. While some markets cater to specific product types such as drugs or financial data, many host vendors who collectively sell a large variety of illicit goods.

The scale of these networks is well documented. For instance, as of June 2017, the Tor network had over 2.2 million directly connecting users, and hosted almost 60 000 unique .onion domains. What is difficult to quantify is the proportion of activity on these networks that is illicit, compared to its legitimate use by regular users to browse the web more securely. In one study however, almost 57% of active sites that could be classified related to some form of illicit activity.[80]

The trade in illicit goods on the Darknet has a number of added advantages for both buyer and seller. Firstly, transactions have a high degree of anonymity; neither the customer nor vendor need reveal any personal information about themselves, although the customer must provide a delivery address when purchasing physical goods. Transactions are also carried out using hard-to-trace virtual currencies such as Bitcoin. There is also a reduced physical risk compared to a street sale. Trade on the Darknet is also accessible to anyone with an internet connection, regardless of age or location, and presents them with a huge diversity in suppliers and illicit products. Finally, the quality of particular goods and the reliability of a vendor are often rated by customers.

A combination of these factors has opened up the trade in illicit goods to not only new customers who might otherwise lack the opportunity or desire to deal with real world criminal vendors, but also to new criminal merchants, many of whom can operate as lone offenders, who may otherwise find it hard to operate in real world markets where organised crime groups may hold a monopoly.

Throughout 2016, there were few areas of criminality on the Darknet where law enforcement did not record increasing

levels of activity. However, law enforcement has two main areas of focus when it comes to investigations on the Darknet: the drugs market, and trade in online child abuse material.

ONLINE TRADE IN DRUGS

The drugs market is undoubtedly the largest criminal market on the Darknet, offering almost every class of drug for worldwide dispatch. As of June 2017, AlphaBay, one of the largest Darknet markets, had over 250 000 separate listings for drugs, accounting for almost 68% of all listings. 30% of the drugs listings related to Class A drugs. While it is assessed that the majority of vendors are lone offenders, dealing in small amounts, it is reported that many of the 'top sellers' are likely organised crime groups earning significant profits. Some studies suggest that the total monthly drugs revenue of the top eight Darknet markets ranges between EUR 10.6 million and EUR 18.7 million when prescription drugs, alcohol and tobacco are excluded.[81]

ONLINE TRADE IN CHILD ABUSE MATERIAL

One online community operates distinctly to those on criminal marketplaces: those dealing in child abuse and child abuse imagery. These customers and commodities are neither wanted nor welcomed on criminal market places, and consequently form their own closed communities on the Darknet. This activity is discussed in greater depth elsewhere in this report.

CYBERCRIME TOOLS AND SERVICES

Most cybercrime communities, where tools and services for committing cybercrime can be bought and sold, appear to operate largely outside of the Darknet, on language-specific forums on the deep web. However, the market for cybercrime tools on the Darknet appears to be growing steadily. On AlphaBay there were over 75 000 listings for products and services related to numerous cyber-dependent or cyber-facilitated crime areas by the end of 2016, a 25% increase from the start of the year. For tools for cyber-dependent crime, such as exploits, exploit kits, botnets and malware, there was over a 200% increase in the same period.

While the extent to which cybercrimes available on Darknet markets compare to those available on established cybercrime forums in the deep web remains unclear, several Member States highlight that services such as bullet-proof hosting, malware and Ransomware-as-a-Service are readily available.

ONLINE TRADE IN COUNTERFEIT GOODS

Infringements of intellectual property rights (IPR) are a widespread and ever-increasing worldwide phenomenon. In 2013, the international trade in counterfeit products represented up to 2.5% of world trade. The impact of counterfeiting is even higher in the European Union, with counterfeit and pirated products amounting to up to 5% of imports.[82] As discussed earlier, most counterfeit products can more readily be sold on the surface web, being presented as, or mixed with, genuine products. Consequently, counterfeit products only account for between 1.5% and 2.5% of listings on Darknet markets. Moreover, the most commonly listed counterfeit products are those which are obviously illegal - counterfeit bank notes and fake ID documents, which account for almost one third and almost one quarter of counterfeit listings respectively. The majority of reported law enforcement investigations in the EU relating to counterfeit goods on the Darknet relate to counterfeit bank notes.

In July 2016, to strengthen the fight against counterfeiting and piracy online and offline, Europol and the European Union Intellectual Property Office (EUIPO) joined forces to launch the Intellectual Property Crime Coordinated Coalition (IPC3). The IPC3 provides operational and technical support to law enforcement agencies and other partners in the EU and beyond by facilitating and coordinating cross-border investigations, monitoring and reporting online crime trends and emerging modus operandi, enhancing the harmonisation and standardisation of legal instruments and operating procedures to counter intellectual property crime globally, and reaching out to the public and law enforcement by raising awareness and providing training on this specific field of expertise.

ONLINE TRADE IN DATA

Compromised data is another key commodity commonly traded online, and subsequently used for the furtherance of fraud. Typically this is financial data such as compromised payment card data - both 'dumps' (the data copied from the magnetic strip of a card) and 'CVVs' (the data required to make an online or telephone card purchase), or bank account logins. However, any data that could be exploited to commit fraud or other crimes is also readily available for sale. This includes everything from lists of full personal details and scanned documents to email lists and online account logins.

While compromised data typically ranks as the second or third largest category of listing on most Darknet markets, this activity is by no means concentrated on the Darknet. The surface web is host to a large number of websites selling compromised card data, particularly automated credit card shops which often stock tens of thousands of stolen credit cards. That said, AlphaBay also ran one of the largest known card shops on the internet.

ONLINE TRADE IN WEAPONS

Only a few markets openly list weapons as a category of commodity sold on their sites. For those that do, they typically account for less than 1.5% of their total listings, although on AlphaBay, this still represented well over 5000 listings. Given the number of

terrorist attacks throughout 2016/2017, the potential easy availability of firearms and explosives is a worrying trend.

In December 2016, assisted by intelligence provided by Europol's Firearms Analysis Project to the Slovenian National Police, two Slovenian nationals were arrested in Ljubljana for allegedly selling lethal weapons and explosives on the Darknet. A large quantity of weapons uncovered during the house searches were also seized, including automatic and semi-automatic guns, hand grenades and ammunition. The two suspects sold weapons on the Darknet which were then sent via postal mail to buyers throughout Europe.

FUTURE THREATS AND DEVELOPMENTS

Darknet markets continue to grow each year, in both numbers and size, with new markets opening either spontaneously or to fill the void from other markets shutting down, either voluntarily, following an exit scam, or as a result of law enforcement activity. Darknet markets remain a substantial threat, providing easy, anonymous access to a large variety of illicit commodities which facilitate or enable a cascade of other crimes.

In June and July 2017, two major law enforcement operations, led by the Federal Bureau of Investigation (FBI), the US Drug Enforcement Agency (DEA) and the Dutch National Police, with the support of Europol and a number of other LEA partners, led to the takedown of two of the largest Darknet markets: AlphaBay and Hansa.

AlphaBay was the largest criminal marketplace, utilising a hidden service on Tor to effectively mask user identities and server locations. Prior to its takedown, AlphaBay reached 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 and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and fraudulent services. A conservative estimate of USD 1 billion was transacted in the market since its creation in 2014, paid in Bitcoin and other cryptocurrencies.

Prior to the takedown of AlphaBay in July, the Dutch National Police, with the assistance of authorities in Germany and Lithuania, had seized control of the Hansa servers, allowing them to covertly take over the marketplace and collect valuable information on high-value targets and delivery addresses.

Hansa was the third largest criminal marketplace on the Dark Web, trading similarly high volumes in illicit drugs and other commodities.

In shutting down two of the three largest criminal Darknet marketplaces, a major element of the infrastructure of the underground criminal economy has been taken offline. It has severely disrupted criminal enterprises around the world, has led to the arrest of key figures involved in online criminal activity, and yielded large amounts of intelligence that will lead to further investigations.

Leveraging the combined operational and technical strengths of multiple agencies in the US and Europe, the operation has been an extraordinary success and a stark illustration of the collective power the global law enforcement community can bring to disrupt major criminal activity.

Law enforcement has shown that it is capable of action against Darknet markets in their current form. In previous years' reports we have highlighted the potential threats posed by decentralised markets, which would be resistant to such intervention. In April 2016, the first such market was launched. Despite earlier concerns, so far the volume of criminal activity on the market has turned out to be minimal. This may have been due, in part, to the fact that users' IP addresses were not hidden. In February 2017 however, the development team behind the market announced that the code to integrate Tor was ready. The code is still currently in the experimental stages so the impact of how this will affect the market and how much illicit trade it will attract has yet to be seen.

RECOMMENDATIONS

While the expertise for investigating crime on the Darknet often resides within cybercrime units, only a small proportion of the criminality thereon relates to cyber-dependent crime. It is therefore essential that investigators responsible for all crime areas represented on Darknet markets obtain the knowledge and expertise required to effectively investigate and act in this environment.

Law enforcement must continue to cooperate and collaborate, and share tools, expertise and intelligence, in order maintain the momentum in the successful concerted effort law enforcement has made in tackling crime on the Darknet.

Law enforcement needs to develop a globally coordinated strategic overview of the threat presented by the Darknet, and monitor and understand emerging threats and relevant developments. Such analysis would allow for future coordination of global action to destabilise and close down such marketplaces.

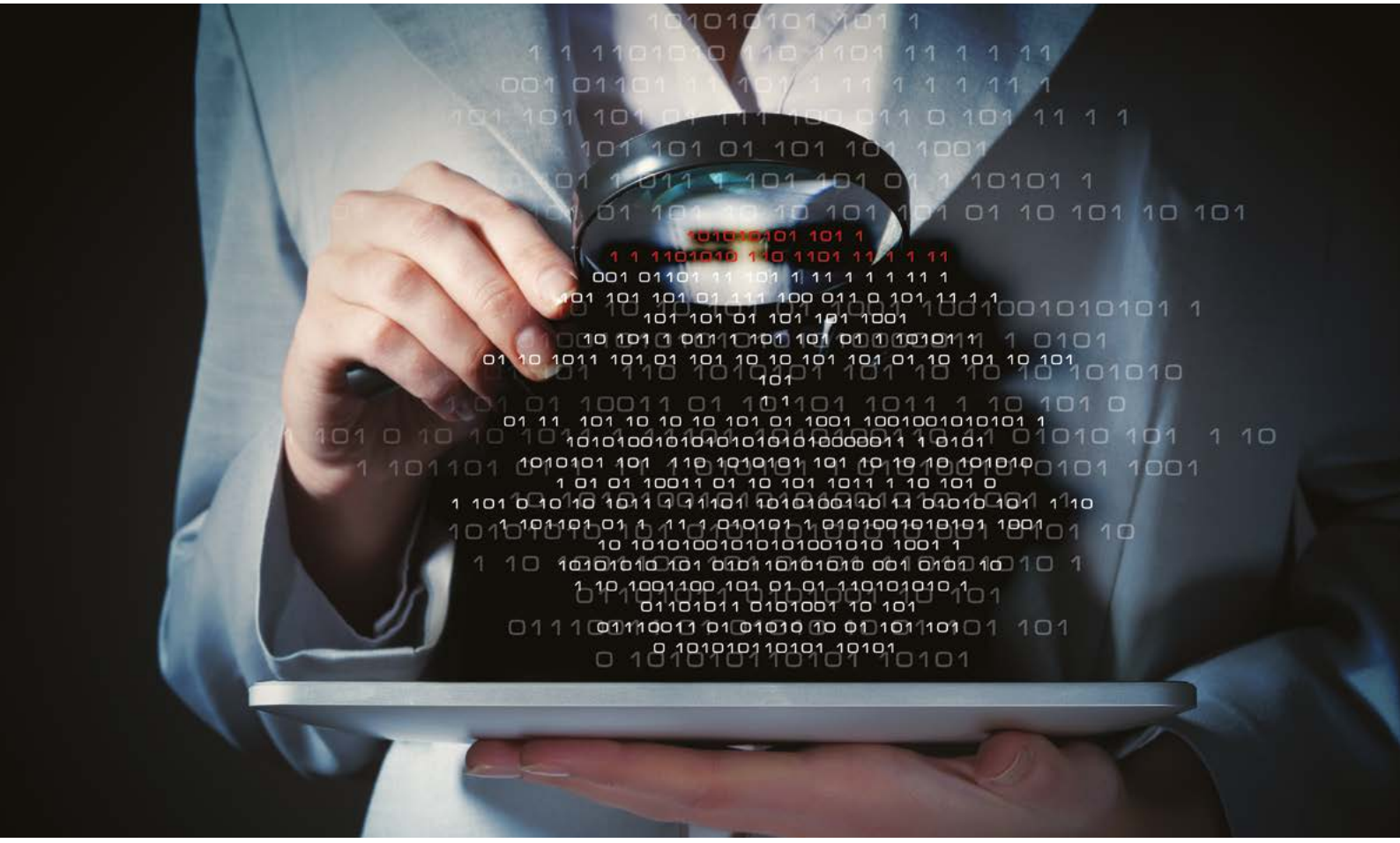
This is the splash page users will see when attempting to log into the Hansa Darknet market.

THE CONVERGENCE OF CYBER AND TERRORISM

Counter-terrorism investigations in Europe have shown that the use of the internet is an integral component in any terrorist plot.

KEY FINDINGS

- While terrorists continue to use the internet mostly for communication, propaganda and knowledge sharing purposes, their capabilities to launch cyber-attacks remain limited.
- Most terrorist activity concerns the open internet; however there is a share of terrorist exchange in the Darknet too. The concerns mostly fundraising campaigns, the use of illicit markets and advertisement of propaganda hosted on mainstream social media.



RECRUITMENT AND PROPAGANDA

Terrorist recruitment on the internet is often limited to cases when the recruiting agent was previously known to recruits through sharing the same social networks. Experimentation with social media in recent years has encouraged terrorists to rely on the relatively safe environment of the internet to conduct their activities. Despite the noise created by counter-messaging and disinformation campaigns, major terrorist groups such as the so-called Islamic State (IS) and al-Qaeda (AQ) still manage to get their propaganda messages through to a wide variety of audiences. IS has put forward a sophisticated communication strategy on social media through the employment of a robust network of core supporters (core disseminators) who are responsible for maintaining an uninterrupted online presence for the terrorist organisation. To that end the terrorist media campaigns are being prepared in encrypted social media platforms, such as Telegram, before the terrorist message is spread to the wider social media network. At the time of writing, Europol's EU IRU has identified over 150 social media platforms abused by terrorists to perform a variety of roles in their strategy of propaganda dissemination: file sharing sites that function as terrorist content depositors; messaging and bot services that advertise links to content; social media aggregators in which content can be stored, streamed and advertised to other social media at the same time.

Over the past year, territorial loss and dwindling resources in terms of infrastructure and human capital have had an adverse impact on IS's propaganda production. In particular, there has been a noticeable decline in the release of new audio-visual material, which is also accompanied by lower production of textual content and photo-reports. To compensate, IS's media

apparatus has concentrated its efforts on the creation of special social media accounts (i.e. Telegram channels) operated by core disseminators and bots and dedicated to the regular re-uploading of older productions. This action is instantly replicated to a large number of pro-IS channels and advertised with outlinks to the galaxy of social media ensuring the availability of content for longer periods of time. In fact, the recycling of propaganda serves the purpose of maintaining a virtual presence on the internet that would survive the collapse of the territorial caliphate for IS. In these changing circumstances it seems that one of the IS-leadership priorities is to leave the virtual content as a legacy and point of reference for the future generations of jihadis.

Terrorist propagandists' focus on the 'echo phase' (re-uploading of old, high profile propaganda items) and agile move across social media puts challenges to the disruptive efforts by law enforcement and social media companies alike. Although recent efforts resulted in curbing terrorist abuse of mainstream platforms such as Twitter, YouTube and Facebook, among others, similar progress has yet to be made with start-up social media and companies with limited resources. Differences in assessment of content, lack of linguistic capabilities and expertise, are being exploited by terrorists to infest social media with their toxic messages. In that regard, new initiatives bringing social media companies together to devise common strategies to fight abuse by terrorists are under way. These efforts are being supported by law enforcement and the EU IRU in particular with sharing expertise and best practices in flagging terrorist content.

TERRORIST OPSEC

The use of encrypted instant messaging services by terrorists remains a concern. Apart from elements on jihadist security awareness in the official terrorist propaganda, user-generated content (video tutorials, manuals) with tips on how to conduct secure communications is an increasing phenomenon. Encrypted communication is of particular importance to the preparation of plots and subsequent claim of responsibility. It has been observed that short video messages are being shared by the perpetrators with their handlers prior to an attack through encrypted apps. Those would reach IS's media department which would claim the attack through its central news agency 'A'maq', uploading the perpetrators' video as a proof. This method shows that besides dominating the virtual space, the terrorist organisation has deployed a physical network of media operatives on the ground that follow the security protocol for jihadist communications.

CYBER-ATTACKS

The absence of any major cyber-attacks by terrorist organisations can be interpreted as the result of not enough technical skills on their side, at least for the present time. In fact, the targeting of jihadist cyber experts, in the past year, by anti-IS forces appears to have further contributed to the weakening of the jihadist cyber infrastructure and capabilities. This hypothesis can be supported by the diminishing activity of pro-IS hacking conglomerates such as the so-called United Cyber Caliphate (UCC) which specialises in the publication of 'kill-lists' compiled with the method of doxing. Nonetheless, jihadist receptiveness of new technologies and commitment to 'jihad in the virtual space' leaves little room for complacence.

FUTURE THREATS AND DEVELOPMENTS

The difficulty in disrupting the terrorist propaganda online has encouraged an increasing number of jihadist sympathisers to produce their own content to glorify terrorism and incite followers to commit new attacks. As official propaganda is in steady decline, this user-generated content gains in visibility and importance, requiring special focus by the law enforcement authorities.

RECOMMENDATIONS

Cooperation and coordination of effort among the multitude of stakeholders in law enforcement and the private sector is required for a robust answer to the jihadist online threats and to ensure the attribution of such acts in cyberspace.

Law enforcement must continue to engage with and support social media companies in initiatives to devise common strategies to fight their abuse by terrorist groups.

CROSS-CUTTING CRIME FACTORS

Cross-cutting crime factors are those which impact on, 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, the Internet of Things and social engineering. In this chapter we will also address common challenges faced by EU law enforcement.

KEY FINDINGS

- Social engineering techniques are an essential tactic for the commission of many, often complex, cyber-dependent and cyber-facilitated crimes, but one which can be countered with adequate training.
- While Bitcoin remains a key facilitator for cybercrime, other cryptocurrencies such as Monero, Ethereum and Zcash are also gaining popularity within the digital underground.
- The ease with which new bank accounts can be opened in some countries, particularly online accounts, is facilitating the laundering of illicit funds by money mules.
- Criminal forums still remain a key environment for cyber-criminals, providing meeting places and market places, and allowing access to the skills and expertise of other members of the cybercrime community.
- Law enforcement is witnessing a transition into the use of secure apps and other services by criminals across all crime areas. The majority of the apps used are the everyday, brand names popular with the general populace.
- A combination of legislative and technical factors which deny law enforcement access to timely and accurate electronic communications data and digital forensic opportunities, such as lack of data retention, the implementation of CGN, and the criminal abuse of encryption, are leading to a loss of both investigative leads and the ability to effectively attribute and prosecute online criminal activity.

SOCIAL ENGINEERING

Social engineering is the use of deception to convince a person to either unwittingly divulge sensitive information or carry out some act which they otherwise would not normally do. While this sounds simplistic, many crime areas, both cyber-dependent and cyber-facilitated, rely heavily on social engineering tactics in order to be successful. The reason for this is simple: IT security systems are objective, operating by measurable rules and parameters and are therefore harder to breach with a direct technical assault. Conversely, humans are subjective, and that subjectivity can be exploited in order to bypass those technical security measures, relying instead on the victim's trust and lapses in judgement.

Many cyber-dependent crimes commonly use social engineering in order to obtain a foothold in a target network or computer. Some of the top malware threats highlighted in this report, such as Dridex, Locky, Ramnit and Cerber, all use malware-loaded spam either in conjunction with other infection methods, or exclusively, as a means to infect their targets. Similarly, many sophisticated network intrusions by threat actor groups, such as the Carbanak group in 2015[83], or more recently the Cobalt group[84], both of whom infiltrated bank networks in order to transfer funds and/or jackpot ATMs, relied on an initial spear

phishing attack to target employees within the target institutions. A common approach is to attach a malicious attachment to an email, often a Microsoft Office document containing malicious macro code – a tactic that Dridex is notorious for resurrecting. Alternatively the message may include a link to a malicious URL which will then attempt to infect the target computer when they visit the site. However, some reports suggest that up to 60% of hacks do not use malware at all, instead relying solely on compromised credentials and social engineering.[85]

Similarly, many cyber-facilitated crimes rely heavily on social engineering such as the grooming of children online. In payment fraud, social engineering is used to obtain genuine payment cards and PIN numbers from victims. Social engineering is also a key component in all other cyber-facilitated frauds, including IT support scams, advance fee frauds and romance scams, all of which are still prevalent throughout Europe.

There are two main types of social engineering attacks commonly reported to EU law enforcement: phishing and business email compromise.

PHISHING/SMISHING/VISHING

Phishing, smishing and vishing are all forms of social engineering that rely on unsolicited communications by email, SMS or telephone respectively, where the attacker purports to represent a third party, typically in an attempt to convince the victim to divulge sensitive information, such as login credentials or payment details. Credentials for any and all online accounts are phished for, with the most common targets being e-commerce, banking and financial services, social networking accounts, and money transfer services.[86] Some reports indicate that over 57% of all global phishing attacks targeted only four companies, however – PayPal, Yahoo!, Apple and Taobao.com.[87]

While some of these attacks are purely for direct financial gain, others are just the first step in a more complex attack, such as installing malware on the target's computer, ID theft, or gaining key login credentials which might be essential to further cyber-attacks.

Of these attacks, phishing is naturally the most common, as it is easy to spam potential victims en masse. Some reports suggest attackers use email to contact their victims 95% of the time.[88] Almost 40% of Member States highlighted investigations into phishing. Two trends continue from previous year's reports; year on year phishing continues to increase, and phishing emails continue to become more professional and 'believable'. The Anti-Phishing Working Group (APWG) recorded that the total number of phishing attacks in 2016 was 65% higher than in 2015.[89]

In March 2016, the German Police (Hessisches Landeskriminalamt), in close cooperation with law enforcement officers from Latvia, the UK and Europol, disrupted an international criminal group involved in phishing, hacking bank accounts, spreading malware, fraudulent transactions and money laundering. Losses incurred by the criminals' activities were estimated to be several million euros.

The modus operandi of the criminals consisted of obtaining one-time codes and passwords to get online access to credit balances, and spying on victims as they received transaction authentication numbers (TANs) on their cell phones.[90]

BUSINESS EMAIL COMPROMISE

Business email compromise (BEC) takes a number of forms, but typically involves some variant of spoofing or hacking a high ranking company executive's email or that of a third party supplier, in order to instruct an unwitting employee to make a payment to accounts under the fraudster's control. In some instances this may involve malware, such as key loggers[91], although in most cases it is pure social engineering.[92]

Unlike 'normal' phishing, most BEC frauds are highly targeted and may require some reconnaissance or research in order to successfully target a particular company or individual.

BEC was the most commonly reported social engineering scam reported in the EU, with almost 50% of Member States reporting cases, and with two-thirds of those reporting that the threat is increasing. The victims highlighted by law enforcement were almost exclusively small to medium sized businesses (SMBs).[93] Industry reporting emphasises that while the majority of BEC frauds occur in the US, within Europe attacks are concentrated in the UK, with France and Norway also affected.[94] In August 2016, German wire manufacturer Leoni AG suffered reported losses of EUR 40 million, allegedly as a result of such a scam.[95] Globally, since 2013, the known BEC frauds have cost companies over an estimated USD 5 billion.[96]

Two main modi operandi dominated European law enforcement cases: CEO fraud and mandate fraud.

In mandate fraud, fraudsters spoof the email address or website of, for example, a foreign third party supplier or other company the victim makes regular payments to. They often manage to do this by changing only a single letter in the character string. They then provide an alternate, fraudulent payment destination for the victim company to make payments to.

CEO fraud is not dissimilar, except the email address impersonated is that of an internal executive, typically someone high ranking (hence the name CEO fraud). The fraudsters then use that email to direct other employees to make (often urgent)

wire transfers to an account they control. In most cases spoofed email addresses are used for these attacks, with these being relatively cheap and simple to create. In a smaller number of cases the targeted executives have their accounts compromised, perhaps from an earlier phishing attack or the compromise of the company's email server.

Several reports highlight that attacks of this nature are increasingly originating from west Africa, as west African cybercriminals evolve their tactics from more traditional areas of social engineering such as advance fee fraud.[97,98]

FUTURE THREATS AND DEVELOPMENTS

Targeted social engineering attacks often require some data gathering and research by attackers, to obtain such information as company structure, supplier details, and employee email addresses. Much of this can already be obtained with minimal effort using OSINT. The growing amount of data about our lifestyles, activities and habits produced by the Internet of Things is likely to make identifying an individual from their unique 'lifestyle fingerprint' a possibility. This is likely to offer entirely new avenues for data harvesting to be used in phishing attacks.

As we have seen in other areas, criminals often revisit 'old' techniques as they often prove effective while industry and law enforcement focus on combating the current popular or emerging tactics. Criminals involved in the production of spam have returned to a technique known as a 'hailstorm', which uses large numbers of IP addresses to send low volumes of spam emails per IP address, thereby attempting to avoid reputation or volume-based spam filters. With the growing number of cases involving malware-infected IoT devices, it is likely that we may see an increasing number of further attacks of this nature harnessing IoT botnets.

CRIMINAL COMMUNITIES AND CRIME-AS-A-SERVICE

One of the more unique aspects of cybercrime is the large communities that cybercriminals form online, where those just beginning their criminal careers can rub virtual shoulders with experienced cybercrime veterans. This is a trait particular to cybercrime, not seen in other crime areas, and is undoubtedly a legacy from the days before cybercrime as we know it, when these communities were purely the domain of internet enthusiasts.

Today however, these communities are the places where cybercriminals learn from their peers and betters, and buy and sell the services and tools needed to commit crime online. Here cybercrime differs again from more traditional crime areas. The term 'cybercrime', as it is used in this report, clearly covers a wide range of criminality, and a wider range of skill-sets. Given the particular level of expertise required for certain aspects of cybercrime, particularly in the cyberdependent area, it is highly unlikely that any one person would have the breadth of skills required to carry out every stage of any remotely complex cyber-attack on their own.

This is where the Crime-as-a-Service (CaaS) business model that we have discussed extensively in previous reports comes into play. Instead of even attempting to learn everything, cybercriminals specialise in smaller, more manageable skill-sets. When they require something outside their own area of competency, they need only to find someone offering the appropriate tool or service in the digital underground; they can simply buy access to what they need. It is also on this basis of reciprocity and complementary skills that cybercriminals come together to commit crime in more coordinated groups, although other factors are also important here, such as language. Such associations are often transient however, only remaining together for the execution of a particular project, before disbanding. This makes

Operation Avalanche

EUROPOL

1st layer
Double fast flux

Potentially millions of infected devices

request to connect to a list of DNS addresses

List of DNS addresses
are hardcoded in the malware or created daily by a DGA

...
hellosd4f.com
hellog7hr.com
helloxyz1.com
....

Domain Generation Algorithm (DGA): Generating thousands of new domain names every day

DNS query for helloxyz1.com

DNS query to authoritative name server

Top-level domain (TLD) .com
if the domain is registered then refers to a authoritative Name Server (NS)

Domain (criminal) Name Server
checks the records and provides the IP address of the domain

Fast flux: the IP addresses change every five minutes (300s) - TTL (time to live)

.COM TLD Name Server
checks the records and responds back the IP address of the authoritative Name Server (NS) for the domain (It can be .com or any other TLD such as .info or .eu)

Fast flux: the name server record changes every five minutes (300s) - TTL (time to live)

provides multiple IP addresses

2nd layer
Proxy layer

Network of compromised computers
multiple individual computers are used to host the domain for a short period of time

redirect to a proxy

The proxies redirect the traffic and are used to disguise the originating source of these instructions.

Will normally point to an IP where bots go for registration, to receive instructions, or to activate attacks.

deliver money muling pages or deploys multiple malware

redirects to the criminal cluster infrastructure and splits per botnet

3rd layer
Backend infrastructure

Cluster infrastructure
The criminals controlling the cluster can now give instructions to and/or extract data from your computer

Money muling

Malware

Gozy malware

URLzone malware

Rovnix malware

TeslaCrypt malware

Administration infrastructure

Avalanche administrator

attribution based on associates and business partners more challenging compared to traditional organised crime groups.

Currently, the primary hub for this activity is online forums, primarily in the deep web, and to a lesser extent on the Darknet. Almost half of the Member States highlighted the key role these environments play in cybercrime. While such forums provide a crucial environment for access to cybercrime tools and services, it is not fully clear to which extent some of this activity may have shifted to more structured markets on the Darknet.

BULLETPROOF HOSTING

An important service provided on the digital underground is that of bulletproof hosting. This refers to hosting that not only allows illicit content, but is typically resistant to attempts by authorities to shut the service down, either due to its geographic location, or some methods of technical evasion, such as fast flux.[III] Bulletproof hosting services are known to host content related to all aspects of online criminality, from malware command and control servers to child abuse images.

In November 2016, an international criminal infrastructure platform known as 'Avalanche' was dismantled by the Public Prosecutor's Office Verden and the Lüneburg Police (Germany), in close cooperation with the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice and the FBI, Europol, Eurojust and global partners.

The Avalanche network was used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns, affecting victims in over 180 countries. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the high number of malware families managed through the platform.

The operation marked the largest-ever use of sinkholing to combat botnet infrastructures and was unprecedented in its scale, with over 800 000 domains seized, sinkholed or blocked.

ANONYMISATION TOOLS

Like anyone seeking additional privacy and/or anonymity while operating on the internet, cybercriminals also routinely use anonymisation tools and services as part of their OPSEC in order to, for example, hide their original IP address or encrypt their internet traffic. In order of increasing prevalence, as seen by law enforcement, cybercriminals make use of 'simple' proxies, VPNs, and Tor. While there are criminal vendors offering these services, allegedly offering greater security, the proxy and VPN services used are often freely available or commercial products. Tor is not just used as a proxy, but also to host websites anonymously. Such sites are commonly referred to as 'hidden services' and include the Darknet markets discussed elsewhere in this report.

COMMUNICATION TOOLS

Law enforcement is witnessing a transition into the use of secure apps and other services by criminals across all crime areas. The majority of the apps used are the everyday brand names popular with the general populace.[99] As these become increasingly secure, incorporating end-to-end encryption for example, they are readily adopted by criminals seeking reliable, secure communications. This creates additional challenges for law enforcement as it renders many traditional investigative techniques, such as wire-tapping, ineffective.

While everyday apps are commonly used, there are some channels which appear to remain peculiar to cybercrime. Internet Relay Chat (IRC) is one of the oldest tools for communication on the internet, allowing group discussions, private messaging, data transfer and file sharing. Despite dwindling usage globally, several countries encountered its use during their investigations. Other European law enforcement agencies report that Jabber continues to be used by cybercrime groups. Other reports highlight that Jabber remains a key communication tool for European cybercriminals.[100] Jabber also allows encrypted communications, with the added advantage of users being able to host their own private jabber servers.

CRIMINAL FINANCES

A significant proportion of cybercrime is carried out by financially motivated criminals. Those criminals, whether trading in criminal markets or extorting funds from their victims, need some currency or other financial instruments in order to carry out and profit from their activities. In 'real world' crime this would likely be cash in some local or globally accepted currency; but for cybercriminals, operating in a digital world, a digital solution is required.

CRIMINAL ABUSE OF CRYPTOCURRENCIES

For the past few years this has almost universally meant Bitcoin,

[III] A fast flux network is one where a domain name can have its IP address rapidly changed to another under the criminals' control.

the criminal abuse of which has grown in parallel with its general adoption and legitimate use. It is the most commonly used currency for criminal to criminal payments, for example when purchasing or renting cybercrime tools or services on the digital underground. It is the only currency accepted on most Darknet marketplaces and automated card shops, and is the currency required by almost all of today's ransomware and DDoS extortion demands.

While the abuse of Bitcoin remains a key enabler for criminal conduct on the internet, a number of other cryptocurrencies are beginning to emerge in the digital underground.

Monero - Launched in 2014, much of Monero's growing popularity relates to the additional security and privacy features it offers; transactions cannot be attributed to any particular user/address, all coins used in a transaction are 'hidden' by default, and transaction histories are kept private. Monero is now accepted on a number of Darknet markets, and 2017 saw the first ransomware, Kirk, which used Monero for ransom payments.[101]

Ethereum - We touched upon the possibility of Ethereum's 'smart contracts' becoming a tool for the Crime-as-a-Service business model in last year's report. While we have yet to see this, at least one Darknet market has begun accepting Ethereum for payments and purchases. Furthermore, as discussed earlier in this report, a team of developers plan to run a decentralised Darknet market on the Ethereum blockchain.[102]

Zcash - Zcash is another cryptocurrency that focuses on improved privacy for its users, obscuring both the transaction recipient and transaction amount. While Zcash has yet to feature in any reported law enforcement investigations, Zcash was due to be included in the currencies accepted by Darknet market AlphaBay.[103]

Other recent trends include the increasing number of offenders using Bitcoin ATMs, the numbers of which are steadily growing,[104] and the use of Bitcoin topped-up debit cards, which can be used for purchases as well as cash withdrawals at the majority of typical ATMs.

MONEY MULES

Many cyber-dependent and cyber–facilitated crimes at some point generate fiat currency with the regulated financial sector, whether it be from a victim's compromised bank account or a malware infected ATM. Accessing these funds often carries considerably greater risk than the steps taken to put them in the criminals' control in the first place. This is where the services of a third party come into play – money mules.

Money mules are either hired, or in some cases tricked, into accepting or collecting funds on behalf of criminals. For example, the mules may open new banks accounts or use existing ones to receive funds from accounts compromised by banking Trojans. The funds are then either transferred to other accounts, perhaps those that are in direct control of the criminals, or withdrawn and sent to the criminals via another method such as a money service bureau; all for a small percentage of the funds as payment.

Various scams are used to recruit unsuspecting money mules, most of who, at least initially, believe they have been recruited for gainful employment in a legitimate company.[105] Other mules are fully aware and complicit in their activities. Such mules can often be found on criminal forums, offering their services for their share of the profits. Professional money mules are often highly organised and operate in coordinated groups.

Those most targeted to become mules include those with little or no regular income such as students or the unemployed, and newcomers to a specific country. In some European countries there is considerable financial incentive to engage in this activity.

This activity is partly facilitated by the ease with which new accounts can be opened, especially in certain European countries, with many banks now allowing customers to open an account online, with no need to physically attend a branch or provide identity documentation.

In November 2016, Europol's EC3, the Joint Cybercrime Action Taskforce, Eurojust, and the European Banking Federation supported the second coordinated European Money Mule Action, culminating in the arrest of 178 individuals. Law enforcement agencies and judicial authorities from 18 countries participated in the international operation which identified 580 money mules across Europe. 380 suspects were interviewed in the course of the action week. The suspects were collectively tied to criminal activity which has resulted in EUR 23 million in losses. 95% of this activity was directly linked to some form of cybercrime. The successful hit on this wide-spread crime was supported by 106 banks and private-sector partners.

FUTURE THREATS AND DEVELOPMENTS

Cash continues to play an important role when it comes to criminals realising their criminal gains; it has well-established methodologies for laundering, and is as readily exchangeable, relatively untraceable, and pseudo-anonymous – similar to the cryptocurrencies favoured in the digital underground. As a result, virtual currencies have yet to be adopted to any large degree by established money launderers who are likely to favour long established methodologies.

Cryptocurrencies will continue to gain traction however, both online and offline, with several newer currencies already establishing themselves on the criminal markets. Some European law

enforcement already report that even street level drug dealers are converting to crypto-currencies. Whether any will grow to challenge the role of Bitcoin in terms of criminal use will remain to be seen, but the likes of Monero or Zcash certainly appear to have more to offer criminals wishing to operate with greater anonymity. How much the criminal use of a currency drives the market however is unclear.

While knowledge and experience of how to investigate, trace and seize virtual currencies continues to grow in the law enforcement community, enhanced by various private sector tools for attribution, this is often limited to Bitcoin, and not the other cryptocurrencies emerging in the criminal markets. Successful law enforcement activity related to Bitcoin-using cybercriminals may push users further towards alternative cryptocurrencies.

COMMON CHALLENGES FOR LAW ENFORCEMENT[106]

In this section we will summarise the various factors which influence the effectiveness of law enforcement and prosecutors to combat cybercrime. Many of these factors, while particularly pertinent to cybercrime, impact on almost all types of investigation: counter terrorism, cybercrime, drug trafficking, online child sexual exploitation, facilitated illegal immigration, homicide and fraud.

LOSS OF DATA

Data Retention. Electronic communication data is essential to the successful investigation and prosecution of serious crimes (including cybercrime). The overturning of the Data Retention Directive (DRD) by the Court of Justice of the European Union (CJEU) in its ruling of 8 April 2014[107] has had significant impact on law enforcement's ability to obtain such data, which has in turn had a negative impact on subsequent investigations, leading to a loss of both investigative leads and the ability to effectively prosecute online criminal activity.

While some Member States have retained some national legislation to ensure that internet service providers (ISPs) retain data for law enforcement purposes, other Member States have not. Since the Court's 2014 ruling, the lack of unified retention of electronic communication data across the EU has proven a key challenge to investigating cross-border cybercrime.

Carrier Grade Network Address Translation. The widespread implementation of Carrier Grade NAT[IV] (CGN) technologies by internet access providers (IAPs) adds an additional element of data loss to law enforcement investigations. With CGN, IAPs and electronic content providers may not log certain types of information (like source port numbers and destination IP addresses) that are essential in attributing criminal activity to a specific end-user. Without that information, one enquiry may result in a list of hundreds or even thousands of end-users associated with a particular public IP address. The impracticality of this may even lead authorities to drop a case.

A recent study showed that in 2016, 90% of mobile internet network operators (GSM, 2G, 3G, 4G providers) and 38% of fixed line internet access providers (cable, fibre and ADSL) are using CGN technologies, while 12% are planning to deploy

[IV] CGN is a technology that allows a single IP address to be shared by potentially thousands of subscribers/end-users on the same network simultaneously.

them in the near future.[108]

Encryption. While the growing use of encryption is a boon to cybersecurity in general, its increasing use by the criminal community renders many traditional investigative techniques ineffective, and often negates the possibilities of digital forensic analysis. In an assessment performed by the Council of the EU under the Slovak Presidency,[109] 20 Member States responded that encryption is encountered often or almost always in the context of criminal investigations. This was also reflected in the contribution to this year's IOCTA report, where law enforcement highlights the difficulties posed by the criminal use of VPNs, anonymising networks such as Tor, encrypted communication apps and software, and the use of encryption to effectively and indefinitely hide critical evidence. Law enforcement also unanimously emphasises that this trend is increasing. This is applicable across all aspects of cybercrime, and is an established trend in both cyber-dependent crime, terrorists and among child sex offenders.

This issue is compounded by the growing number of electronic service providers who implement encryption of their services by default.

Virtual currencies. In many aspects, the criminal use of virtual currencies does for the financial trail what encryption does for the evidential trail of communications data. They hamper law enforcement's ability to 'follow the money' through the use of obfuscated blockchains or mixing services, and significantly complicate the process of asset seizing and recovery.

LOSS OF LOCATION

A combination of the factors described above has led to a situation where frequently law enforcement may no longer (reasonably) establish the physical location of the perpetrator, the criminal infrastructure or electronic evidence central to a particular investigation. Moreover, as any one case may have perpetrators, victims, data and infrastructure in multiple locations, it can often be unclear which country has jurisdiction and what legal framework regulates the collection of evidence or the use of special investigative powers. It may also result in competing claims to prosecution.

LEGAL FRAMEWORK

Differences in domestic legal frameworks in the Member States (MS) and international instruments often prove to be a serious impediment to the international criminal investigation and prosecution of cybercrime. This is partly due to an incomplete transposition of international instruments into domestic legislation. The main differences relate to the provisions to investigate cybercrime and gather e-evidence, and to the criminalisation of conduct, where some activities are criminal in some jurisdictions and not in others, leading to 'safe havens' for certain types of criminality.

A key issue in relation to cybercrime issues in particular is the lack of case law, which can be a valuable tool to compensate for a lack of specific legislation; unfortunately little case law exists with regard to the new technological developments at the heart of cybercrime activity.

PUBLIC-PRIVATE PARTNERSHIPS

In every IOCTA report we highlight how essential close cooperation with the private sector is in combating cybercrime. Not only does the private sector retain much of the evidence of cybercrimes, but they are a key player in joint efforts to takedown criminal infrastructure and remove illicit content. Public-private partnerships are also key in enabling a more pro-active and agile approach to combatting cybercrime. There is however little consensus on the legal framework that is required to facilitate effective and trust-based cooperation with the private sector, while at the same time regulating legal and transparency issues surrounding that cooperation. Furthermore, data protection regulations and fear of liability may pose serious obstacles to cooperation with private industry.

INTERNATIONAL COOPERATION

In previous years' reports we have highlighted the scope and scale of international cybercrime investigations and the frequency with which it requires some form of mutual legal assistance for the purpose of gathering evidence from foreign jurisdictions. The collection of electronic evidence is often a time-sensitive issue, particularly when considering the current situation with regards to data retention. However, the current process of mutual legal assistance (MLA) has long been per-

ceived by practitioners as being too slow and cumbersome to gather and share evidence effectively due to the differences in legal systems and frameworks. There is a clear need for a better mechanism for cross-border communication and the exchange of information for the purpose of investigation, prevention and protection. The implementation of the European Investigation Order (EIO) Directive may go some way in addressing these issues for the majority of MS.

THE EVOLVING THREAT LANDSCAPE AND THE EXPERTISE GAP

Cybercrime continually evolves, creating a constant challenge for both law enforcement and prosecutors in terms of acquiring and maintaining the expertise required to successfully investigate and prosecute. Such expertise is also required in the courts.

The European Cybercrime Training and Education Group (ECTEG), the Training of Trainers (TOT) project, and various activities under the umbrella of the EU Policy Cycle framework are already making some headway into addressing the expertise gap at EU level. However, no EU-wide standards for training and certification exist yet, and the alignment of existing programmes within the Member States and broader implementation of the current EU-wide initiatives is necessary.

RECOMMENDATIONS

Innovation, in terms of the pro-active and adaptive approaches and counter strategies employed, and collaboration, in terms of the involvement of all relevant partners, should be at the core of any response to tackling cybercrime.

There is a need to continue to develop coordinated action at EU level and beyond to respond to cybercrime at scale, building on and learning from successful operations.

Law enforcement must continue to develop, share and propagate knowledge on how to recognise, track, trace, seize and store cryptocurrencies. Existing training on investigating cryptocurrencies should be shared and promoted within the law enforcement community.

Law enforcement should engage early with the private sector, academia and developers to seek solutions to investigating those emerging cryptocurrencies which boast additional security measures designed to hamper lawful investigation.

Private sector partners and law enforcement should continue cooperating to target mule networks which are an essential element of the criminal ecosystem, following successful models such as the European Money Mule Actions (EMMA).

Where not already present, Member States should consider implementing more efficient fraud reporting mechanisms. Online reporting channels are particularly suitable for such high volume crimes, and allow victims to report the crime without the need to contact local police.

While the implementation of the European Investigation Order (EIO) is expected to simplify cooperation between judicial authorities and expediting investigations, existing legal frameworks and operational processes need to be further harmonised and streamlined for dealing with cross-border e-evidence. Such measures, as well as the parallel EU policy processes on encryption, data retention and internet governance challenges, should thoroughly consider the specific law enforcement needs and strive for practical and proportionate solutions to empower innovative, efficient and effective approaches to conducting lawful cybercrime investigations.

The growing prevalence and sophistication of cybercrime requires dedicated legislation that more specifically enables law enforcement presence and action in an online environment.

Member States should continue to support and expand their engagement with Europol in the development of pan-European awareness and prevention campaigns with a view to increasing baseline cybersecurity protection and further improving digital hygiene. This includes security-by-design and privacy-by-design principles such as the use of encryption to safeguard sensitive data.

There is a need for standardised rules of engagement with private industry and need to surround this form of cooperation with a solid and uniform legislative framework. This includes a clear understanding of the extent to which private parties can obtain evidence themselves and the legal implications of their actions.

CGN technology has created a serious online capability gap in law enforcement efforts to investigate and attribute crime. This needs to be addressed through dialogue with content service providers and internet access providers to collectively examine ways of limiting the impact of CGN technologies on criminal investigations, such as source port number logging or limiting either the use of CGN or the number of subscribers behind each IPv4 address.[110]

As human beings are the direct targets of social engineering, the investment in combating it must also be in the employees and members of the public that are likely to be potential victims. Training and education are crucial to allow prospective victims to identify and respond accordingly to social engineering attacks. Cases show significant improvement where specific and effective training is given.

THE GEOGRAPHIC DISTRIBUTION OF CYBERCRIME

The following is a brief summary of geographic threats and cybercrime activity throughout 2016 based on law enforcement and industry data. The overview makes use of the United Nations geoscheme[111] to group countries and regions.

For this year's IOCTA, contributors were requested to highlight which countries presented a particular threat in terms of the criminal activity described in this report. While the comments below summarising these contributions are not assessed to represent a complete intelligence picture, they are judged to be indicative of some general trends in activity relative to those countries and regions. This data does not include self-reporting.

AFRICA

In previous years' reports we have highlighted the rapidly growing internet infrastructure on the African continent. While this may be true, compared to 2016 there has been little growth in internet penetration, which has actually dropped marginally. Almost one third of African countries have less than 10% internet penetration, although Africa still hosts almost 10% of the world's internet users.[112]

Almost half of the EU Member States highlighted Africa as the source of specific cyber threats. The most commonly reported threats were social engineering attacks and cyber-facilitated frauds. This largely referred to romance scams and phishing, but also IT support scams, CEO fraud and the sexual extortion of minors. Several countries also reported Africa as the source of various attacks on their critical infrastructure. Lastly, CNP fraud using compromised EU cards was also reported by several Member States.

African nations did not feature prominently in industry reporting in 2016.

THE AMERICAS

Despite having an internet penetration of over 88%, North America hosts a smaller percentage of the world's internet users than Africa, only 8.6%. Nevertheless, North America is a key target for financially motivated cybercrime. 37% of the world's business email compromise frauds target that region.[113] North America also tops the list for the largest number of data breaches (49% of global data breaches), the number of records stolen and the average cost per breach.[114,115,116] The US is the top target for ransomware according to some industry reports that indicate 34% of all ransomware detections are in the US.[117] The US is also a top target for banking malware.[118]

In addition to financial crime, one of the regions identified as a primary origin of children featuring in child abuse imagery is also North America.[119] This was mirrored in the threats highlighted by Member States.

North America hosts a significant proportion of the world's webservers. Consequently it also hosts almost 50% of the world's phishing sites,[120] and 39% of global botnet control servers.[121]

South America typically features less in both law enforcement and industry reporting. Some industry reports highlight South America as a source of ATM malware.[122] As in previous reports, it also hosts a significant proportion of global phishing sites.[123]

EU law enforcement highlighted the role of the Americas, both North and South, in card-present (CP) fraud, highlighting once again how the US is still a key destination for the cashing out of comprised EU cards. Card-not-present (CNP) fraud was also reported, but to a lesser degree.

ASIA

Asia not only houses over 55% of the world's population but over 50% of global internet users. Despite this, it is the focus for a disproportionately small percentage of cyber threats. Out of all the continents commented on by EU law enforcement, Asia featured the least. What comments were made related to a wide variety of crime types, although CP fraud accounted for the highest percentage. Industry does report that Japan, South Korea and China are all top 10 countries for hosting botnet control servers, hosting 11% of global servers between them.[124] Furthermore, China, and to a lesser degree North Korea, are allegedly home to a number of APT attack groups.[125]

Countries in Asia do however feature heavily as victims of cybercrime. It features in several industry reports as a hotspot for mobile malware infections.[126] As an example, some reports indicate that in Bangladesh, over 50% of mobile users are attacked by mobile malware, with several other Asian countries severely affected.[127] Many Asian countries, including India, Taiwan, Malaysia, South Korea and Pakistan also feature in some reporting as the countries with the highest rates of attacked computers.[128] This is possible due to the high incidence of pirated software in use in these countries which remains unpatched and therefore vulnerable.[129]

Some Asian countries are also notable targets for business email compromise (BEC) frauds, including Japan, Hong Kong and India.[130]

EUROPE

It is perhaps unsurprising that majority of threats affecting the EU were identified by EU law enforcement as coming from within Europe, in fact more than all the regions outside Europe combined. This is perhaps a reflection however of the greater levels of cooperation and information exchange between European law enforcement, which put emphasis on cases involving European partners. Of these threats, social engineering (CEO Fraud), CNP fraud, internet-facilitated sexual offences against children, malware, and attacks on critical infrastructure were highlighted.

Much of this is supported by industry reporting. Eastern Europe is reported as a key source of ATM malware.[131] Russia is also reportedly home to a number of APT attack groups.[132]

Europe is also a key target for financially motivated cyber-attacks and frauds. Second only to the US, the UK reports the highest number of BEC frauds (over 9.5%). France and Norway also see a notable proportion of these attacks, each suffering over 2% of global attacks.[133] Germany, Italy, the Netherlands, and the UK also account for a small but notable proportion of global ransomware detections (16% combined),[134] and Germany and Russia are identified as key targets for banking malware.[135] The UK suffers the second most data breaches globally, albeit a distant second place from the US. Germany and Ireland also feature in a global top 10 list.[136]

Despite this, Europe still has some of the lowest rates of attacked computers globally.[137]

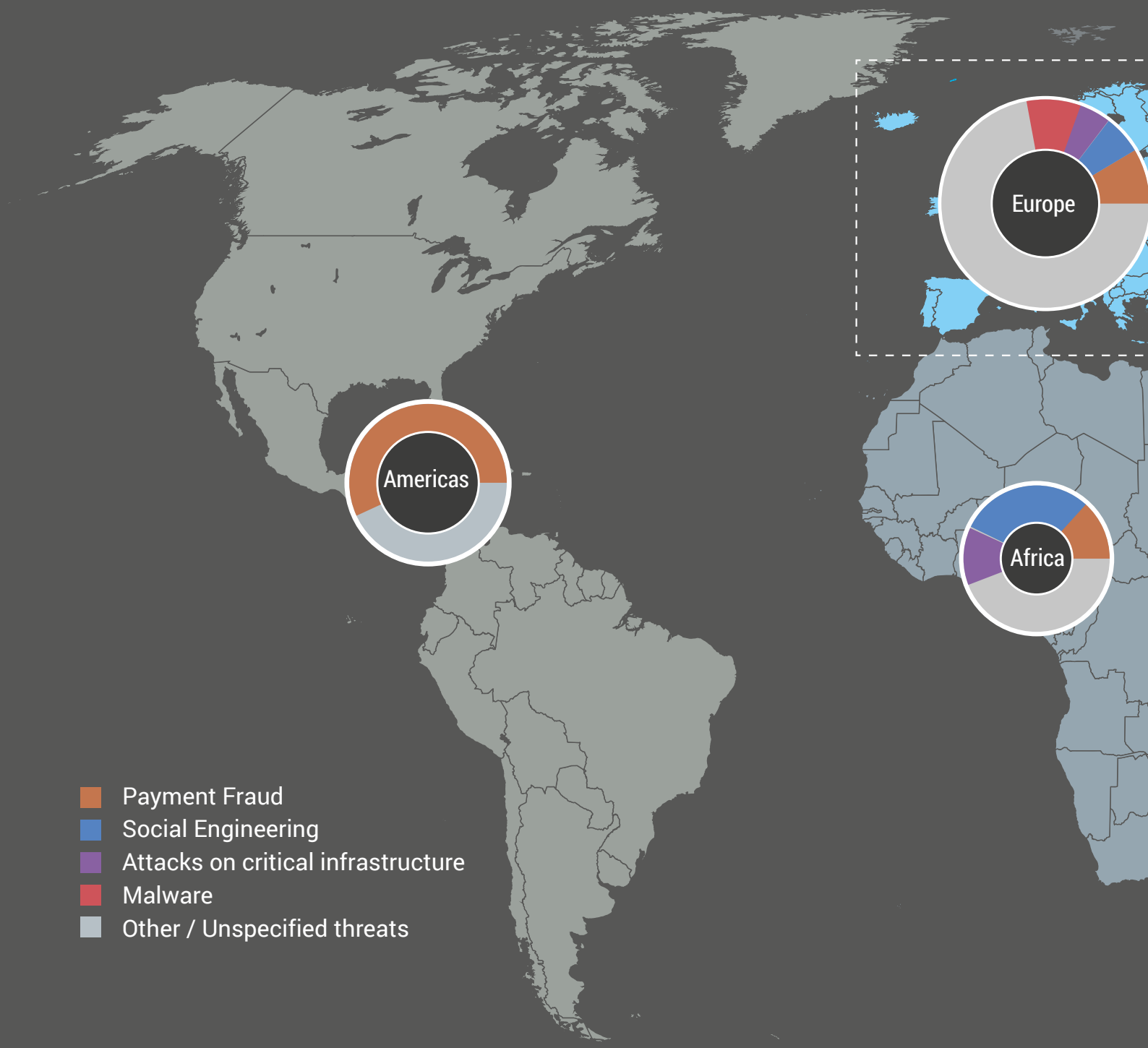
Several trends continue from previous years. Fast, reliable internet infrastructure continues to attract cybercriminals, resulting in Europe hosting some of the top locations for Botnet control servers, namely the Netherlands with 24% of global servers, Germany with 10%, and Russia and the UK with 3% each.[138]

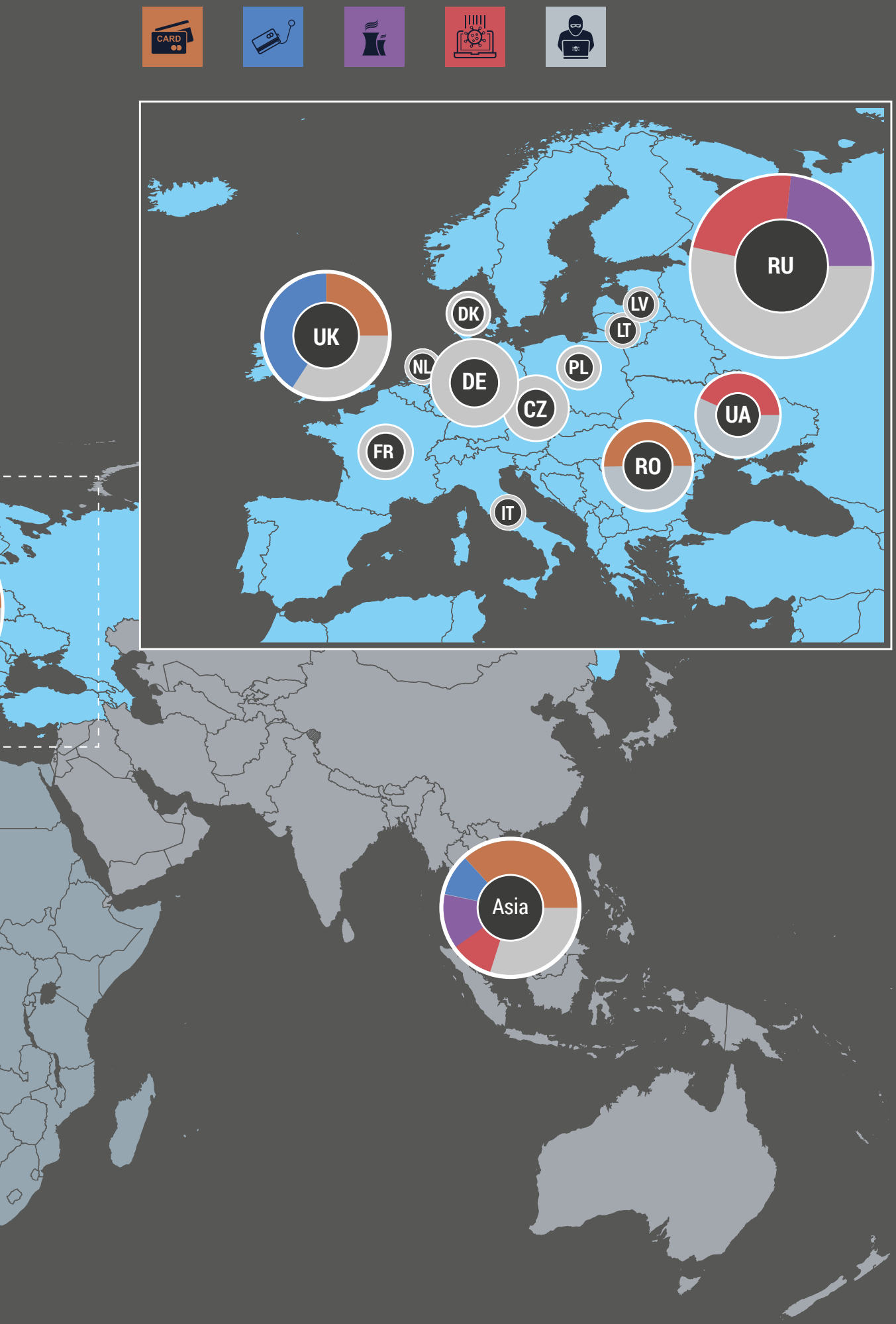
OCEANIA

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 Australian law enforcement remain data stealing malware, ransomware, and social engineering related frauds, including BEC. BEC frauds, which appear to target English speaking countries more prevalently, also affect Oceania (typically Australia), which accounts for almost 2% of global attacks.[139]

THE CYBERCRIME THREAT MAP

The following map highlights the key cybercrime threats emanating from each country or region, as identified by European law enforcement.




CARD
RU
UK
DK
LV
LT
NL
DE
PL
CZ
UA
FR
RO
IT
Asia

APPENDIX

CYBER ATTACKS IN THE CONTEXT OF/ AGAINST ELECTIONS

By Marco Gercke, Director Cybercrime Research Institute, Germany

Cyber-attacks in the context of elections, or more precisely cyber-attacks targeting elections, are no new phenomenon. Reported attacks go back more than a decade. In 2007 the website of the Kyrgyz Central Election Commission was reportedly attacked and defaced. But the topic got more attention in 2016 during and in the aftermath of the US presidential election. The following chapter provides an overview of the main focus areas of the offenders and related challenges for investigators.

1 RANGE OF ATTACKS

The ongoing digitalisation has opened new doors for attacks. Similar to 'online auction fraud' or 'payment fraud' there is not just one type of attack covered under the umbrella of 'attacks in the context of elections'. The following chapter provides an overview of the main types of attacks currently witnessed.

1.1 DEFACEMENT

Defacement describes the illegal modification of online content. The above mentioned reported attack against the Kyrgyz Central Election Commission is an example of such an attack. Defacement is a type of attack often carried out as part of a politically motivated attack to spread propaganda. Taking into account that election commissions, as well as political parties and interest groups, use online channels to communicate with the public, this underlines the potential for future attacks. Furthermore, successful attacks against the US Central Commands Twitter and Facebook accounts in 2015 highlight that even organisations with strict security procedures face challenges in protecting online services.

1.2 DENIAL-OF-SERVICE ATTACKS

In some ways comparable to the defacement of websites are Denial-of-Service (DoS) attacks that are aiming to make websites or services unavailable. Typical targets within the context of elections are websites of election commissions, political parties and candidates. In 2011 websites from the National Election Commission of South Korea and one candidate for the October 2011 by-election were targeted. Taking into account that in the last few years communication through social media services such as Twitter and Facebook have become more dominant, it is uncertain if DDoS attacks against websites will play a major role in future attacks as popular social media websites tend to have more sophisticated technical protection measures in place.

1.3 ESPIONAGE/DATA EXFILTRATION

Two of the most widely publically discussed attacks within the US presidential election 2016 were related to the alleged exfiltration of data. It was reported that offenders were able to obtain data (e-mails) both from computer systems of the Democratic Nation Convention, the governing body of the United States Democratic Party, as well as e-mails of the Campaign Chairman of Hillary Clinton's Campaign. A similar attack took place in the 2017 French national election when offenders were able to obtain e-mails from Emmanuel Macron's campaign. Despite various security risks related to e-mail communication (especially unencrypted), this method of communication remains popular even for confidential information.

1.4 PUBLICATION OF OBTAINED INFORMATION

Both in the reported attacks in the 2016 US presidential election and in the 2017 French election, the mere fact that offenders obtained access to e-mails was not seen as the greatest damage – it was the fact that those e-mails were published. In the case of the 2017 French election, e-mails were published only hours before the voters went to the polls. In the 2016 US presidential election obtained emails were published over several months – mainly through WikiLeaks. While it is uncertain to what extent the publication of those internal e-mails had an impact on the election polls in the context of the US election, the constant publication of e-mails and subsequent coverage in the press did influence the topics of the debate.

1.5 ATTACKS AGAINST VOTER REGISTRATION

In some countries voters need to actively register to be able to cast a vote. Both within the context of the 2016 US presidential election, as well as in the context of the British EU Referendum 2016, reports about attacks against voter registration were published. With regard to the 2016 US presidential election the reported number of states affected by such attacks vary between 21 and 39. Attacks reportedly included attempted manipulations as well as illegally obtaining voter information from voter databases. While it is in general easy to imagine the potential impact of such attacks (ranging from obtaining the list to influence voters, to removing voters from the list or even manipulating entries in a way that will make it impossible to run an election) it is currently uncertain what precisely the offenders were able to achieve through these attacks.

1.6 ATTACKS AGAINST VOTING MACHINES

Potential attacks against machines casting votes with the intention to interfere with an election have been discussed for decades. In 1898 the Californian 'Commission for Examining Voting' machines expressed concerns related to the 'danger of manipulation of the machinery'. The bandwidth for attacks increases when electronic systems are utilised to cast the vote. Within the context of the 2016 US election there were reports about attacks against suppliers of voting machines/software. And after the election some scientists believed that they saw indications of a potential computer attack that enabled offenders to manipulate the election results in three states. However, the completed recounts did not produce any evidence that a manipulation took place. But the theoretical risk that voting computers could be manipulated remains present and, consequently, various countries decided not to use voting computers and online voting but continue to cast votes on ballots.

1.7 MISLEADING INFORMATION

Both the Clinton and Macron campaigns, whose computer systems were reported to have been hacked and internal e-mails published, have indicated that some published e-mails were manipulated to mislead the public. Mixing authentic and manipulated documents could be a strategy to maximise the negative impact of such an attack. This was not the only incident where 'misleading' or 'fake' news played a role. One key component of possible interference in the US election could be the intentional spreading of false information. Some reports indicate that during the campaign botnets, fictitious news websites, social media accounts of non-existing persons, and so-called trolls were used to spread inaccurate news that was designed to look authentic and harm one candidate. While research that looks into the potential impact of the spreading of false information is still ongoing, it is certainly an area with increasing potential for attacks.

2 RELEVANCE FOR LAW ENFORCEMENT – PART 1: CRIMINALISATION OF ATTACKS

A frequently asked question from law enforcement agencies in Europe is related to their responsibility in case of such attacks. A responsibility requires that the underlying acts are criminalised. Almost all attacks described above are covered by European harmonisation approaches in the field of cybercrime legislation. Member States should have therefore implemented such legislation in their national legislation. However, it is important to point out that the harmonisation instruments pointed out below do not specifically refer to attacks against elections but computer systems in general.

2.1 DEFACEMENT

The defacement of websites was not included as a separate provision in the 2013 EU Directive on Attacks against Information Systems. However, a defacement usually consists of two steps: circumventing the protection of the server system and subsequently modifying the data (website). Unauthorised access to a computer system is covered by Art. 3 of the Directive and the illegal interference with stored computer data is covered by Art. 5.

2.2 DENIAL-OF-SERVICE ATTACKS

Denial-of-Service attacks are not only taking place with regard to elections but are a common problem. The 2013 EU Directive on Attacks against Information Systems addresses the issue in Art. 4 that calls upon Member States to criminalise the illegal interference with computer systems.

2.3 ESPIONAGE/DATA EXFILTRATION

One of the attack vectors that is not directly addressed by the 2013 EU Directive on Attacks against Information Systems is illegal data acquisition. This gap, that most likely unintentionally already occurred when the Council of Europe Convention on Cybercrime was drafted, that in part served as model for the 2005 EU Framework Decision on Attacks on Information Systems and subsequently the 2013 EU Directive on Attacks against Information Systems, is certainly significant. Attempted justifications that the Directive refers to 'information systems' and not 'data' fail as the Directive addresses interference (Art. 5) with and interception (Art. 6) of computer data. However, usually a data exfiltration requires that offenders first gain access to the computer system where this data is stored. If this takes place illegally, Art. 3 is applicable. However, the gap in legislation leads to challenges for law enforcement agencies when insiders are involved.

2.4 PUBLICATION OF OBTAINED INFORMATION

The publication of illegally obtained information is not addressed by the 2013 EU Directive on Attacks against Information Systems. Some Member States, such as Germany, have gone beyond the Directive and criminalised interactions with such illegally obtained data.

2.5 ATTACKS AGAINST VOTER REGISTRATION

The illegal interference with voter registration registers – from modifications to deletion of electronic databases – is covered by Art. 5 of the 2013 EU Directive on Attacks against Information Systems that requires Member States to criminalise the unauthorised interference with computer data. In this regard it is important to highlight that voting registration systems could be categorised as critical infrastructure. Art. 9, paragraph 4 c) of the 2013 EU Directive on Attacks against Information Systems addresses attacks against critical infrastructure.

2.6 ATTACKS AGAINST VOTING MACHINES

The range of possible attacks against voting machines is broad and potentially touches upon different provisions of the 2013 EU Directive on Attacks against Information Systems. If offenders illegally access voting computer systems, servers controlling such systems or servers used to collect data from the machines, Art. 3 is applicable. If casted votes are manipulated this potentially triggers provisions of the national legislation that implemented Art. 5. If as a consequence of the attack voting machines are seriously hindered or interrupted, Art. 4 is applicable. With regard to the fact that voting machines could be considered as critical infrastructure, Art. 9 is of relevance here as well.

2.7 MISLEADING INFORMATION

Publishing misleading information is in general not covered by the 2013 EU Directive on Attacks against Information Systems. In some cases (especially when it comes to the modification of the content of leaked e-mails) Art. 9, paragraph 5 could be applicable. However, it is important to recognise that this issue was not in the focus of the drafters of the Directive. And most likely the debate about a potential criminalisation of such activities will be controversial and any approach will face significant challenges. Background is the fact, that the published examples of spreading misleading information revealed a strategy of the authors to combine authentic information with misleading information. This combination (especially in the context of a political campaign) will in some countries most likely be covered by legislation protecting freedom of expression.

2.8 RELEVANCE FOR LAW ENFORCEMENT – PART 2: CHALLENGES RELATED TO CRIMINAL INESTIGATION

The main challenge for law enforcement agencies involved in the investigation of such attacks from a criminal law investigation perspective will most likely not be the degree of criminalisation or potential gaps in criminalisation. Most likely the key challenges will be attribution — or the degree of certainty required to identify the offenders and determine their motivation, potential state involvement and motivation. These challenges are likely to provide obstacles for the involvement of law enforcement agencies in dealing with the consequences of attacks against elections.


PgUp

REFERENCES

1 https://www.nomoreransom.org/

2 Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Article 15.3.

3 Levi et al., 2016, 'Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research', Crime, Law and Social Change, 67 (1): 77-96. DOI: 10.1007/s10611-016-9648-0

4 https://securelist.com/dridex-a-history-of-evolution/78531/

5 Checkpoint Technologies/Europol, 2017, Banking Trojans: From Stone Age to Space Era, p7

6 https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation

7 Trend Micro, 2017, TrendLabs 2016 Security Roundup, p22

8 Checkpoint Technologies/Europol, 2017, Banking Trojans: From Stone Age to Space Era, p6

9 Symantec, 2017, Internet Security Threat Report: Volume 22, p42

10 Checkpoint Technologies/Europol, 2017, Banking Trojans: From Stone Age to Space Era, p5,6

11 Trend Micro, 2017, TrendLabs 2016 Security Roundup, p4

12 https://themerkle.com/bitcoin-ransomware-education-satan/

13 Symantec, Internet Security Threat Report, 2017, p61

14 http://blog.trendmicro.com/trendlabs-security-intelligence/torrentlocker-changes-attack-method-targets-leading-european-countries

15 https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/

16 https://www.nomoreransom.org/

17 https://www.europol.europa.eu/newsroom/news/over-28-000-devices-decrypted-and-100-global-partners-—-no-more-ransom-celebrates-its-first-year

18 https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/mobile-malware

19 Kaspersky Lab, 2017, Mobile Malware Evolution 2016, p12

20 Checkpoint Technologies / Europol, 2017, Banking Trojans: From Stone Age to Space Era, p10

21 http://blog.checkpoint.com/2016/06/23/the-infamous-nuclear-exploit-kit-shuts-down/

22 http://blog.talosintelligence.com/2016/09/shadowgate-takedown.html

23 https://blogs.rsa.com/shadowfall/

25 https://www.europol.europa.eu/newsroom/news/cybercrime-ring-dismantled-europol%E2%80%99s-support

26 https://www.europol.europa.eu/newsroom/news/international-operation-targets-customers-of-counter-anti-virus-and-crypter-services-6-arrested-and-36-interviewed

27 Check Point Software Technologies, http://www.checkpoint.com

28 Trend Micro

29 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

30 https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

31 http://www.reuters.com/article/us-deutsche-telekom-outages-idUSKBN13O0X4

32 ENISA, 2017, Annual Incident Reports 2016: Analysis of Article 13a annual incident reports in the telecom sector, p15.

33 ENISA, 2017, Annual Incident Reports 2016: Analysis of Article 13a annual incident reports in the telecom sector, p28.

34 https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/

35 Kaspersky Lab, 2017, Threat Landscape for Industrial Automation Systems in the Second Half of 2016, p10.

36 https://securelist.com/analysis/publications/77784/the-cost-of-launching-a-DDoS-attack/

37 http://www.dupre.co.uk/hosted-voip-telephone-systems/isdn-and-pstn-services-to-end-by-2025/

38 FraudFit, 2016, Preventing PBX Fraud, p5

39 Verizon, 2017, 2017 Data Breach Investigation Report: 10th Edition, p3

40 http://securityaffairs.co/wordpress/59671/hacking/unsecure-hadoop-distributed-file-system.html

41 Source: http://www.breachlevelindex.com

42 http://www.breachlevelindex.com/#!breach-database

43 https://www.tripwire.com/state-of-security/featured/adultfriendfinder-data-breach-what-you-need-to-know/

44 https://www.wired.com/2017/05/us-sanctions-didnt-stop-russias-election-hacking-even-slow/

45 https://www.bloomberg.com/news/articles/2017-05-09/cyber-crime-fears-drive-growing-demand-for-anti-hacker-insurance

46 https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Spora.A

47 Checkpoint Technologies / Europol, 2017, Banking Trojans: From Stone Age to Space Era, p9

48 McAfee Labs, 2015, Threats Report November 2015, pp9-11

49 Trend Micro

50 https://steemit.com/shadowbrokers/@theshadowbrokers/oh-lordy-comey-wanna-cry-edition

[51] https://www.nomoreransom.org/

[52] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose

[53] The Brookings Institution, 2016, Sextortion: Cybersecurity, teenagers, and remote sexual assault, p12

[54] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

[55] NetClean, 2016, The NetClean Report 2016: 10 important insights into child sexual abuse crime, p14

[56] https://www.europol.europa.eu/partners-agreements/police2peer

[57] NetClean, 2016, The NetClean Report 2016: 10 important insights into child sexual abuse crime, p16

[58] https://www.europol.europa.eu/newsroom/news/global-action-tackles-distribution-of-child-sexual-exploitation-images-whatsapp-39-arrested-so-far

[59] http://www.wired.co.uk/article/freedom-hosting-ii-hack-dark-web-offline

[60] NetClean, 2016, The NetClean Report 2016: 10 important insights into child sexual abuse crime, p14

[61] Internet Watch Foundation, 2012, Study of Self-Generated Sexually Explicit Images & Videos Featuring Young People Online, p5

[62] NetClean, 2016, The NetClean Report 2016: 10 important insights into child sexual abuse crime, p12

[63] https://www.europol.europa.eu/newsroom/news/victims-of-child-sexual-abuse-centre-of-europol-efforts

[63] https://www.europol.europa.eu/stopchildabuse

[64] https://www.europol.europa.eu/stopchildabuse

[65] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Article 15.3

[66] https://www.europol.europa.eu/newsroom/news/credit-card-fraud-in-130-000-cases-organised-crime-group-disrupted-in-european-cross-border-action

[67] European Central bank, 2015, Fourth Card Report, p2, p18

[68] European Central bank, 2015, Fourth Card Report, p18

[69] European Association for Secure Transactions (EAST)

[70] Trustwave, 2017, Global Security Report

[71] https://www.s21sec.com/en/blog/2017/01/alice-simplicity-for-atm-jackpotting/

[72] European Association for Secure Transactions (EAST)

[73] https://www.europol.europa.eu/newsroom/news/27-arrested-in-successful-hit-against-atm-black-box-attacks

[74] http://securityaffairs.co/wordpress/53758/cyber-crime/jackpotting-attacks.html

[75] https://www.visaeurope.com/newsroom/news/european_used_contactless_3_billion_times_last_year

[76] The UK Cards Association, 2017, Card Expenditure Statistics, p2

[77] The UK Cards Association, 2017, Debit Card Report: March 2017, p1

[78] https://ec.europa.eu/home-affairs/what-is-new/work-in-progress/initiatives/ezmmp_intro_en

[79] https://metrics.torproject.org

[80] D. Moore and T. Rid 2015, Cryptopolitik and the Darknet, p. 21

[81] RAND Europe 2016, Internet-facilitated drugs trade – An analysis of the size, scope and the role of the Netherlands, p27

[82] OECD/EUIPO, 2016, Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, p5

[83] https://blog.kaspersky.com/billion-dollar-apt-carbanak/7519/

[84] Group IB, 2016, Cobalt: Logical Attacks on ATMs, p5

[85] http://www.wired.co.uk/article/dnc-hack-proof-russia-democrats

[86] APWG, 2017, Global Phishing Survey: Trends and Domain Name Use in 2016, p9

[87] APWG, 2017, Global Phishing Survey: Trends and Domain Name Use in 2016, p5

[88] Verizon, 2017, Data Breach Digest, p13

[89] APWG, Phishing Activity Trends Report: 4th Quarter 2016, p5

[90] https://www.europol.europa.eu/newsroom/news/organised-crime-group-involved-in-phishing-dismantled

[91] Trend Micro

[92] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise

[93] Symantec, 2017, Internet Security Threat Report: Volume 22, p26

[94] Trend Micro, 2017, Trend Labs 2016 Security Roundup: A Record Year for Enterprise Threats, p8

[95] https://www.leoni.com/en/press/releases/details/leoni-targeted-by-criminals/

[96] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise

[97] http://www.darkreading.com/threat-intelligence/nigerian-cybercrime-matures-morphs/d/d-id/1328392?_mc=sm_dr&hootPostID=bd29eb877f75104659619ef-9ca29c24f

[98] Trend Micro

[99] Flashpoint, 2017, Cybercrime Economy, An analysis of criminal communications strategies, pp3-17

[100] Flashpoint, 2017, Cybercrime Economy, An analysis of criminal communications strategies, p10

[101] https://www.bleepingcomputer.com/news/security/star-trek-themed-kirk-ransomware-brings-us-monero-and-a-spock-decryptor/

[102] https://www.deepdotweb.com/2017/07/08/behind-scenes-darknet-market-ethereum-blockchain/

[103] https://www.deepdotweb.com/2017/06/11/alpha-bay-support-yet-another-payment-method-zcash/

[104] https://coinatmradar.com/

[105] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling

[106] Eurojust/Europol, 2017, Common challenges in combating cybercrime

[107] ECLI:EU:C:2014:238 (case C-293/12)

[108] Richter et al., 2016, A Multi-perspective Analysis of Carrier-Grade NAT Deployment, ISBN 978-1-4503-4526-2/16/11

[109] 13434/16

[110] Eurojust/Europol, 2017, Common challenges in combating cybercrime

[111] http://unstats.un.org/unsd/methods/m49/m49regin.htm

[112] http://www.internetworldstats.com/stats1.htm

[113] Trend Micro, 2017, TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats, p8

[114] Ponemon Institute, 2017, 2017 Cost of Data Breach Study, p5

[115] Trustwave, 2017, Global Security Report

[116] Symantec, 2017, Internet Security Threat Report: Volume 22, p50

[117] Symantec, 2017, Internet Security Threat Report: Volume 22, p57

[118] Kaspersky Lab, 2017, Financial Cyberthreats 2016, p2

[119] Netclean, 2017, The Netclean Report 2016, p14

[120] Anti-Phishing Working Group (APWG), 2017, Phishing Activity Trends Report: 4th Quarter 2016, p11

[121] McAfee, 2017, McAfee Labs Threat Report June 2017, p82

[122] Trend Micro, 2017, TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats, p21

[123] Anti-Phishing Working Group (APWG), 2017, Phishing Activity Trends Report: 4th Quarter 2016, p11

[124] McAfee, 2017, McAfee Labs Threat Report June 2017, p81

[125] Symantec, 2017, Internet Security Threat Report: Volume 22, p15

[126] McAfee, 2017, McAfee Labs Threat Report June 2017, p72

[127] Kaspersky Lab, 2017, Mobile Malware Evolution, p12

[128] Panda Security. 2017, PandaLabs Report Q1 2017, p8

[129] https://www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html

[130] Trend Micro, 2017, TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats, p8

[131] Trend Micro, 2017, TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats, p21

[132] Symantec, 2017, Internet Security Threat Report: Volume 22, p15

[133] Trend Micro, 2017, TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats, p8

[134] Symantec, 2017, Internet Security Threat Report: Volume 22, p57

[135] Kaspersky Lab, 2017, Financial Cyberthreats 2016, p2

[136] Symantec, 2017, Internet Security Threat Report: Volume 22, p50

[137] Panda Security. 2017, PandaLabs Report Q1 2017, p9

[138] McAfee, 2017, McAfee Labs Threat Report June 2017, p81

[139] Trend Micro, 2017, TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats, p8

[140] Schiller, 2010, Cyber Attacks and Protection, p13

[141] See in this regard for example: Gercke, 2012, Understanding Cybercrime, ITU, p38

[142] Schiller, 2010, Cyber Attacks and Protection, p13

[143] Theohary, 2016, Information warfare: DOD's Response to the Islamic State Hacking Activities, CRS Insight, IN10486

[144] Gercke, 2012, Understanding Cybercrime, ITU, p38

[145] Jeong-ju, Student councils call for thorough investigation into DDoS scandal, The Kores Times, 4.1.2012

[146] Office of the Director of National Intelligence, Assessing Russian Activities and Intentions in Recent US Elections, ICA 2017-01D; Newman, Was Russia Behind the DNC Leaks?, Late, 25.07.2016

[147] Assessing Russian Activities and Intentions in Recent US Elections, ICA 2017-01D

[148] Willsher/Jenley, Emmanuel Macron's campaign hacked on eve of French election, The Guardian, 6.5.2017

[149] Symantec, 2016, Internet Security Threat Report Vol. 21, p31

[150] Willsher/Jenley, Emmanuel Macron's campaign hacked on eve of French election, The Guardian, 6.5.2017

[151] Peterson, Wikileaks posts nearly 20,000 hacked DNC emails online, The Washington Post, 22.7.2016

[152] Newport/Singh/Soroka/Traugott/Dugan, Email Dominates What Americans Have Heard About Clinton, Gallup, 19.9.2016

[153] Calabresi, Election Hackers Altered Voter Rolls, Stole Private Data, Officials Say, Time Magazine, 22.06.2017

[154] Watts, Foreign hackers may have hit voter registration site days before EU referendum, say MPs, The Independent, 11.4.2017

[155] Tillett, DHS official: Election systems in 21 states were targeted in Russia cyber attack , CBS News, 21.7.2017

[156] Riley/Robertson, Russian cyberattack hit electoral systems in 39 states before 2016 election, Dalls News, 13.6.2017

[157] Calabresi, Election Hackers Altered Voter Rolls, Stole Private Data, Officials Say, Time Magazine, 22.06.2017

[158] See for example: Klonowski, in Zhou/Lopez/Deng/Bao, Information Security, 8th International Conference, ISC 2005, p496; Kiewiet/Hall/Alvarez/Katz, Fraud or Failure? In Alvarez/Hall/Hyde, Election Frau, p127

[159] Commission for Examining Voting Machines, Report to the Senate and Assembly, 33rd Session of the Legislature, California, 1898, p11

[160] Bannet/Price/Rudys/Singer/Wallach, 2004, Hack-a-Vote: Demonstrating Security Issues with Electronic Vocting Systems, IEEE Security Privacy Magazine 2 (1), p32 et seq.

[161] Cole/Esposito/Biddle/Grimm, Top-Secret NSA report details Russian hacking effort days before the 2016 election

[162] Shermann, Experts Urge Clinton Campaign to Challenge Election Results in 3 Swing States, The NewYork Magazine, 22.11.2016

[163] With regard to Germany see for example: Gerling; Cyber Attacks on Free Elections, MaxPlackResearch 2/17, p10

[164] See for for example: Carroll, Are the Clinton WikiLeaks emails doctored, or are they authentic?; Politifact, 23.10.2016

[165] Willsher/Jenley, Emmanuel Macron's campaign hacked on eve of French election, The Guardian, 6.5.2017

[166] See for example: Timberg, Russian propaganda effort helps spread „fake news" during election, experts say, The Washington Post, 24.11.2016

[167] Regarding the harmonization approaches see: Gercke, 2012, Understanding Cybercrime, ITU, p114 et seq.

[168] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[169] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[170] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[171] Gercke, 2012, Understanding Cybercrime, ITU, p182

[172] See in this regard: Sec. 202d German Penal Code

[173] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[174] Regarding the principle of freedom of speech, see: Tedford/Herbeck/Haiman, 2005, Freedom of Speech in the United States; Barendt, 2007, Freedom of Speech; Baker, Human Liberty and Freedom of Speech; Emord, 1991, Freedom, Technology and the First Amendment; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; Volokh, 2001, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, p57 et seq.

[175] Gercke, 2012, Understanding Cybercrime, ITU, p225

QL-AL-17-001-EN-N

P.O. Box 908 50
2509 LW The Hague
Netherlands

www.europol.europa.eu

Follow us

Twitter: @Europol and @EC3Europol

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu