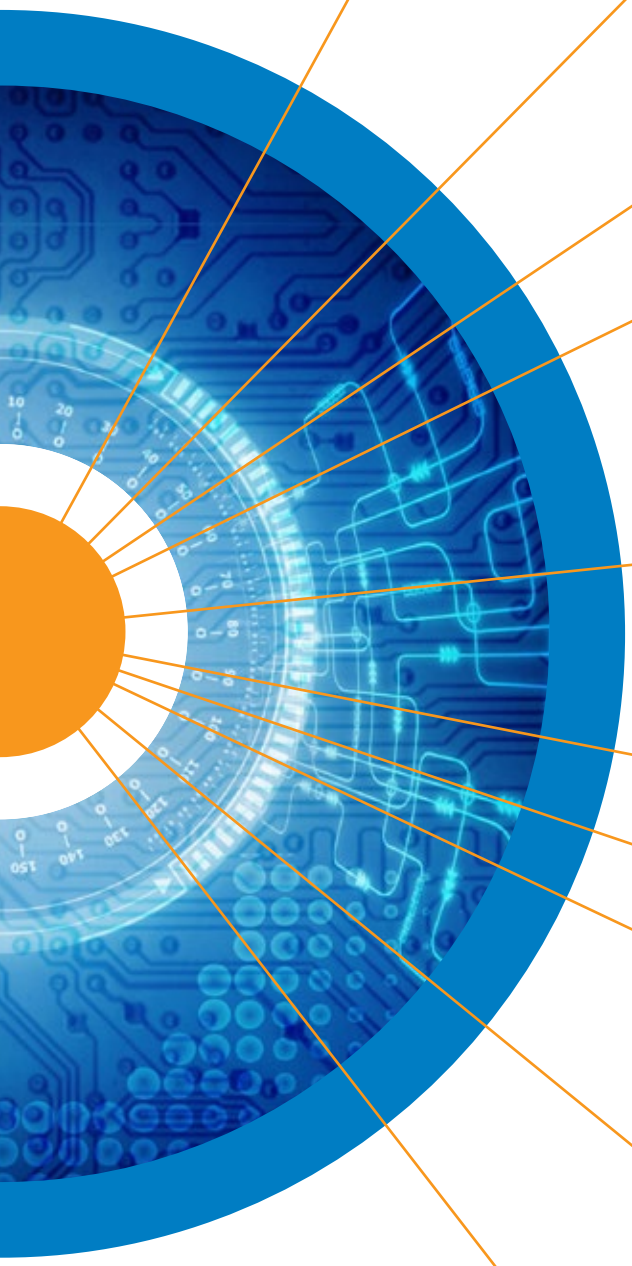
EUROPOL

The Internet Organised Crime Threat Assessment (IOCTA)

2015

TABLE OF CONTENTS



FOREWORD 5

ABBREVIATIONS 6

EXECUTIVE SUMMARY 7

KEY FINDINGS 10

KEY RECOMMENDATIONS 12

SUGGESTED OPERATIONAL PRIORITIES 15

INTRODUCTION 16

MALWARE 18

ONLINE CHILD SEXUAL EXPLOITATION 29

PAYMENT FRAUD 33

SOCIAL ENGINEERING 37

DATA BREACHES AND NETWORK ATTACKS 40

ATTACKS ON CRITICAL INFRASTRUCTURE 44

CRIMINAL FINANCES ONLINE 46

CRIMINAL COMMUNICATIONS ONLINE 50

DARKNETS 52

BIG DATA, IOT AND THE CLOUD 54

THE GEOGRAPHICAL DISTRIBUTION OF CYBERCRIME 57

GENERAL OBSERVATIONS 62

APPENDICES 67

A1. THE ENCRYPTION DEBATE 67

A2. AN UPDATE ON CYBER LEGISLATION 70

A3. COMPUTER CRIME, FOLLOWED BY CYBERCRIME FOLLOWED BY .... ROBOT AND AI CRIME? 72

FOREWORD

I am pleased to present the 2015 Internet Organised Crime Threat Assessment (IOCTA), the annual presentation of the cybercrime threat landscape by Europol's European Cybercrime Centre (EC3).

Using the 2014 report as a baseline, this assessment covers the key developments, changes and emerging threats in the field of cybercrime for the period under consideration. It offers a view predominantly from a law enforcement perspective based on contributions by EU Member States and the expert input of Europol staff, which has been further enhanced and combined with input from private industry, the financial sector and academia.

The assessment highlights the increasing professionalisation of cybercriminals in terms of how attacks are planned and orchestrated using both new methods and techniques in addition to employing well-known attack vectors, and with an increased risk appetite and willingness to confront victims.

The report lists a number of key recommendations to address the growing phenomenon of cybercrime and identifies several priority topics to inform the definition of operational actions for EU law enforcement in the framework of the EMPACT Policy Cycle.

These include concrete actions under the three main mandated areas – child sexual exploitation, cyber attacks, and payment fraud – such as targeting certain key services and products offered as part of the Crime-as-a-Service model, addressing the growing phenomenon of live-streaming of on-demand abuse of children, or targeted actions with relevant private sector partners against online payment fraud. The report also identifies several cross-cutting crime enablers such as bulletproof hosting, illegal trading sites on Darknets and money muling and laundering services that require concerted and coordinated international law enforcement action.

I am confident that the 2015 IOCTA, and Europol's work in supporting the implementation of the proposed recommendations and operational actions, will help set priorities for an international law enforcement response to cybercrime. The last 12 months have shown some remarkable successes by EU law enforcement in the fight against cybercrime, and I look forward to celebrating further successes as we move towards 2016 with law enforcement continuing to push the boundaries of traditional policing with our partners in the EU and beyond.

Rob Wainwright
Director of Europol

ABBREVIATIONS

AI	artificial intelligence
AV	anti-virus
APT	Advanced Persistent Threat
ATM	automated teller machine
CaaS	Crime-as-a-Service
CAM	child abuse material
C&C	command and control
ccTLD	country code top-level domain
CERT	computer emergency response team
CI	critical infrastructure
CNP	card-not-present
CP	card-present
CSE	child sexual exploitation
CSECO	commercial sexual exploitation of children online
DDoS	Distributed Denial of Service
EC3	European Cybercrime Centre
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EMV	Europay, MasterCard and Visa
EU	European Union
FP	Focal Point
I2P	Invisible Internet Project
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	information & communications technology
IaaS	Infrastructure-as-a-Service
IETF	Internet Engineering Task Force
IoE	Internet of Everything
IoT	Internet of Things
IOCTA	Internet Organised Crime Threat Assessment
IP	Internet protocol
ISP	Internet service provider
J-CAT	Joint Cybercrime Action Taskforce
JIT	joint investigation team
LE	law enforcement
MLAT	mutual legal assistance treaty
MS	Member State(s)
OCG	organised crime group
OSINT	open-source intelligence
P2P	peer to peer, or people to people
PGP	Pretty Good Privacy
PIN	personal identification number
PoS	point-of-sale
RAT	Remote Access Tool
SEPA	Single Euro Payments Area
SGIM	self-generated indecent material
SMS	short message service
SSDP	Simple Service Discovery Protocol
TLD	top-level domain
Tor	The Onion Router
UPnP	Universal Plug and Play
URL	uniform resource locator
VoIP	Voice-over-Internet Protocol
VPN	virtual private network

EXECUTIVE SUMMARY

The 2015 Internet Organised Crime Threat Assessment (IOCTA) shows that cybercrime is becoming more aggressive and confrontational. While certain elements of cybercrime such as social engineering have always had an element of interaction between victim and attacker, such contact would typically be of a passive, persuasive nature; otherwise cybercriminals were content to stealthily steal what they wanted with confrontation actively avoided. Today, however, cybercrime is becoming increasingly hostile. Instead of subterfuge and covertness, there is a growing trend of aggression in many cyber-attacks, and in particular the use of extortion, whether it is through sexual extortion, ransomware or by Distributed Denial of Service (DDoS) attacks. This boosts the psychological impact of fear and uncertainty it has on its victims. Whilst the cautious, stealthy approach goes with the stereotype of the uncertain, geeky hacker, the aggressive, confrontational approach of putting blunt pressure on individuals and businesses bears the signature of organised crime.

Cybercrime remains a growth industry. The Crime-as-a-Service (CaaS) business model, which grants easy access to criminal products and services, enables a broad base of unskilled, entry-level cybercriminals to launch attacks of a scale and scope disproportionate to their technical capability and asymmetric in terms of risks, costs and profits.

The sphere of cybercrime encompasses an extremely diverse range of criminality. In the context of 'pure' cybercrime, malware predictably persists as a key threat. As projected in the 2014 IOCTA, ransomware attacks, particularly those incorporating encryption, have grown in terms of scale and impact and almost unanimously represent one of the primary threats encountered by EU businesses and citizens as reported by law enforcement (LE). Information stealing malware, such as banking Trojans, and the criminal use of Remote Access Tools (RATs) also feature heavily in law enforcement investigations.

Banking malware remains a common threat for citizens and the financial sector alike, whilst generating sizeable profits for cybercriminals. A coordinated effort between law enforcement, the financial sector and the Internet security industry will be required in order to effectively tackle this problem. This will necessitate better sharing of banking malware samples and criminal intelligence, particularly relating to enabling factors such as money mules.

The media commonly referred to 2014 as the "Year of the data breach", with record numbers of network attacks recorded. Although this undoubtedly represents an actual increase in attacks, it also signifies a change in attitude by victim organisations. The perception of how an organisation handles a breach – which today is considered inevitable – is crucial. This has led to greater publicity and more frequent involvement of law enforcement in such attacks. Nonetheless, is it is evident that data has become a key target and commodity for cybercrime.

Notably, there is blurring of the lines between Advanced Persistent Threat (APT) groups and profit-driven cybercriminals with both camps borrowing tools, techniques and methodologies from each other's portfolios.

While it is possible for organisations to invest in technological means to protect themselves, the human element will always remain as an unpredictable variable and a potential vulnerability. As such social engineering is a common and effective tool used for anything from complex multi-stage attacks to fraud. Indeed, CEO fraud – where the attackers conduct detailed research on selected victims and their behaviour before initiating the scam – presents itself as a prominent emerging threat which can result in large losses for those affected.

Child sexual exploitation (CSE) online poses major concerns in several respects. Hidden services within the Darknet are used as a platform for the distribution of child abuse material (CAM). The nature of these services drives the abuse of new victims because the production of fresh material is demanded for membership on child abuse forums and it reinforces the status of the contributors. These offences will require more intensive cooperation and capacity building in jurisdictions where they occur. Law enforcement must focus on identifying and dismantling these communities and forums in which offenders congregate. The identification and rescue of victims must also be paramount.

The apparent proliferation of self-generated indecent material (SGIM) can be attributed to the increased availability of mobile devices and their ease of use in producing such content and communicating it to others. Photos and videos of this nature that are initially shared with innocent intent often find their way to those who collect this material or intend to further exploit the victim, in particular by means of extortion. The volume of SGIM and the rate of its growth represents a serious challenge for LE.

The live streaming of child abuse may grow, fuelled by increasing broadband coverage in developing countries. Commercial streaming is expected to become more prolific as streaming tools incorporating anonymous payment mechanisms are adopted by offenders. This development further reinforces the necessity for closer cooperation and enhanced capacity building within the international law enforcement community.

Furthermore, child abuse offenders are facilitated by many of the same services and products as mainstream cybercriminals including encryption, anonymisation and anti-forensic tools. Use of these methods among offenders is no longer the exception but the norm. Increasing abuse of remote storage facilities and virtual currencies was also observed last year and has continued to grow since.

Card-not-present (CNP) fraud grows steadily as compromised card details stemming from data breaches, social engineering attacks and data stealing malware become more readily available. The push towards CNP fraud is further driven by the effective implementation of measures against card-present fraud such as EMV (chip and PIN), anti-skimming ATM slots and geoblocking. This trend is only likely to increase as the USA, a primary cash-out destination for compromised EU cards, will implement EMV technology as of October 2015.

It is a common axiom that technology, and cybercrime with it, develops so fast that law enforcement cannot keep up. Whilst this may be true in some respects, the vast majority of cybercrimes consist of using vulnerabilities that were well-known for quite a while. It is the lack of digital hygiene of citizens and businesses that provides fertile ground for the profitable CaaS market of reselling proven exploit kits to the expanding army of non-tech-savvy cybercriminals. Ingenuity often only extends to finding new ways to use or implement such tools and methods. The scope and pace of true innovation within the digital underground is therefore more limited than many may believe. Furthermore, a key driver of innovation within cybercrime may be law enforcement itself. Every law enforcement success provides impetus for criminals to innovate and target harden with the aim of preventing or mitigating further detection and disruption of their activities.

That said, where genuine innovation exists in technology, criminals will rapidly seek ways to exploit it for criminal gain. Developing technologies such as Darknets, the Internet of Things, artificial intelligence, and blockchain technology all provide new attack vectors and opportunities for cybercrime, often combined with existing tools and techniques such as steganography.

The attention of industry is yet not fully focussed on cyber security or privacy-by-design. Many of the so-called smart devices are actually quite dumb when it comes to their security posture, being unaware of the fact that they are part of a botnet or being used for criminal attacks. The Simple Service Discovery Protocol (SSDP), which is enabled by default on millions of Internet devices using the Universal Plug and Play (UPnP) protocol including routers, webcams, smart TVs or printers, became the leading DDoS amplification attack vector in the first quarter of 2015[1].

1 Akamai, State of the Internet – Security Report, https://www.stateoftheinternet.com/resources-web-security-2015-q1-internet-security-report.html, 2015

The response of law enforcement has produced several successes in the fight against cybercrime. Strong elements in the approach taken are the increasing level of international cooperation between main cybercrime divisions within the EU and with those of non-EU partners. The alignment of priorities under the operational actions of EMPACT and the establishment of the Joint Cybercrime Action Taskforce (J-CAT) have clearly contributed to that. But also the close involvement of private sector partners, especially in the Internet security industry and among financial institutions has helped to get a better grip on cybercrime.

Tactically, some consideration should be given to the investigative focus and approach to increase the effectiveness of operational activities even further. Merely trying to investigate what gets reported is unlikely to lead to the best results. It is important to identify the different components and facilitating factors to understand with which tactics specific types of crime can be addressed most effectively. The key enablers of the pertinent threats reported by EU law enforcement that are deemed most important to take out by means of criminal investigations are bulletproof hosting, criminal expert forums, malware distribution through botnets, CaaS vending sites, counter-anti-virus services and carding sites. Also, financial facilitation by the criminal use of Bitcoins, laundering services and money mules deserve priority. To the extent possible and realistic, the focus should primarily be on the arrest of key perpetrators and organised crime groups (OCGs). Yet such an approach should be complemented by dismantling, awareness raising, prevention, dissuasion and asset recovery.

The main investigative challenges for law enforcement are common to all areas of cybercrime: attribution, anonymisation, encryption and jurisdiction. Even cybercriminals with minimal operational security awareness can pose a challenge in terms of attribution due to the range of easily accessible products and services that obfuscate their activity and identity. These include the abuse of privacy networks like I2P and The Onion Router (Tor) for communications and trade, and virtual currencies for criminal transactions. Effective investigations require an increasing volume of digitised data and yet law enforcement often faces inadequate data retention periods and regulations. Encryption is increasingly used to safeguard communications and stored data but also to frustrate forensic analysis and criminal investigations. Cybercriminals continue to operate from – or house infrastructure in – jurisdictions where EU law enforcement lacks adequate basis for support.

KEY FINDINGS

- Cybercrime is becoming more aggressive and confrontational. Various forms of extortion requiring little technical skills suggest changes in the profile of cybercrime offenders, and increase the psychological impact on victims.

- While there may always be a need for laws which compel private industry to cooperate with law enforcement, there is greater benefit in establishing and building working relationships in order to stimulate the voluntary and proactive engagement of the private sector.

- Malware predictably remains a key threat for private citizens and businesses. Ransomware attacks, particularly those incorporating encryption, were identified as a key threat both in terms of quantity and impact. Information stealers, such as banking Trojans, and the criminal use of Remote Access Tools (RATs) also feature heavily in malware investigations.

- Due to the support for many of the 'old school' banking Trojans such as Zeus, Citadel or Spyeye being withdrawn, either voluntarily or as a result of law enforcement action, the use of many of these products is in decline, paving the way for a new generation of malware such as such as Dyre or Dridex.

- The number and frequency of publically disclosed data breaches is dramatically increasing, highlighting both a change in attitude by industry and that data is still a key target and commodity for cybercriminals. Such breaches, particularly when sensitive personal data is disclosed, inevitably lead to secondary offences as the data is used for fraud and extortion.

- Social engineering is a common and effective tool used for anything from complex multi-stage cyber-attacks to fraud. CEO fraud is one such threat which is emerging, leading to significant losses for individual companies and requiring little technical knowledge to commit.

- Payment fraud has seen a further shift to card-not-present fraud, and is increasing in line with the growing number of merchants embracing e-commerce and the implementation of effective measures to combat skimming and card-present fraud. While card-present fraud is slightly in decline, novel malware attacks on ATMs are still evolving.

- Rather than devising novel attack methods, most cyber-attacks rely on existing, tried and tested exploits, malware code and methodologies such as social engineering, which are re-used and recycled to create new threats.

- The lack of digital hygiene and security awareness contributes to the long lifecycle and continued sales of exploit kits and other basic products through CaaS models, bringing opportunities and gain to the criminal masses.

- Operation Onymous resulted in an unprecedented mass takedown of Darknet marketplaces and disruption of market interactions. The underground ecosystem has since recovered to some degree but confidence has been further eroded by a number of prominent marketplaces exit scams.
- In the aftermath of operation Onymous, there were many proponents for a shift to allegedly more secure platforms such as I2P. This has not occurred however and Tor remains the preferred platform for underground fora and marketplaces.
- Growing Internet coverage in developing countries and the development of pay-as-you-go streaming solutions providing a high degree of anonymity to the viewer, are furthering the trend in the commercial live streaming of child sexual abuse.
- Growing numbers of children and teenagers own smart phones that they use to access social media and communication apps. This enables the generation and distribution of large amounts of self-generated indecent material (SGIM), which makes these adolescents vulnerable to sexual extortion.
- The use of anonymisation and encryption technologies is widening. Although these address a legitimate need for privacy, they are exploited by criminals. Attackers and abusers use these to protect their identities, communications, data and payment methods.
- Bitcoin is establishing itself as a single common currency for cybercriminals within the EU. Bitcoin is no longer used preferentially within Darknet marketplaces but is increasingly being adopted for other types of cybercrime as well.

KEY RECOMMENDATIONS

INVESTIGATION

- Cybercrime investigations are often complex and resource intensive. Law enforcement therefore must be granted the latitude it requires in order to conduct long-term comprehensive investigations for maximum impact without undue pressure to obtain rapid results or arrests.

- While targeting high profile, high value targets such as malware developers may be beneficial, the disruptive effect of targeting either shared criminal infrastructure or the less ubiquitous actors who provide key support services, such as bulletproof hosting, may have more significant impact across a greater division of the cybercrime community and represent a more pragmatic approach for law enforcement.

- Law enforcement requires greater flexibility and/or resources to effectively investigate underlying criminality instead of simply that which is directly reported by victims.

- A coordinated effort between law enforcement, the financial sector and the Internet security industry will be required in order to effectively tackle banking malware. This will necessitate better sharing of banking and ATM malware samples (using the Europol Malware Analysis System (EMAS) for example) and criminal intelligence, particularly relating to enabling factors such as money mules.

- The protection of victims of child abuse is paramount. Therefore victim identification investigations should be given equal priority to those directed at the arrest of offenders for production of CAM. The efficient use of available Victim ID databases, taking into account the current and future efforts undertaken by EC3 and Interpol in this field, as well as detailed analysis of the material, often lead to successful rescue operations.

- Law enforcement investigation of CSE must focus on identifying and dismantling the communities and forums in which offenders congregate. These environments act to stimulate the production of fresh child abuse material, thus generating new victims and ensuring the continued abuse of existing victims.

- Law enforcement must continue and expand successful initiatives to share knowledge, expertise and best practice on dealing with Bitcoin and other emerging/niche digital currencies in cyber investigations.

CAPACITY BUILDING & TRAINING

- In order to counter the increasing occurrence of encryption used by offenders, law enforcement should invest in live data forensics capability and prioritise in situ analysis of devices, in order to capture the relevant artefacts in an unencrypted state.

- Investigators must familiarise themselves with the diverse range of account and payment references and the file formats of digital wallets used by different payment mechanisms.

- Law enforcement requires the tools, training and resources to deal with high volume crime such as payment card fraud and social engineering. Such crimes also require an efficient, fit-for-purpose reporting mechanism. Online reporting channels are considered to be highly suitable for high-volume crimes of a minor nature.

- In order to continue the successes law enforcement has demonstrated in tackling crime on the Darknet, law enforcement must continue to share best practice, knowledge and expertise in performing such investigations, focusing on such issues as the ability to trace and attribute criminal transactions and communication on the Darknet.

- There is a need to inform law enforcement on a broad basis about Big Data and the challenges and opportunities that come with it.

PREVENTION

- While dismantling or disrupting criminal groups is effective and necessary, adequate resources should be given to prevention strategies in order to raise awareness of cybercrime and increase standards in online safety and information security.
- Prevention activity in relation to child sexual exploitation online should incorporate school visits and explain the potential impact of SGIM. Real case examples can demonstrate how seemingly harmless interactions may lead to serious consequences for the victim.
- To mitigate the risk of ATM malware attacks law enforcement should promote Europol's 'Guidance and Recommendations regarding Logical Attacks on ATMs', at a national and international level, to banking and payments industry contacts.

PARTNERSHIPS

- It is essential for law enforcement to build and develop working relationships with the financial sector including banks, payments industry, money transfer agents, virtual currency scheme operators and exchangers in order to:
  - Promote the lawful exchange of information and intelligence in relation to areas of criminality such as banking malware, money mules and fraud;
  - In this regard Europol's EC3 will drive a comprehensive initiative to counter the threat of money mules, drawing on data from private industry and law enforcement in order to inform and direct EU law enforcement in tackling this key support service.
  - Establish a secure common channel through which to pass details of compromised card and account data in order to prevent their subsequent use in fraud.
- In order to address the under-reporting and cybercrime in general, law enforcement must continue to engage with private industry to increase confidence in law enforcement's ability to investigate both effectively and discretely.
- In the context of the draft Directive on Network and Information Security (NIS), there is a need to improve coordination, active partnership, and relationships between the private sector, law enforcement and the CERT community.
- Law enforcement should continue to collaborate with the private sector and academia to explore investigative and research opportunities related to emerging technologies such as decentralised marketplaces, artificial intelligence and blockchain technology.
- EU law enforcement must develop working relationships and build capacity within law enforcement in non-EU jurisdictions, particularly south-east Asia, in order to improve information sharing and investigative capability in relation to criminality such as live streaming of child abuse and payment card fraud.

- EU Member States should provide intelligence relating to hidden services to Europol's EC3 to allow it to build a comprehensive intelligence picture of hidden services across Europe. Additionally there needs to be greater engagement from non-cybercrime law enforcement in tackling hidden services. Extremism and the sale of drugs or firearms are as much of an issue on these services as cybercrime.

- Law enforcement must continue to share information with and via Europol in relation to high volume crime such as social engineering attacks in order to identify the campaigns that are having the greatest impact, thereby allowing law enforcement to manage its resources more effectively.

- Law enforcement should seek to actively engage in and share the success of multi-stakeholder initiatives such as Europol's Airline Action Days[2] and E-commerce initiative in order to combat payment fraud in their jurisdiction.

LEGISLATION

- There is still a need for harmonised legislative changes at EU level, or the uniform application of existing legal tools such as laundering regulations to address the criminal use of virtual currencies.

- In order to effectively investigate closed offender communities on the Darknet and other networks, investigators require relevant legal instruments that allow undercover work and the efficient online use of traditional policing investigation methods.

- Policymakers must ensure the swift implementation of the EU Directive on attacks against information systems[3] which will introduce tougher, consistent and EU-wide penalties for cyber-attacks and criminalise the use of malware as a method of committing cybercrimes.

- Legislators and policymakers, together with industry and academia, must agree on a workable solution to the issue of encryption which allows legitimate users to protect their privacy and property without severely compromising government and law enforcement's ability to investigate criminal or national security threats. A quantitative analysis of the impact of encryption on law enforcement investigations is required in order to support the qualitative arguments in this debate.

2 Europol Press Release, Global Action against Online Air Ticket Fraudsters Sees 130 Detained, https://www.europol.europa.eu/content/global-action-against-online-air-ticket-fraudsters-sees-130-detained, 2015

3 EU Directive on Attacks against Information Systems, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF, 2013

SUGGESTED OPERATIONAL PRIORITIES

In view of the role of the IOCTA to inform the priority setting for the operational action plans in the framework of the EMPACT, and considering the information presented in this report, the following topics are proposed for the forthcoming definition of operational actions for EU law enforcement for 2016:

CYBER ATTACKS

- Botnet takedowns, in particular those deployed for DDoS attacks and distribution of banking malware (e.g. Dyre and Dridex);
- Sales of ransomware and exploit kits as part of the CaaS model;
- Structured deployment of malware, in particular ransomware and banking malware;
- Data breaches and APTs;
- Counter anti-virus services.

CSE

- Live streaming of on-demand abuse;
- Sexual extortion;
- Lawful infiltration and takedown of online communities that stimulate active CAM production, in particular on the Darknet;
- Victim identification and rescue.

PAYMENT FRAUD

- Takedowns of carding sites;
- Targeted actions with relevant private sector partners;
- ATM malware;
- (Cyber-facilitated) CEO fraud and phishing.

CROSS-CUTTING CRIME ENABLERS

- Bulletproof hosting;
- Illegal trading sites on the Darknet;
- Money mules and money laundering services;
- Criminal schemes around Bitcoin and other virtual currencies;
- Criminal expert online forums.

To the extent possible and realistic, the focus should primarily be on the arrest of key perpetrators and OCGs. This should be complemented by dismantling, awareness raising, dissuasion and asset recovery.

In addition to these predominantly investigative topics, it is also advised to implement facilitating actions around intelligence sharing and tactical analysis, especially around the above mentioned themes to better enable successful operations. Furthermore, these activities can be complemented by more strategic initiatives around training and capacity building, as well as prevention and awareness.

INTRODUCTION

AIM

The 2015 Internet Organised Crime Threat Assessment (IOCTA) was drafted 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, and in particular the priority setting for the 2016 EMPACT[4] operational action plan in the three sub-areas of the cybercrime priority: cyber attacks, payment fraud and child sexual exploitation.

Building on the broad basis established in the 2014 IOCTA, this report provides an update on the latest trends and the current impact of cybercrime within the EU from a law enforcement perspective. It highlights 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.

Unlike the 2014 IOCTA which offered a broad, strategic overview of the cybercrime threat landscape, the 2015 IOCTA has taken a slightly different approach and presents *a view from the trenches*. This year, the focus is on the threats and developments within cybercrime, based predominantly on the experiences of cybercrime investigators and their operational counterparts from other sectors, drawing on contributions from more strategic partners in private industry and academia to support or contrast this perspective. In this sense the report chiefly highlights the threats that are more visibly impacting industry and private citizens.

The 2015 IOCTA challenges the conception that law enforcement lags behind the criminals they investigate in terms of skills or technical capability by highlighting the successes of law enforcement across the EU and globally in tackling complex cybercrime in areas such as the Darknet and dismantling botnets.

SCOPE

The 2015 IOCTA focuses on EC3's three mandated crime areas – cyber attacks, child sexual exploitation online and payment fraud. Where relevant, it also covers other related areas such as money laundering and social engineering.

The report examines the main developments since the previous report, highlighting the increasing professionalisation of cybercrime and further refinement of the CaaS model. In addition to the identification of some emerging trends such as the use of decentralised online platforms for criminal purposes and a convergence of tools and tactics used by different groups, the assessment also shows the continuing criminal exploitation of well-known attack vectors and vulnerabilities.

Despite the identified technical, legal and operational challenges, the report offers a number of examples of successful law enforcement actions against cybercriminals and organised crime in cyberspace, for instance in relation to the criminal abuse of Tor. At the same time, it highlights the pressure such operations put on cybercriminals requiring them to update their modus operandi and to become more innovative in their attacks. This is evident, for instance, in the increasing tendency towards the criminal abuse of encryption, anonymity and the increased use of obfuscation and anti-forensic tools and methods.

The assessment provides an update on topics such as the Internet of Things and Big Data that have or are likely to have an impact on the crime areas covered in this report.

Each chapter provides a law enforcement centric view on the most prominent crimes or threat areas, followed by a prediction of the future developments that are likely to impact law enforcements ability to combat the threat. Each chapter ends with a set of specific recommendations predominantly for law enforcement to effectively address the threats presented.

4 The European Multidisciplinary Platform Against Criminal Threats (EMPACT), is a structured multidisciplinary co-operation platform of the relevant Member States, EU Institutions and Agencies, as well as third countries and organisations (public and private) to address prioritised threats of serious international and organised crime.

Not covered in this year's edition of the IOCTA is the development of online radicalisation and the proliferation of violent extremism through social media. With the establishment of the EU Internet Referral Unit (EUIRU) at Europol from 1 July 2015, it is most probable that this subject will be covered next year, either as part of the 2016 IOCTA or as a separate product by the newly-established unit.

METHODOLOGY AND ACKNOWLEDGEMENTS

The 2015 IOCTA was drafted by a team of strategic analysts within EC3 drawing predominantly on contributions from EU Member States, the EUCTF, Focal Points Cyborg, Terminal and Twins, as well as the Cyber Intelligence team, and the SOCTA team via structured surveys, moderated workshops and interviews. This has been enhanced with open source research and input from the private sector, including EC3's advisory groups, and academia. These contributions have been essential to the production of the report.

Europol would like to extend special thanks to Professor Marco Gercke, Professor Michael Levi and Professor Alan Woodward of the IOCTA Advisory Board for their contributions.

MALWARE

Whether it is used in direct methods of attack or as an enabler for downstream cybercrime, malware remains one of the key threat areas within cybercrime. The malware identified as the current threats across the EU by EU law enforcement can be loosely divided into three categories based on their primary functionality – ransomware, Remote Access Tools (RATs) and info stealers. It is recognised that many malware variants are multifunctional however and do not sit neatly in a single category. For example, Blackshades is primarily a RAT but has the capability to encrypt files for ransom attacks; many banking Trojans have DDoS capability or download other malware onto infected systems.

KEY THREAT – RANSOMWARE

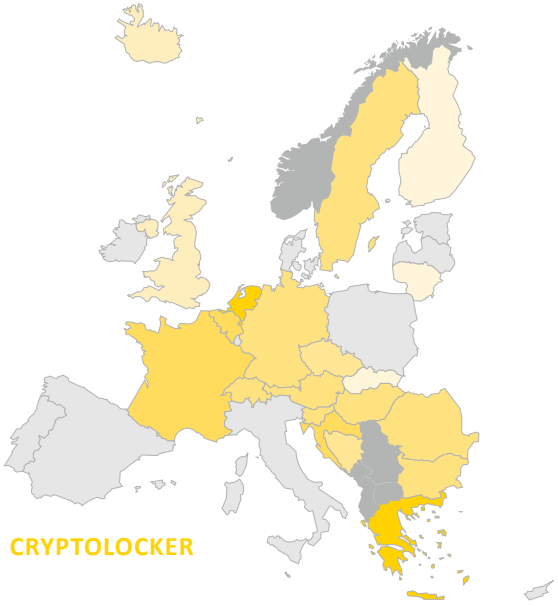
Ransomware remains a top threat for EU law enforcement. Almost two-thirds of EU Member States are conducting investigations into this form of malware attack. Police ransomware accounts for a significant proportion of reported incidents, however this may be due to an increased probability of victim reporting or it simply being easier for victims to recognise and describe. Industry reporting from 2014 indicates that the ransomware phenomenon is highly concentrated geographically in Europe, North America, Brazil and Oceania[5].

5 Microsoft SIR v18, http://download.microsoft.com/download/7/1/A/71ABB4EC-E255-4DAF-9496-A46D67D875CD/Microsoft_Security_Intelligence_Report_Volume_18_English.pdf, 2015

CryptoLocker

CryptoLocker is not only identified as the top malware threat affecting EU citizens in terms of volume of attacks and impact on the victim, but is considered to be one of the fastest growing malware threats. First appearing in September 2013, CryptoLocker is believed to have infected over 250 000 computers and obtained over EUR 24 million in ransom within its first two months[6]. CryptoLocker is also a notable threat amongst EU financial institutions.

In May 2014, Operation Tovar significantly disrupted the Gameover Zeus botnet, the infrastructure for which was also used to distribute the CryptoLocker malware[7]. At the time the botnet consisted of up to one million infected machines worldwide. The operation involved cooperation amongst multiple jurisdictions, the private sector and academia. Tools to decrypt encrypted files are now also freely available from Internet security companies8.



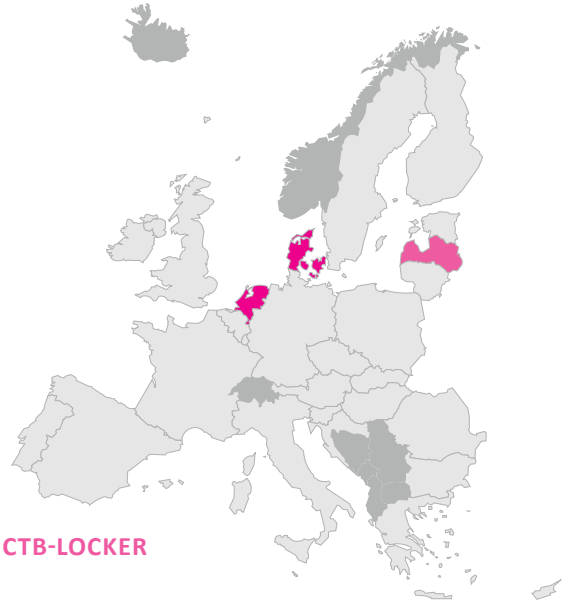
6 Europol Press Release, International Action against Gameover Zeus Botnet and Cryptolocker Ransomware, http://www.europol.europa.eu/content/international-action-against-gameover-Zeus-botnet-and-cryptolocker-ransomware, 2015

7 Europol Press Release, International Action against Gameover Zeus Botnet and Cryptolocker Ransomware, http://www.europol.europa.eu/content/international-action-against-gameover-Zeus-botnet-and-cryptolocker-ransomware, 2015

8 Decryptolocker, https://www.decryptcryptolocker.com/, 2014

CTB-LOCKER

Curve-Tor-Bitcoin (CTB) Locker is a more recent iteration of cryptoware using Tor to hide its command and control (C2) infrastructure. CTB Locker offers its victims a selection of language options to be extorted in and provides the option to decrypt a "test" file for free. Although not as widespread as CryptoLocker, CTB Locker was noted as a significant and growing threat by a number of EU Member States. This is supported by industry reporting which indicates that up to 35% of CTB Locker victims reside within Europe[9].



KEY THREATS – REMOTE ACCESS TOOLS (RATS)

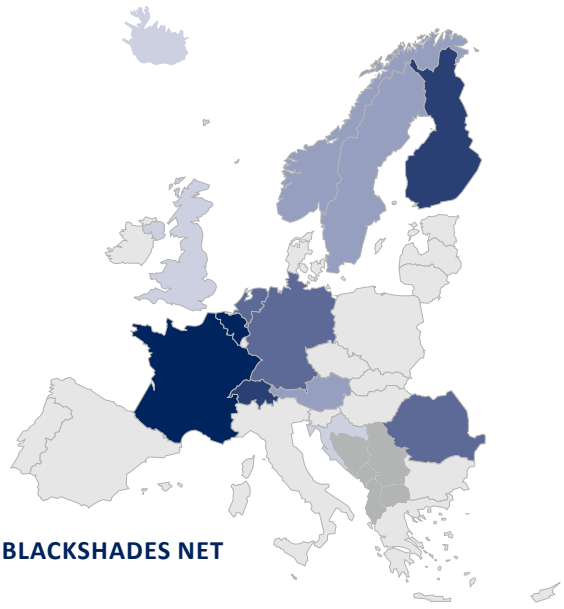
Remote Access Tools exist as legitimate tools used to access a third party system, typically for technical support or administrative reasons. These tools can give a user remote access and control over a system, the level of which is usually determined by the system owner. Variants of these tools have been adapted for malicious purposes making use of either standard or enhanced capabilities to carry out activities such as accessing microphones and webcams, installing (or uninstalling) applications (including more malware), keylogging, editing/viewing/moving files, and providing live remote desktop viewing, all without the victims knowledge or permission.

9 McAfee Labs Threat Report, Q1 2015, http://www.mcafee.com/nl/resources/reports/rp-quarterly-threat-q1-2015.pdf, 2015

Blackshades.NET

Blackshades first appeared in approximately 2010 and was cheaply available (~€35) on hacking forums. In addition to typical RAT functionality, Blackshades can encrypt and deny access to files (effectively acting as ransomware), has the capability to perform DDoS attacks, and incorporates a "marketplace" to allow users to buy and sell bots amongst other Blackshades users[10].

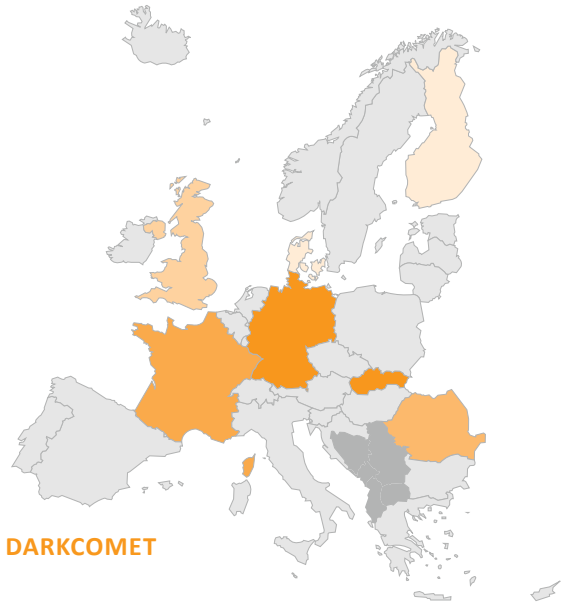
In May 2014, a two-day operation coordinated by Eurojust and Europol's EC3 resulted in almost 100 arrests in 16 countries worldwide. The operation targeted sellers and users of the Blackshades malware including its co-author. Despite this, the malware still appears to be available, although its use is in decline.



10 Malwarebytes, You Dirty RAT! Part 2 – Blackshades NET, https://blog.malwarebytes.org/intelligence/2012/06/you-dirty-rat-part-2-blackshades-net/, 2012

DarkComet

DarkComet was developed by a French security specialist known as *DarkCoderSC* in 2008. The tool is available for free. In 2012 *DarkCoderSC* withdrew support for the project and ceased development as a result of its misuse[11]. However it is still in circulation and widely used for criminal purposes.



KEY THREATS – INFO STEALERS

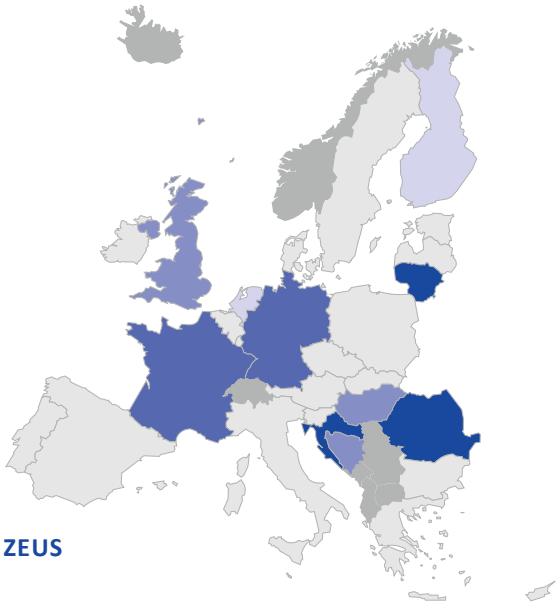
Data is a key commodity in the digital underground and almost any type of data is of value to someone; whether it can be used for the furtherance of fraud or for immediate financial gain. It is unsurprising then that the majority of malware is designed with the intent of stealing data. Banking Trojans – malware designed to harvest login credentials or manipulate transactions from online banking – remain one of the top malware threats.

Zeus

First appearing in 2006, Zeus is one of most significant pieces of malware to date. The Zeus source code was publically leaked in May 2011 after its creator abandoned it in late 2010. Since then a number of cybercrime groups have adapted the source code to produce their own variants. As such Zeus still represents a considerable threat today and will likely continue to do so as long as its original code can be updated and enhanced by others.

Gameover Zeus (GOZ) or Peer-to-Peer (P2P) Zeus was one such variant which used a decentralised network of compromised computers to host its command and control infrastructure, thereby making it more resistant to law enforcement intervention.

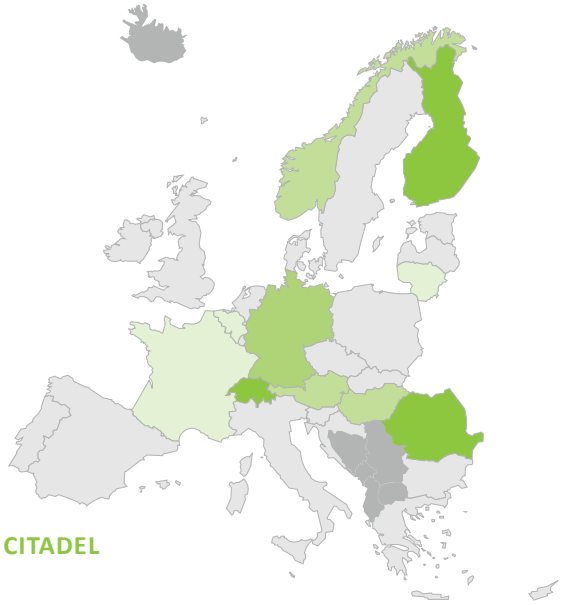
In June 2015, a joint investigation team (JIT) consisting of investigators and judicial authorities from six European countries, supported by Europol and Eurojust, arrested a Ukrainian cybercrime group who were developing and distributing the Zeus and Spyeye malware and cashing-out the proceeds of their crimes. The group is believed to have had tens of thousands of victims and caused over EUR 2 million in damages.



11 Symantec Official Blog, DarkComet RAT – It is the END, http://www.symantec.com/connect/blogs/darkcomet-rat-it-end/, 2012

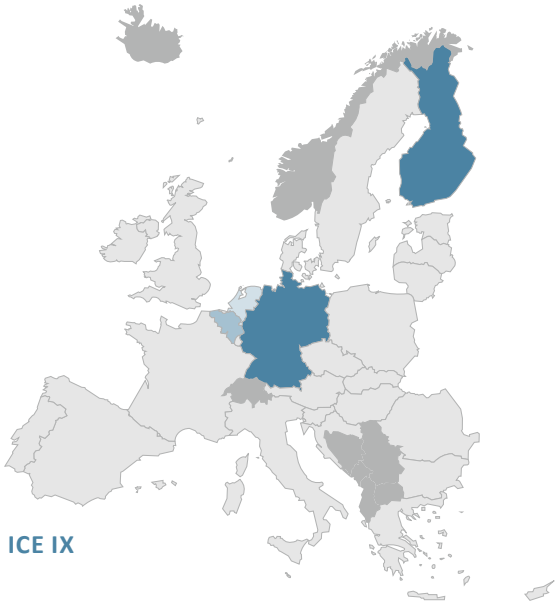
Citadel

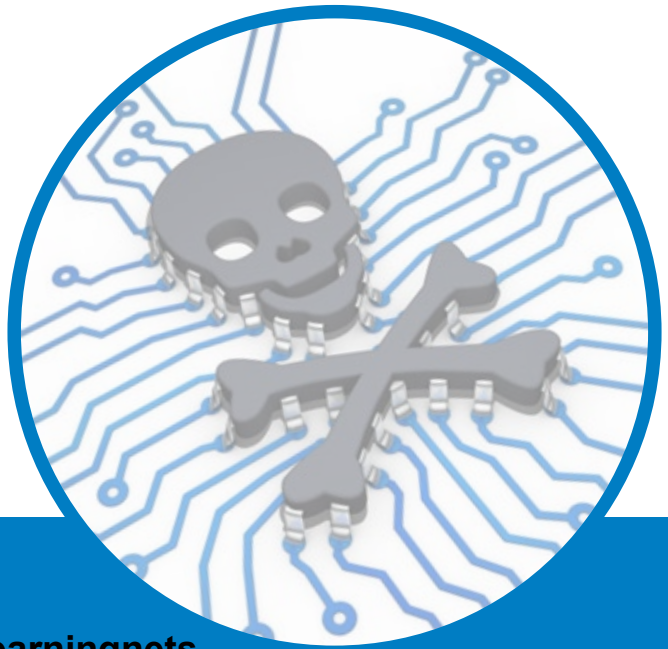
Citadel is a successful descendant of Zeus. It first appeared in circa 2012 and was initially sold openly on underground forums before being withdrawn from general distribution later that year. Its sale and use is now limited to select groups. Citadel infection rates have never reached the huge numbers Zeus itself has attained. Instead Citadel appears to be used for much more targeted (APT) attacks – campaigns targeting specific businesses or government entities[12,13]. Citadel has been noted as the first malware to specifically target password management solutions[14].



Ice IX

Ice IX is another first generation Zeus variant following the release the Zeus source code, appearing in the same time period as Citadel. Although its use appears to be in decline, several EU Member States have still actively investigated cases of its use.





12 McAfee Labs, Labs Paper Looks 'Inside the World of the Citadel Trojan', https://blogs.mcafee.com/mcafee-labs/labs-paper-looks-inside-the-world-of-the-citadel-trojan/, 2013

13 Security Intelligence, Massively Distributed Citadel Malware Targets Middle Eastern Petrochemical Organizations, https://securityintelligence.com/massively-distributed-citadel-malware-targets-middle-eastern-petrochemical-organizations/, 2014

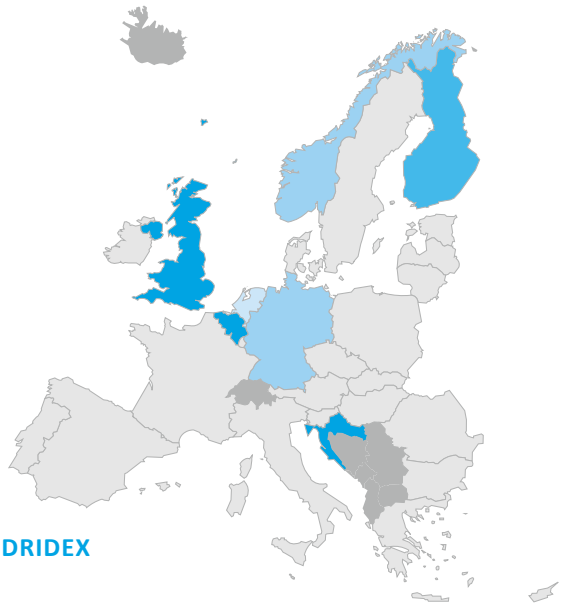
14 Security Intelligence, Cybercriminals Use Citadel to Compromise Password Management and Authentication Solutions, http://securityintelligence.com/cybercriminals-use-citadel-compromise-password-management-authentication-solutions/, 2014

Spyeye

Spyeye appeared in late 2009 on Russian underground forums. Cheaper than the leading malware kit at the time (Zeus) while mirroring much of its functionality, Spyeye quickly grew in popularity. It is believed that when Zeus developer *Slavik* ceased Zeus's development, the source code was sold/transferred to Spyeye developer *Harderman/Gribodemon*, only a short while before the Zeus source code was leaked publically. In January 2014, Russian national *Panin* pleaded guilty before a US federal court on charges related to the creation and distribution of Spyeye. Despite this several EU Member States are still actively investigating cases related to Spyeye, although its use is apparently in decline.

Dridex

Dridex first appeared in circa November 2014 and is considered the successor to the Cridex banking malware. However, unlike Cridex, which relied on exploit kit spam for propagation, Dridex has revived the use of malicious macro code in Microsoft Word attachments distributed in spam in order to infect its victims[15]. Several EU Member States have encountered Dridex and, although instances are low in number, the sensitivity of the harvested data, increasing degree of sophistication and growing number of cases confirm Dridex is an upcoming threat.



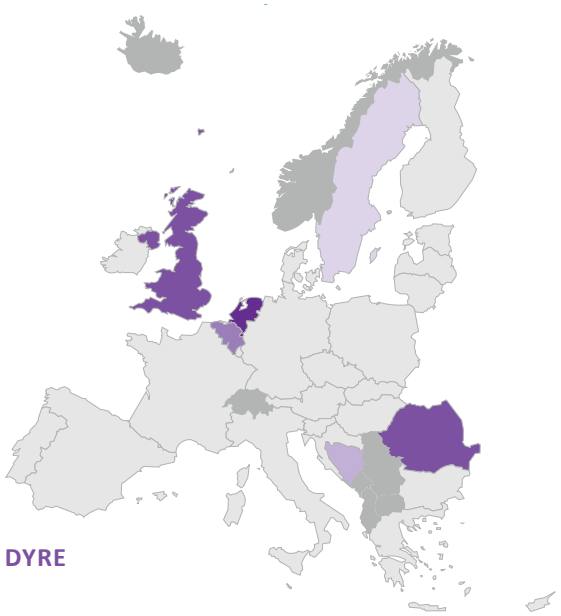
15 Trend Micro, Dealing with the Mess of Dridex, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3147/dealing-with-the-mess-of-dridex, 2014

Dyre

Dyre is a new malware kit which appeared in 2014, using a number of 'Man-in-the-Browser' attack techniques to steal banking credentials. Dyre targets over 1000 banks and other organisations including electronic payment and digital currency services, with a particular focus on those in English-speaking countries[16]. Some campaigns use additional social engineering techniques to dupe their victims into revealing banking details[17]. Dyre is also noted for its ability to evade popular sandbox environments used by researchers to analyse malware[18] and by its ability to download additional malware payloads onto an infected system such as the Cryptowall ransomware[19].

Tinba

Tinba, the truncation of 'tiny banker' – referring to its small file size (~20kb) – first appeared in 2012. Tinba has been noted as largely targeting non-English language countries such as Croatia, Czech Republic[20] and Turkey[21]. The source code for Tinba was leaked in 2014 allowing its ready-made code to be used by other cybercriminals for free.



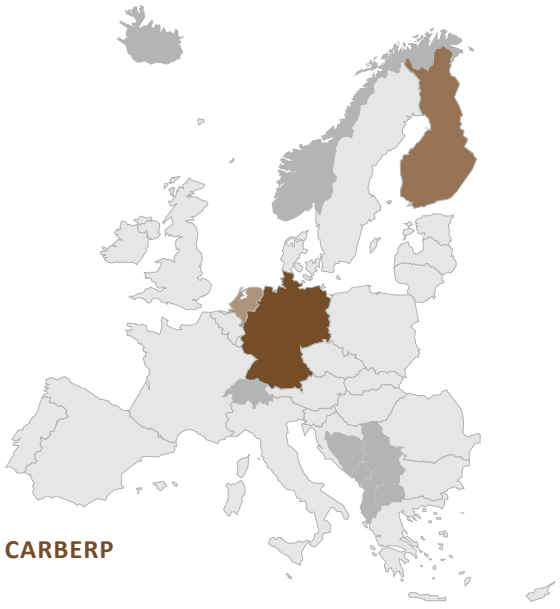
16 Symantec, Dyre: Emerging Threat on Financial Fraud Landscape, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dyre-emerging-threat.pdf, 2015
17 Security Intelligence, The Dyre Wolf Campaign: Stealing Millions and Hungry for More, http://securityintelligence.com/dyre-wolf/, 2015
18 The Register, Nasty Dyre Malware Bests White Hat Sandboxes, http://www.theregister.co.uk/2015/05/04/dyre_malware_sandbox_evasion/, 2015
19 McAfee Labs Threat Report, Q1 2015, http://www.mcafee.com/nl/resources/reports/rp-quarterly-threat-q1-2015.pdf, 2015
20 Avast Blog, Tinybanker Trojan Targets Banking Customers of Major Banks Worldwide, https://blog.avast.com/2014/07/17/tinybanker-trojan-targets-banking-customers/, 2014
21 CSIS and Trend Micro Threat Report, Tinybanker: The Turkish Incident, http://www.trendmicro.nl/media/wp/tiny-banker-the-turkish-incident-whitepaper-en.pdf, 2012

Carberp

First encountered in 2010, Carberp was initially found to be only targeting Russian-speaking countries but was later modified to additionally target Western financial organisations[22]. The Carberp source code was leaked in June 2013.

Torpig

Torpig was originally developed in 2005 and was mainly active circa 2009. Torpig is installed on a system's Master Boot Record allowing it to execute before the operating system is launched making it harder for anti-virus software to detect[23]. Several European countries have active Torpig investigations however numbers are low and decreasing.



22 Symantec Official Blog, New Carberp Variant Heads Down Under, http://www.symantec.com/connect/blogs/new-carberp-variant-heads-down-under 2015

23 Carnegie Mellon University, Torpig, http://www.cmu.edu/iso/aware/be-aware/torpig.html

Shylock

Shylock first appeared in 2011 and used advanced 'Man-in-the-Browser' attacks to steal financial data and make fraudulent transactions. Shylock is a privately owned (by its creators) financial Trojan and as such its use and distribution is highly constrained. It is not available for purchase on underground markets[24]. Despite successful disruption activity, several EU Member States still report significant Shylock activity.

In July 2014, a UK-led operation resulted in the seizure of command and control (C2) servers and domains associated with the operation of a Shylock botnet consisting of 30 000 infected computers. The malware campaign had largely targeted customers of UK banks. The operation involved cooperation between several other jurisdictions, private sector companies and CERT-EU, and was coordinated by EC3 at Europol.

24 Symantec Official Blog, All That Glitters Is No Longer Gold – Shylock Trojan Gang Hit by Takedown, http://www.symantec.com/connect/blogs/all-glitters-no-longer-gold-shylock-Trojan-gang-hit-takedown, 2014

OTHER MALWARE THREATS – ENABLERS

Although the harm deriving from any malware attack is ultimately the result of one of the above mentioned attack methods, there are many other types of malware which facilitate or enable these attacks. These malware products are infrequently the main focus of law enforcement activity as it is the malware they enable that will spark an investigation. These enabling malware products are offered 'as-a-service' on the digital underground.

Exploit kits

Exploit kits are programs or scripts which exploit vulnerabilities in programs or applications to download malware onto vulnerable machines. Since the demise of the ubiquitous Blackhole exploit kit in late 2013, a number of other exploit kits have emerged to fill the vacuum. Some of the current, most widely-used exploit kits include Sweet Orange, Angler, Nuclear and Magnitude[25].

Spam

One of the most common methods of malware distribution is by malicious email attachment and the most productive way to reach the most potential victims is via spam. The primary function of some malware is to create botnets geared to generate large volumes of spam. One such example of such 'spamware' is Cutwail which has been known to distribute malware such as CTB Locker, Zeus and Upatre[26].

25 Trend Micro, Evolution of Exploit Kits, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf, 2015

26 Trend Micro Threat Encyclopedia, Cutwail, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/CUTWAIL, 2013

Droppers

The core function of some malware is simply, once installed, to download other malware onto the infected system. Malware such as Upatre is one such product and has been observed downloading malware such as Zeus, Crilock, Rovnix and more recently Dyre[27]. Upatre itself is commonly distributed via malicious email attachment distributed by botnets such as Cutwail.

In April 2015, Europol's EC3 and the Joint Cybercrime Action Taskforce (J-CAT), joined forces with private industry and the FBI to support Operation Source. This Dutch-led operation targeted the Beebone (also known as AAEH) botnet, a polymorphic downloader bot that installs various forms of malware on victims' computers. The botnet was 'sinkholed' and the data was distributed to the ISPs and CERTs around the world, in order to inform the victims.

OTHER MALWARE THREATS – MOBILE MALWARE

Industry reporting indicates that the volume of mobile malware continues to grow, although some reporting suggests that the rate of growth is decelerating[28] or that infection levels are even decreasing[29]. While it remains a recurring, prominent and contemporary topic in both industry reporting and the media, mobile malware currently does not feature as a noteworthy threat for EU law enforcement.

The majority of mobile malware is typically less malicious than its desktop counterpart. Although there is a growing volume of banking malware and trojanised financial apps on mobile devices, the majority of mobile malware is still from premium service abusers, i.e. those that subscribe victims or make calls to premium rate services. It is less probable therefore that a victim would feel the need to report an attack due to the relatively small losses incurred. Furthermore, victims are more likely to either reset their own device or take it to a phone repair shop, than they would be to take it to a police station. Reporting of this threat is therefore low and consequently the law enforcement response is minimal.

The following table highlights the threats posed by different malware variants reported to and/or investigated by EU law enforcement.

FUTURE THREATS AND DEVELOPMENTS

The recent experiences and investigative focus of European law enforcement suggests that the top malware threats of the last 5+ years are steadily in decline as a new generation of malware comes to the fore. Although some variants remain a threat, the investigation rates of Zeus (plus its variants Ice IX and Citadel), Torpig, Spyeye and Carberp have either plateaued or are in decline. Many of these products have had their development and support discontinued by the developer either voluntarily or as a result of their arrest. The continued threat posed by these products is likely due to their availability, with the source code for most publically leaked. Instead, newer names on the malware scene such as Dridex and Dyre are becoming more prominent in law enforcement investigations, a trend which is likely to increase.

A common and perhaps inevitable fate for any malware is to have its source code publically leaked, either by a rival criminal gang or by security researchers. Whilst this may be of tremendous benefit to the Internet security community it also puts the code into the hands of prospective coders allowing them to rework and enhance the code to create their own products with a large part of their work already done for them. As an example, a hybrid of the Zeus and Carberp Trojans, dubbed Zberp, was detected in mid-2014[30]. It is likely that, given the success and sophistication of many of the older malware products, we will continue to see new threats which draw on their code.

27 Trend Micro Threat Encyclopedia, Upatre, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/upatre, 2015

28 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015

29 Verizon, 2015 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2015/, 2015

30 Security Intelligence, Meet the Zberp Trojan, https://securityintelligence.com/new-zberp-Trojan-discovered-zeus-zbot-carberp/, 2015

Malware	Threat Level	Primary Function	Primary Infection Vector	Aliases/Variants	Trend
Cryptolocker	**HIGH**	Ransomware	Email attachment	-	▲
DarkComet	**HIGH**	RAT	Exploit kit	Fynloski, Fynlos, Krademok,DarkKomet	▲
Dridex	**HIGH**	Data Stealer	Email attachment (Word macros)	Bugat,Feodo, Cridex	▲
Zeus	**HIGH**	Data Stealer	Exploit kit	Zbot, Gameover (GOZ)	◆
Blackshades	**HIGH**	RAT	Exploit kit	-	▼
Citadel	**HIGH**	Data Stealer	Exploit kit	-	▼
SpyEye	**HIGH**	Data Stealer	Dropper	-	▼
CTB-Locker	**MEDIUM**	Ransomware	Email attachment (.zip)	Critroni	▲
Dyre	**MEDIUM**	Data Stealer	Dropper (UPATRE)	Dyreza	▲
Tinba	**MEDIUM**	Data Stealer	Exploit kit	Tinybanker, Zusy	▲
Carberp	**MEDIUM**	Data Stealer	Exploit kit	-	◆
Shylock	**MEDIUM**	Data Stealer	Exploit kit	Caphaw	◆
Ice IX	**MEDIUM**	Data Stealer	Exploit kit	-	▼
Torpig	**MEDIUM**	Data Stealer	Exploit kit	Sinowal, Anserin	▼

Similarly newly published vulnerabilities are rapidly incorporated into exploit kits. This often occurs faster than patches can be released and almost certainly quicker than most potential victims would update their software. As an example, the Zero-Day exploits which were released as a result of the Hacking Team exposure in June 2015 appeared in the Angler, Neutrino and Nuclear exploit kits within days[31].

As more consumers move to mobile devices for their financial services (banking, mobile payments, etc) the effectiveness and impact of mobile malware will increase. It can therefore be expected to begin to feature more prominently on law enforcement's radar.

One advanced technique that we can expect to see further future examples of is the use of 'information hiding' methods such as steganography. Rather than simply encrypting data so that it is unreadable, such techniques hide data within modified, shared hardware/software resources, inject it into network traffic, or embed it within the structure of modified file structures or media content. Malware employing these techniques can, for example, stealthily communicate with C2 servers or exfiltrate data. It may therefore become increasingly difficult to detect malware traffic if such methods become more widely employed. Smartphones may be particularly vulnerable to such malware as, coupled with their array of in-built sensors, they provide additional channels via which hidden data can be transmitted[32].

RECOMMENDATIONS

- In order to maintain the trend of successful multi-jurisdictional operations targeting cybercrime groups, law enforcement should continue to:
  - Pro-actively share criminal intelligence related to cybercrimes with other EU Member States via Europol;
  - Build and maintain relationships with private industry and academia with expertise and capability in Internet security and cybercrime;
  - Contribute malware samples to the Europol Malware Analysis System (EMAS).
- While a focus on the apprehension of the groups and individuals behind malware campaigns is recommended, consideration should also be given to targeting shared criminal infrastructure which may have a disruptive impact on multiple OCGs carrying out a range of attacks and may increase their cost of operation.
- Where the capacity and capability exists, law enforcement should target criminal groups developing and distributing enabling malware such as exploit kits, spamware and droppers.
- While dismantling or disrupting criminal groups is effective and necessary, adequate resources should be given to prevention strategies in order to raise awareness of cybercrime and increase standards in online safety and information security. This must include awareness in relation to mobile devices.

31 Trend Micro Security Intelligence Blog, Hacking Team Flash Zero-Day Integrated into Exploit Kits, http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/, 2015

32 Mazurczyk, W., Luca Caviglione, L.; Information Hiding as a Challenge for Malware Detection. IEEE Security & Privacy, 2015

ONLINE CHILD SEXUAL EXPLOITATION

Online child sexual exploitation (CSE) is a constantly evolving phenomenon, shaped by developments in technology, growing levels of Internet adoption via territorial coverage and bandwidth, and further expansion of mobile connectivity.

The key threat areas include criminal activities in P2P environments and the Darknet, live streaming of child sexual abuse, sexual extortion, and developments in the commercial distribution of child abuse material (CAM). Focus will also be on the offender environments and threats relating to the growing level of competence amongst offenders in terms of networking and technical capability, use of encryption and anonymisation tools as well as the abuse of hosting services for distributing CAM.

Some of these areas were already reported in the 2014 IOCTA; they still remain the main challenges, even if there were no significant developments over the last year.

KEY THREAT – P2P ENVIRONMENT

P2P file sharing methods remain the main platform to access child abuse material and the principal means for non-commercial distribution. These are invariably attractive for CSE offenders and easy to use. They are a highly effective and efficient means of building and rebuilding a collection quickly after accidental loss or apprehension.

Some specialists describe the material which is being shared there as known and often dated. However, P2P is an important part of a possible offending pathway, from open searching using search engines, via exchanges on the open Internet to the hidden services in the Darknet.

This environment is also – due to its nature – deemed to be the one where the greatest volume of offending is identified. P2P cases still constitute the majority of investigations conducted by specialised units.

Some specialists noted a slight shift of users of hidden services to P2P environments as a result of recent successful LE interventions. While it is impossible to confirm such observations by reliable quantitative data, it perfectly supports an assumption that current online distribution of CAM is very dynamic, and the operations of LE agencies inevitably influence the extent of misuse of particular environments.

KEY THREAT – THE DARKNET

Criminals who are present on the Darknet appear more comfortable offending and discussing their sexual interest in children than those using the Surface Web. The presumed greater level of anonymity and strong networking may be favouring their sexual urges, which would not be revealed in any other environment lacking such features.

The use of use of Tor in the proliferation of CAM remains a key threat, regardless of some loss of trust about its complete anonymity and technical limitations.

Restricted areas of Tor pose the highest risk to children as they are linked to the production of new CAM to retain community membership and status, which inevitably leads to further hands-on abuse. It is likely that more abuse of an extreme and sadistic nature is being requested and shared in these areas.

KEY THREAT – LIVE STREAMING

The live streaming of abuse[33] is no longer an emerging trend but an established crime, the proliferation of which is expected to further increase in the near future. Child sexual abusers continue to exploit technology that enables the streaming of live images and video in many different ways. This includes use of live streaming methods in sexual extortion cases, organising invitation-only videoconferencing of contact abuse among members of closed networks, as well as the trend reported in 2014 concerning the profit driven abuse of children overseas, live in front of a camera at the request of Westerners[34].

33 Live-distant child abuse (LDCA) is a term suggested by specialists to underline the fact of sexual abuse even if physical contact between an offender and a victim does not take place

34 Europol, IOCTA 2014, https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-IOCTA, 2014

The low cost to consumers of pay-per-view child sexual abuse makes it possible to order and view the abuse regularly without the need for downloading. This represents a significant driver for such a modus operandus to become even more widespread. The frequent small amounts of money being transferred through intermediaries minimises any red flags from financial transaction monitoring agencies[35].

Recently, some intelligence strengthened the connection between live streaming and hands-on abuse, where live-distant abuse is followed by travel to another country to contact abuse the same children.

KEY THREAT – ONLINE SOLICITATION AND SEXUAL EXTORTION

The last few years have witnessed changes in the online distribution of self-generated indecent material (SGIM) produced by young people, much of which is distributed through mobile devices and social media platforms. Although intended to be shared with trusted partners, there is the potential for such material to be captured and distributed among CSE offenders if it is later placed on the open Internet.

SGIM can also be acquired by offenders through online solicitation, often combined with grooming, where children are offered money or gifts in exchange for complying with the desires of the offender. Using mobile devices or webcams to record the media, a victim is lured into sending photos or videos to the abuser, who may also pretend to be a teenager. Voluntary involvement, however, frequently turns into involuntary participation as the abuser turns to coercive measures to obtain valuable new material.

In the most extreme cases online solicitation may turn into sexual extortion, where victims are threatened by disseminating indecent materials depicting them and have to comply with offender demands, leaving them with psychological damage and increasing the potential for self-harm or suicide attempts. Such modus operandi reflects the general trend towards more extreme, violent or degrading demands where coercive techniques are adopted.

As a methodology, business models based on blackmailing young people may also be attractive to those who are not sexually interested in children but seek financial gain. Although such crimes are not primarily aimed at minors, it is likely that children (below the age of 18 years) may be among its victims, and may experience serious psychological damage. Cybercrime groups running such schemes are known to operate out of north-west African states and south-east Asia.

KEY THREAT – COMMERCIAL DISTRIBUTION

There is a need to widen the understanding of the current scope of online commercial CAM distribution. It is necessary to acknowledge that new CAM can be a currency in itself. The value of an image is its novelty which is likely to define the means of its circulation. This needs to be differentiated from instances of obtaining financial gain from distribution of CAM.

A full understanding of the commercial distribution of CAM requires taking into account all forms of commercial activity involving its distribution, not only the 'traditional model' of dedicated websites offering such material on the open Internet. This includes new methods for distributing CSE such as 'disguised websites'[36], dissemination through cyberlockers, live streaming of child sexual abuse for payment as well as instances of commercial CSE in the Darknet. Additionally, a continuation of migration from traditional payment mechanisms to those offering a greater degree of anonymity, particularly pseudonymous payment systems[37] such as Bitcoin, has been observed. Commercial distribution exists, and is evolving. This is despite the producer's perception that financial flows may compromise their security.

35 EFC Strategic Assessment 2014, https://www.europol.europa.eu/content/live-streaming-child-sexual-abuse-established-harsh-reality, 2015

36 The disguised websites' present different content depending on the route the user takes to reach them. When the URL is loaded directly into the browser, the page which loads contains legitimate adult content. However, when accessed via a particular gateway site ('referrer') the page displays child sexual abuse content. IWF Annual report 2013

37 ICMEC, The Digital Economy, http://www.icmec.org/en_X1/ICMEC_Digital_Economy.pdf, 2014

The traditional distinction between commercial and non-commercial distribution, which cast the former as largely profit driven and conducted by those with limited sexual interest in children, is no longer as obvious. It is weakened by the fact that offenders with a sexual interest in children who produce and distribute CAM are becoming entrepreneurial, exploiting developing technologies[38].

KEY THREAT – NETWORKING AND FORENSIC AWARENESS OF CSE OFFENDERS

CSE offenders continue to exploit currently available technology, coupled with anonymous networks to hide their activities from LE attention. Increasingly user-friendly Internet-related technologies provide access to a variety of services they can feel comfortable and secure with. It is likely that some of them will make use of more than one route to access CAM simultaneously.

The use of techniques such as anonymisation, encryption and anti-forensic tools, such as 'wiping' software or operating systems (OS) run from removable media, are now considered the norm rather than the exception.

Communities of offenders mature and learn from the mistakes of those that have been apprehended by law enforcement, becoming more difficult to infiltrate. This is believed to refer more specifically to the users of the Darknet, who continue to develop trusted relationships and share relevant technical expertise. Offenders have also vacated Hidden Wiki, the Darknet's most popular directory of hidden services, in an effort to keep their profile low. Presumptions of safety, strengthened by the perception of anonymity and strong support from a like-minded community, influence an offender's behaviour and are likely to be reinforcing factors in an individual's offending pathway.

CSE offenders continue to misuse legitimate hosting possibilities to store and distribute CAM. According to INHOPE records, in 2014 the total number of unique URLs confirmed to contain CAM and inserted into their reporting system was 83 644 (48 910 in 2013 and 33 821 in 2012). In 2014 the top hosting countries were United States (37% of identified CAM), Russian Federation (24%), Netherlands (16%) and Canada (11%). Image hosting sites were identified as hosting 42% of the reported URLs (an increase from 22% in 2013), followed by website hosting – 30% (37% in 2013) and file hosting sites – 20% (29% in 2013)[39].

FUTURE THREATS AND DEVELOPMENTS

Historically, CSE offenders were commonly located and identified as a result of their true IP address being revealed during an investigation. These could then be used to obtain subscriber's details from ISPs. The invalidation of the Data Retention Directive in May 2014 was replicated in several EU Member States and will increasingly stand as a barrier to the success of future CSE investigations.

In February 2015, a report passed to US liaison officers at Europol from the US National Center for Missing and Exploited Children (NCMEC) prompted an investigation by EC3's FP Twins. Swift cooperation with the Romanian authorities resulted in the arrest of the offender and the rescue of his 22-month old daughter from further abuse.

The development and use of technologies which complicate traditional police methods of identification of online CSE offenders is likely to continue. It is expected that the link between online content and user will be less visible as a consequence of using anonymising tools, encryption and the remote storage of data. Increasing Internet coverage through broadband and 4G in developing countries will result in live-distant child abuse becoming more widespread, leading to a growing multitude of unknown victims and complicated investigations requiring close cooperation with LE outside the EU.

The further professionalisation of criminal activities on the Darknet, including the evolution of online markets and alternative payment methods, may be leading to the facilitation of illicit payments for novel CAM. Criminals offering commercial live streaming of CAM may also adopt decentralised streaming

38 EFC Strategic Assessment 2014, https://www.europol.europa.eu/content/live-streaming-child-sexual-abuse-established-harsh-reality, 2015

39 INHOPE Statistics 2014, http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2014.aspx, 2014

solutions with built-in payment systems[40] instead of centralised commercial products.

The noticeable online proliferation of SGIM corresponds with the increased online presence of children and teenagers. According to a recent media use survey in the UK, children aged 5-15 spend 12.5 hours online per week. 41% own a mobile phone, which are increasingly capable of accessing the Internet. Ownership of tablets in this age group has almost doubled – growing from 19% in 2013 to 34% in 2014[41]. This trend will most probably increase, and with it the exposure of children to potential threats on the Internet.

It is safe to assume that emerging technologies such as virtual reality headsets, combined also with advancements in other fields such as artificial intelligence, will be adopted for adult entertainment as well[42,43,44].

The adult entertainment industry is a key driver for the adoption of media formats and emerging technologies, and it is therefore likely that such content will find its way to one of the developing virtual reality platforms, allowing for a high degree of immersion and interactivity. This technology may also be abused by CSE offenders to simulate child abuse virtually, although the legal implications of this are unclear[45].

40 Cryptocoinsnews.com, https://www.cryptocoinsnews.com/streamium-decentralizes-streaming-content-producers-get-paid-bitcoins-real-time/, 2015

41 Ofcom, Children and Parents: Media Use and Attitudes Report, http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-use-attitudes-14/Childrens_2014_Report.pdf, 2014

42 The Register, Virtual Reality Porn on the Rift? 'Why not?' Says Oculus Founder, http://www.theregister.co.uk/2015/05/20/vr_pornography_on_the_rift_oculus_founder_says_sure_why_not/, 2015

43 Gizmodo, The Next Oculus Rift Might Let You See Your Actual Hands in VR, http://gizmodo.com/the-next-oculus-rift-might-let-you-see-your-actual-hand-1718371825, 2015

44 SingularityHub, The Future of Sex: Androids, VR, and the Orgasm Button, http://singularityhub.com/2009/05/20/the-future-of-sex-androids-vr-and-the-orgasm-button/, 2009

45 BBC News, Second Life 'child abuse' Claim, http://news.bbc.co.uk/2/hi/technology/6638331.stm, 2007

RECOMMENDATIONS

- EU law enforcement must not only ensure they are familiar with emerging trends, technologies and methodologies used in CSE online, but extend their expertise and experience to jurisdictions that require capacity building and additional support.
- Cooperation with both reporting bodies as well as content service providers is essential. The marked increase in the abuse of hosting services requires its providers to introduce procedures for identifying and mitigating distribution of CAM.
- The relationship between the production of SGIM online and CSE remains unclear and merits additional research. Tailor-made prevention activity resulting in a greater awareness of online threats is vital to reduce the threat of online grooming and solicitation.
- Law enforcement should focus on identifying and dismantling the communities and forums in which offenders congregate as these drive the demand for fresh CAM leading to the abuse of new victims.
- Effectively investigating CSE in closed like-minded offender communities requires relevant legal instruments allowing undercover work and the efficient use of traditional policing investigation methods.
- In order to counter the increasing occurrence of encryption used by offenders, law enforcement should invest in live data forensics capability and prioritise the seizure of devices in situ when arresting suspects, to capture the relevant artefacts in an unencrypted state.
- There is a need to constantly enhance victim identification strategies. Resources spent on the efficient use of available Victim ID databases, taking into account current and future efforts undertaken by EC3 and Interpol in this field, as well as detailed analysis of the material, often lead to successful rescue operations.

PAYMENT FRAUD

In 2013, the number of payment cards issued in the EU reached approximately 760 million, representing approximately 1.5 payment cards per capita, while the number of transactions reached EUR 43.6 billion averaging at almost EUR 50 per transaction[46]. The growing proportion of non-cash payments has encouraged an arms race between new attack methods devised by entrepreneurial cybercriminals and the countermeasures and security features implemented by the card industry to protect their customers and business.

In 2013, the total value of fraudulent transactions conducted using cards issued within SEPA[47] reached EUR 1.44 billion, representing a growth of 8% on the previous year. The growth was driven by a 20.6% increase in card-not-present (CNP) fraud. Of the total fraud value, 66% of value resulted from CNP payments, 20% from point-of-sale (PoS) transactions and 14% from transactions at ATMs[48].

KEY THREAT – SKIMMING

In the last year, only three Member States indicated an increase in the number of investigations into the skimming of payment cards at ATMs. All three instances related to Eastern European countries while in Western Europe the trend has either plateaued or is in decline. Overall, both PoS skimming and attacks via PoS network intrusion are in downturn across the majority of jurisdictions.

Skimmers continue to refine their tools with notable developments in miniaturisation and concealment techniques. Skimming devices are now often sufficiently small that they can be embedded inside the card readers, rendering them invisible to users.

Although ATM-related fraud incidents within the EU decreased by 26% in 2014, overall losses were up 13%[49]. This is mainly due to the cashing out of compromised cards in jurisdictions outside of the EU where EMV (chip and pin) protection has not yet been fully implemented, mainly the Americas and Southeast Asia – Indonesia and the Philippines in particular. Some OCGs set up permanent bases in these locations to facilitate their activities[50].

In 2014, EU-funded **Project Sandpiper** *resulted in 59 arrests in addition to the disruption of five organised crime groups exploiting electronic payments. Over 50 000 compromised cards were recovered, worth over EUR 30 million. The project involved UK and Romanian law enforcement and was supported by Europol's EC3.*

KEY THREAT – ATM MALWARE

There are several common malware-focused methods for attacking ATMs: [51]

- **Software skimming** malware, once installed on the ATM PC, allows the attacker to intercept card and PIN data at the ATM;
- **Jackpotting** is a technique which uses malware to take control of an ATM PC in order to direct the cash dispenser to dispense money;
- **Black Boxing** is a Jackpotting variant where the attacker uses their own PC to communicate with the cash dispenser to direct it to dispense cash;
- **Man-in-the-Middle attacks** manipulate communication between the ATM PC and the merchant acquirer's host system and can, for example, trigger requests to withdraw money without debiting the card account. The malware must however be present in a high software layer of the ATM PC or within the acquirer's network.

46 European Central Bank: Payment Statistics for 2013, https://www.ecb.europa.eu/press/pdf/pis/pis2013.pdf, 2014
47 As of July 2015, SEPA consists of all 28 EU MS as well as Iceland, Liechtenstein, Monaco, Norway, San Marino and Switzerland
48 European Central Bank: Fourth Report on Card Fraud, https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf, 2015
49 European ATM Security Team (EAST), European ATM Crime Report, 2015
50 Input provided by FP Terminal
51 Europol, Guidance and Recommendations regarding Logical Attacks on ATMs, 2015

Many of these attacks can potentially be prevented through a mix of security/technical measures such as securing the BIOS, disabling booting from external drives, hardening OS or equipping ATMs with alarm systems. Non-technical mitigation methods include limiting physical access to ATMs, surveillance and more frequent refilling cycles[52].

KEY THREAT – CARD-NOT-PRESENT (CNP) FRAUD

Payment card data are actively traded on criminal marketplaces and automated card shops. Bulk card data can be purchased cheaply, allowing re-sellers to profit from redistributing the card data in smaller, more refined batches. 'End users' of compromised card data (i.e. those committing CNP fraud) can purchase high value products and use criminal drop and reshipping services to receive their fraudulently obtained goods. These can then either be retained for personal use or monetised via buy-and-sell websites. In some cases this process is carried out by highly organised and experienced groups.

The majority of Member States have witnessed a shift towards CNP fraud as a result of the availability of compromised payment card details stemming from data breaches, social engineering attacks and data stealing malware. Another push towards online fraud is the success of law enforcement in targeting OCGs involved in card-present (CP) fraud, as well as the implementation of effective measures against CP fraud by the financial industry, including EMV, anti-skimming ATM slots and geoblocking.

According to card scheme operators Visa and Mastercard, 67%[53] and 69%[54] of losses respectively in 2014 occurred as a result CNP fraud, including online, postal and telephone orders. Often, however, incidents are reported at a local level, with crime data not collated at a national level. Moreover if this is then not shared at an international level, the linking of related crimes across multiple jurisdictions in order to initiate coordinated international investigations becomes problematic.

Following the successful Airline Action Days operations supported by EC3, Hellas (Greece) has implemented a national initiative to fight airline fraud on an ongoing basis and in close cooperation with airline companies, travel agencies and international airports. Notifications on possible fraudulent transactions using payment cards are channelled through the Cyber Crime Division of the Hellenic Police where they are collated and analysed, leading to the arrest of fraudsters at the boarding gate. The measures have proved to be highly effective; of the suspects identified via a fraud notification, 52% have been arrested, 35% haven't showed up at the airport and 13% have made their flight due to no confirmed fraud.

Proper implementation of 3D Secure[55] and rigid internal anti-fraud procedures could mitigate this threat to some degree. However, some merchants, fearing the loss of customers who dislike having their shopping experience complicated, have instead demonstrated a preference to absorb the losses and invested little effort into tackling online fraud through implementing fraud screening technologies and secure e-commerce solutions.

FUTURE THREATS AND DEVELOPMENTS

The use of 3D printing to produce customised skimmers has already been documented in five EU countries and we are likely to see a progressive development in this area. The ATM skimming devices that used to be produced and distributed within organised crime groups are now traded on legitimate buy-and-sell websites, increasing their availability and convenience for the criminal customers. 3D printing will further lower the bar of entry into the crime, as offenders will increasingly trade schematics for the devices or share these on P2P networks.

The migration to EMV technology in the USA is expected to occur in autumn 2015, as merchants will be liable for losses from 1 October 2015. Similar initiatives are scheduled over the next two years in many other countries where criminals take advantage of a lack of EMV technology to abuse compromised cards. This is expected to lead to a significant decrease in skimming.

52 Europol, Guidance and Recommendations regarding Logical Attacks on ATMs, 2015

53 Visa Europe 2014 Annual Report, http://annualreport.visaeurope.com/Risk-management/index.html, 2015

54 Data provided to EC3 by MasterCard, 2015

55 3D Secure is an online fraud prevention measure familiar through Verified by Visa or MasterCard SecureCode

While there has been a lot of discussion regarding the security of emerging mobile and contactless payments, their rapid growth has not yet led to a notable increase in related fraud. According to Visa Europe, the fraud-to-sales ratio for contactless transactions remains at 0.01%[56]. This is mirrored by law enforcement experience across Europe, with almost all Member States assessing the current threat level for mobile and contactless payment fraud as low to non-existent. However, as EMV technology is further adopted globally and options for card-present fraud diminish, we can perhaps expect growth in this area of fraud.

Several ATM manufacturers have previously proposed fingerprint and face recognition systems on ATMs in order to increase ATM security. Earlier this year, the world's first fully functional ATM equipped with facial recognition was unveiled in China, having its biometric authentication based on facial feature and iris recognition[57]. Whether this turns out to be a failure or a milestone in the development of ATM authentication remains to be seen.

Successful initiatives that bring together law enforcement and the private sector in order to combat industry related threats and often previously under-represented crime areas are becoming increasingly common and growing in impetus. As such initiatives expand in scope and scale, law enforcement will require increased capacity to deal with what is already a high volume crime.

Europol's e-commerce initiative brings together stakeholders in e-Commerce, law enforcement, logistics companies and payment card schemes in a collaborative effort to identify, arrest and prosecute the most prolific criminals involved in using compromised payment cards for fraudulent online purchases and those involved in the receipt and reshipping of fraudulently obtained goods.

56 Visa Europe 2014 Annual Report, http://annualreport.visaeurope.com/Risk-management/index.html, 2015

57 The Telegraph, China Unveils World's First Facial Recognition ATM, http://www.telegraph.co.uk/news/worldnews/asia/china/11643314/China-unveils-worlds-first-facial-recognition-ATM.html, 2015

RECOMMENDATIONS

- Law enforcement should seek to actively engage in multi-stakeholder initiatives such as Europol's Airline Action Days and E-commerce initiative in order to combat payment fraud in their jurisdiction.
- EU Member States should take advantage of the Europol Malware Analysis System (EMAS) by submitting samples of ATM and PoS malware in order to cross-reference them against those supplied by other Member States, and identify potential links to ongoing investigations.
- To mitigate the risk of ATM malware attacks, law enforcement should promote Europol's 'Guidance and Recommendations regarding Logical Attacks on ATMs', at a national and international level, to banking and payments industry contacts.
- To combat the sale and abuse of compromised card data, law enforcement should focus on targets either running carding websites or active traders on those sites, particularly those who offer large numbers of recently compromised cards and have a long and successful transaction history.
- A concerted effort is required to collate data at a national and international level in order to identify the activity of OCGs involved in multi-jurisdictional payment card fraud.
- Law enforcement requires a common secure channel through which they can pass details of compromised card and account details discovered through the course of their investigations to partners in financial institutions and payment card schemes in order to prevent their subsequent use in fraud.
- Law enforcement should engage with providers of content sharing websites abused by criminals to sell or distribute compromised card data, to promote automated mechanisms for the removal of criminal content[58].
- Law enforcement requires the tools, training and resources to deal with high volume crimes such as payment card fraud.
- Following the adoption of EMV technology in previously non-compliant jurisdictions, law enforcement and the payment industry should work together in order to predict where card-present fraud will migrate to and try to ensure that adequate prevention measures are in place.

58 Lenny Zeltser, The Use of Pastebin for Sharing Stolen Data, https://zeltser.com/pastebin-used-for-sharing-stolen-data, 2015

SOCIAL ENGINEERING

No matter how many resources a company spends on securing their networks and systems, they cannot fully prepare or compensate for what is often the weakest link in their security – the human factor. Without (or even with) adequate security awareness training, a lapse in judgement on behalf of an employee can leave a company open to attack.

Social engineering attacks are epitomised in advanced fee fraud (also known as 419 fraud). Increasing Internet access in developing countries has led to higher numbers of innovative yet technically unskilled attackers with access to a greater number of victims.

Social engineering has developed into one of the most prevalent attack vectors and one of the hardest to defend against. Many sophisticated and blended attacks invariably incorporate some form of social engineering. Targeted spear-phishing attacks were identified as a growing trend in 2014 and two-thirds of cyber-espionage incidents have featured phishing[59].

KEY THREAT – PHISHING

Almost all Member States indicated that the amount of phishing has either stabilised or increased in their jurisdiction in 2014. This trend was substantiated by financial institutions where almost every major business indicated that it was targeted by a phishing campaign. Incidents of smishing and vishing throughout the sector have seen an upward trend as well.

Additional security measures adopted by banks have become increasingly successful in identifying fraudulent transactions related to phishing attacks although this in itself has resulted in increased costs due to investment into proactive monitoring capability. As a result of these proactive measures, some institutions noted a decrease in the number of phishing attacks for high-value transfers and have observed fraudsters moving to high-volume low-value based attacks instead.

Phishing traditionally occurred on a larger scale in widely spoken languages such as English. Phishing attacks often originate from countries sharing the same language (e.g. French victims targeted by offenders from French-speaking North African countries). Nevertheless, some smaller EU countries have also observed a notable increase in localised phishing. The quality of phishing has increased over the last few years due to professional web design and translation services.

While companies can invest in increased ICT security which in turn requires criminals to innovate their own technical capability, it is harder to upgrade the "human firewall" [60]. Training in cybersecurity awareness can be provided and safe practice encouraged but is harder to enforce. Each employee may represent a unique fallibility in the overall security. The overall effectiveness of phishing campaigns, which was formerly 10-20%, increased in 2014. Research shows that 23% of recipients who receive a phishing messages will open it and a further 11% will continue to open any attachments[61].

59 Verizon, 2015 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2015/, 2015

60 McAfee, Hacking the Human Operating System, https://community.mcafee.com/docs/DOC-7035, 2015

61 Verizon, 2015 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2015/, 2015

For untargeted attacks, the primary way to distribute phishing emails is via spam. The overall volume of spam has continued to decline over the last few years, dropping to 28 billion spam messages per day in 2014. In June 2015, the overall spam rate fell below 50%; the lowest rate since September 2003[62]. Taking into account overall increases in malware and phishing, it is safe to assume that attackers are gradually shifting their activities to alternative distribution channels such as social media.

In 2014, Dutch and Belgian law enforcement authorities, in cooperation with the EC3 and Eurojust, arrested 12 suspected members of a European voice-phishing ring, seizing their infrastructure and other assets. The group conducted phishing and vishing which purported to originate from financial institutions in an attempt to trick their victims into handing over credentials necessary to perform bank transactions, including one-time passwords generated by the authenticator provided by the bank.

KEY THREAT – CEO FRAUD

Several member countries as well as financial institutions reported an increase in CEO fraud which is now leading to significant losses for individual companies. The modus operandi for such frauds involves an attacker impersonating the CEO or CFO of the company. The attacker will contact an employee targeted for their access and request an urgent transaction into a bank account under the attacker's control. The request may be channelled via email or telephone. Subsidiaries of multinational companies are often targeted, as employees working for regional cells do not usually personally know senior management in the holding company and may be fearful of losing their job if they do not obey their ultimate boss. The scam does not require advanced technical knowledge as everything the attacker needs to know can be found online. Organisation charts and other information available from the company website, business registers and professional social networks provide the attacker with actionable intelligence.

62 Symantec Intelligence Report June 2015, http://www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-06-2015.en-us.pdf, 2015

FUTURE THREATS AND DEVELOPMENTS

As consumers continue to shift much of their online activity to mobile devices, this opens up additional attack opportunities and strategies to enterprising cybercriminals. Mobile phones already provide SMS as an additional contact method, while the growing volume of communication and social networking apps provide further access to potential victims. Smaller, more compact screen sizes and reduced readability increase the likelihood of potential victims inadvertently clicking on a link. We can therefore expect to see the number of social engineering attacks via mobile devices and social media platforms to increase.

In 2014 there was widespread concern that the cessation of support for the still widely-used Microsoft XP operating system would lead to a fresh wave of scams from fraudsters purporting to represent Microsoft support. In 2015, Microsoft released its free upgrade to Windows 10. Although Microsoft has taken precautions to mitigate potential exploitation of this event by notifying customers directly through their current OS, it is still likely that criminals will take advantage of this opportunity to target unsuspecting victims.

In 2016 Brazil will host the thirty-first Olympic Games. As with any sporting event of this scale it can be expected that there will be a notable increase in phishing and other social engineering attacks attempting to exploit both businesses and citizens in relation to the games.

RECOMMENDATIONS

- It is necessary to develop an efficient, fit-for-purpose reporting mechanism covering a range of social engineering offences. Online reporting channels are considered to be especially suitable for high-volume incidents of a minor nature.
- While social engineering attacks are scalable, law enforcement resources are not. Law enforcement should therefore continue to share information with and via Europol in order to identify the campaigns which are having the greatest impact, thereby allowing law enforcement to manage its resources more effectively.
- Where the capacity and capability exists, law enforcement should target criminal groups providing enabling services such as spam which supports many aspects of cybercrime including social engineering attacks and phishing.
- Where it is not possible to identify or arrest individuals, law enforcement should focus on disrupting or dismantling the criminal infrastructure which may be supporting multiple types of criminality.
- Law enforcement should establish and maintain working relationships with both global and national webmail providers to promote the lawful exchange of information relating to criminals abusing those services.

DATA BREACHES AND NETWORK ATTACKS

The scale of the Target data breach of late 2013 made it one of the largest data breaches in history, affecting up to 40 million customers[63]. However, it turned out to only be the first of a series of significant breaches that earned 2014 the title of "Year of the data breach" across a variety of industry and media reporting.

In the 2014 IOCTA it was highlighted how a lack of reporting hindered law enforcement from mounting a suitable response to network intrusions, with industry preferring (where possible) to allow the incident to be handled by private security companies. Since then however, there has been a clear increase in the level of reporting to and subsequent involvement of law enforcement in such investigations.

Almost 75% of Member States indicated that they had investigated some form of data breach or network intrusion, with almost half of Member States running 10 or more distinct investigations. Over one third of EU law enforcement agencies identified network intrusions as an increasing threat.

Not all network intrusions lead to the leakage of data or theft of intellectual property. The defacement of business or private websites was one of the most commonly reported cyber-attacks within EU law enforcement. It was also noted that there is an increasing number of these attacks with a terrorist context. The 2015 Verizon Data Breach Investigation Report (DBIR)[64] identified that in 70% of attacks where the motive could be established, a breach occurs with the intention of instigating further attacks on secondary victims. For example, using a hacked server for hosting malware or phishing.

Nevertheless 2015 has already witnessed a number of significant data breaches. In May and July respectively, adult hookup websites AdultFriendFinder and AshleyMadison[65], an allegedly discreet website for those seeking extra-marital affairs, were hacked. Both leaked personal and sensitive details related to millions of their customers, leaving them vulnerable to extortion and social engineering attacks. AshleyMadison's clientele were largely North American, however AdultFriendFinder had approximately 3.5 million customers worldwide. The proportion of these within Europe is unknown, therefore the impact of these breaches on European citizens may never be fully appreciated. However over 1400 customers were identified as senior executives of Fortune 500 companies[66], over one fifth of which are based within Europe. It is therefore safe to assume that European citizens feature amongst those who have had their personal details disclosed.

The table beside identifies some of the more prominent publicised data breaches from the first half of 2015 which originated from within, or which are believed to impact, the EU[67]. The number of breaches apportioned to each country is at least partly representative of the stringency of the reporting regulations within that jurisdiction.

The majority of data breaches occurred as a result of compromised credentials (typically those with administrator rights), with the rest largely made up of phishing attacks and, in the case of industries using point-of-sale (PoS) terminals, RAM scraping. Broken down differently, 25% of breaches were as a result of crimeware, 20% the result of insider misuse and 15% as a consequence of physical theft or loss. Almost one third were additionally as a result of miscellaneous human errors, such as sending sensitive information to the wrong recipient or accidentally publishing sensitive data to public servers[68].

63 LowCards, 40 Million Card Accounts Affected by Security Breach at Target, http://www.lowcards.com/40-million-card-accounts-affected-security-breach-target-21279, 2015
64 Verizon, 2015 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2015/, 2015
65 Krebs on Security, Online Cheating Site AshleyMadison Hacked, http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/, 2015
66 International Business Times, John McAfee, Is the AdultFriendFinder Hack a Major Threat to National Security?, http://www.ibtimes.co.uk/john-mcafee-adult-friendfinder-hack-major-threat-national-security-1504070, 2015
67 Breach Level Index, http://www.breachlevelindex.com/, 2015
68 Verizon, 2015 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2015/, 2015

Organisation	Industry	Country	Source of breach	Records compromised	Data compromised
Talk Talk	Telecoms	UK	Malicious outsider	4 000 000	Name, address, telephone numbers, account number
AdultFriendFinder	Other	Global	Malicious outsider	3 800 000	Name, DOB, email address, gender, location, sexual orientation
Moonpig Ltd	Technology	UK	Accidental loss	3 600 000	Name, address, partial card details
Vivanuncios	Technology	UK	Malicious outsider	2 000 000	Username, email address
TV Channel MyTF1	Media	FR	Malicious outsider	1 900 000	Name, address, email, password
Scout Association	Other	UK	Accidental loss	450 000	Unknown
MAPP.NL	Retail	NL	Malicious outsider	157 000	Email address, encrypted password
French State TV	Media	FR	Malicious outsider	108 000	Name, address, email address, phone number
Army & Airforce Exchange (Siga Telecom)	Government	DE	Malicious outsider	98 000	Address, email, phone number
World Trade Organization	Financial	Global	Hacktivist	53 000	Name, DOB, email address, phone number, login credentials, job details
CISI	Financial	UK	Malicious outsider	40 000	Name, email address
Temporis	Other	FR	Malicious outsider	24 000	Email, password
British Airways	Transportation	UK	Malicious outsider	10 000	Unknown
PaymyPCN.net	Other	UK	Malicious outsider	10 000	Name, address, photograph, email

DDOS ATTACKS

Approximately half of the Member States highlight Distributed Denial of Service (DDoS) attacks as a considerable threat. This is confirmed by security industry reports documenting hundreds of DDoS attacks per day[69]. So far in 2015, several of the attacks have exceeded 100 Gigabits per second while even attacks which are an order of magnitude smaller, may already cause availability issues for many hosts. Three-quarters of attacks last less than four hours, suggesting that this is sufficient time for an attacker to either achieve their goal or to realise their attack was successfully mitigated[70]. Also, opportunity costs or rental fees prevent those who own or rent the botnet from prolonged attacks.

DDoS extortion attacks have become a well-established criminal enterprise. These attacks further benefit from availability of DDoS capable malware and increasing popularity of

69 Kaspersky, DDoS Intelligence Report Q2 2015, https://securelist.com/analysis/quarterly-malware-reports/71663/kaspersky-ddos-intelligence-report-q2-2015/, 2015

70 Kaspersky, DDoS Intelligence Report Q2 2015, https://securelist.com/analysis/quarterly-malware-reports/71663/kaspersky-ddos-intelligence-report-q2-2015/, 2015

pseudonymous payment mechanisms. One of the most evident personifications of the threat is a group called DD4BC (DDoS for Bitcoin) emerging in early 2015. Their ransoms range between 1 and 100 Bitcoins, depending on the perceived financial standing of the victim and their willingness to comply with the attacker's instructions. To increase the credibility of their claim, the group often launches a small attack against the victim's infrastructure. Companies that pay the ransom risk being approached by the blackmailers again for a higher amount.

DD4BC primarily targets the online gambling industry but has recently broadened their activity to also attack the financial sector. It is no longer clear whether the attacks can be attributed to a single criminal group or whether other criminals are trying to replicate the business model. As the reputation about the crime group and its modus operandi spreads, it may become increasingly effective for attackers with no technical skills and infrastructure to impersonate the group.

FUTURE THREATS AND DEVELOPMENTS

Historically, law enforcement has not been the first port of call when an organisation has been the victim of a network intrusion or data breach. The reasoning behind this is likely a combination of the belief that law enforcement would be either unwilling or unable to investigate the crime and/or a lack of confidence in law enforcement's ability to handle the investigation with the appropriate level of discretion.

This trend appears to be changing however with the number of breaches being both reported to law enforcement and publically disclosed on the increase. Part of this may be a change in thinking amongst the private sector. Prior to 2014, publicising a data breach would have significant reputational damage. Suffering a breach was considered an exception whereas today there is a growing realisation that a breach is to some degree inevitable. In the wake of the volume and scale of the data breaches throughout 2014, it has perhaps become apparent that how an organisation responds to a breach is as important as whether it has had one. A timely 'clear and confident' message to customers and stakeholders as part of an effective communication strategy[71] can do much to maintain confidence in an organisation and prevent rampant speculation by the media.

Part of this strategy is clearly more frequent engagement with law enforcement. A number of European law enforcement agencies noted that the threshold for reporting breaches was decreasing. As both confidence in law enforcement's ability to investigate such crimes and law enforcement's capability and expertise in doing so increases, we can expect law enforcement to become more actively and frequently involved in investigating this type of criminality.

The term Advanced Persistent Threat (APT) was originally used by the U.S. government to describe nation state cyber-attacks which were sophisticated, specifically targeted and took place over a prolonged period, typically with the agenda of stealing data or causing damage for strategic gain. More recently the term has been adopted, and perhaps overused, by the media and security vendors to apply to any cybercrime group operating similar tactics for profit[72,73]. That said, there is evidently a blurring in the use of tools and techniques between the two groups; both factions using social engineering and both custom malware and publically available crimeware[74,75]. Industry reporting indicates that there is a clear trend in cybercrime groups increasingly performing long-term, targeted APT-style attacks instead of indiscriminate scattergun campaigns[76]. This will make it increasingly harder for investigators and security researchers to distinguish between attacks by either group and will require investigators to look more deeply at the motive and purpose behind an attack.

71 Mandiant, M-Trends 2015, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf, 2015

72 Websense, Advanced persistent Threats and Other Advanced Attacks, https://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf, 2011

73 McAfee, Combating Advanced Persistent Threats, http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf, 2011

74 FireEye, Targeted Crimeware in the Midst of Indiscriminate Activity, https://www.fireeye.com/blog/threat-research/2015/05/targeted_crimewarei.html, 2015

75 Mandiant, M-Trends 2015, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf, 2015

76 Computerworld, Cybercriminals Borrow from APT Playbook in Attacking PoS Vendors, http://www.computerworld.com/article/2918406/cybercrime-hacking/cybercriminals-borrow-from-apt-playbook-in-attacking-pos-vendors.html, 2015

Simple Service Discovery Protocol (SSDP) protocol that is enabled by default on millions of Internet devices using the Universal Plug and Play (UPnP) protocol – including routers, webcams, smart TVs and printers – has become the leading DDoS amplification attack vector in the first quarter of 2015. With the proliferation of the Internet of Things, attackers are likely to increasingly abuse large numbers of vulnerable unsecured online devices for powerful DDoS attacks[77].

RECOMMENDATIONS

- In order to be able to effectively investigate this type of crime, law enforcement must share experience, expertise and best practice and seek to increase their capacity and capability in dealing investigations of this nature. Law enforcement must show that it is both ready and able to meet this challenge.
- Law enforcement must continue to engage with private industry to build and maintain relationships in order to increase industry confidence and the likelihood that law enforcement will be approached in the event of a breach.
- If the affected party has not yet done so, law enforcement should advise contacting national CERTs for addressing the incident response and prevention of future incidents using anti-DDoS protection.
- As the business costs of seizure of the targeted infrastructure for forensic examination may be prohibitive, law enforcement should develop in-situ forensics capabilities.
- Law enforcement should closely cooperate with IT departments of the affected companies to assure preservation of relevant evidence.

77 Akamai, State of the Internet – Security Report, https://www.stateoftheinternet.com/resources-web-security-2015-q1-internet-security-report.html, 2015

ATTACKS ON CRITICAL INFRASTRUCTURE

Critical infrastructure continue to be at risk from constantly evolving threats in cyberspace, which need to be addressed in a holistic and effective manner in order to protect economies and societies[78,79].

Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS) and Automatic Identification Systems (AIS) are complex systems composed of various hardware and software components, often from different vendors. They were often designed with little consideration for network security. Mergers and acquisitions, poor assessment management, absence of patch management policies and a lack of knowledge transfer prior to staff turnover can all negatively impact the cybersecurity of CIs. Together with the persistence of legacy systems and the difficulties in maintaining a continuous cycle of updates, a steady increase in the number of opportunities to exploit vulnerabilities can be expected[80].

CI is becoming increasingly automated and interlinked, thereby introducing new vulnerabilities in terms of equipment failure, configuration error, weather and other natural causes as well as physical and cyber-attacks. Network isolation is no longer sufficient to ensure the security of an industrial facility[81].

The threat theatre is increasingly characterised by organised groups or non-state actors and individuals resorting to asymmetric attacks enabled by the universal connectivity the Internet provides and the availability of the necessary tools and attack information. Loss of control over technology as a result of globalisation, the need for online accessibility, and foreign ownership of critical infrastructures is also increasing vulnerabilities.

The time period from when a vulnerable system is breached by a malicious outsider to the breach being discovered and vulnerabilities identified and patched, is currently on average about 200 days[82]. This may be due to a variety of reasons, including the fact that the scope and nature of attacks may not be clear from the beginning.

FUTURE THREATS AND DEVELOPMENTS

The management and operation of critical infrastructure systems will continue to depend on cyber information systems and electronic data. Reliance on the power grid and telecommunications will also continue to increase, as will the number of attack vectors and the attack surface due to the complexity of these systems and higher levels of connectivity due to smart networks. The security of these systems and data is vital to public confidence and safety[83,84,85].

Even though cyber sabotages have been infrequent so far[86], attacks on critical infrastructures are a threat that is here to stay. In the future we will observe an increase in attacks on data brokers, on physical infrastructures, and on telecommunication

78 Tripwire, Cyberterrorists Attack on Critical Infrastructure Could be Imminent, http://www.tripwire.com/state-of-security/security-data-protection/security-controls/cyberterrorists-attack-on-critical-infrastructure-could-be-imminent/, 2015

79 Arstechnica, Fear in the Digital City: Why the Internet has Never been More Dangerous, http://arstechnica.com/information-technology/2015/02/fear-in-the-digital-city-why-the-internet-has-never-been-more-dangerous/2/, 2015

80 Trend Micro, A Security Evaluation of AIS, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf, 2015

81 Kaspersky, Cyberthreats to ICS Systems, http://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_web.pdf, 2014

82 Infosecurity, Hackers Spend 200+ Days Inside Systems Before Discovery, http://www.infosecurity-magazine.com/news/hackers-spend-over-200-days-inside/, 2015

83 NBC News, Critical Infrastructure Is Vulnerable to Cyberattacks, Says Eugene Kaspersky, http://www.nbcnews.com/tech/security/critical-infrastructure-vulnerable-cyberattacks-says-eugene-kaspersky-n379631, 2015

84 Dell, 2015 Annual Threat Report, http://www.dell.com/learn/us/en/uscorp1/press-releases/2015-04-13-dell-annual-threat-report, 2015

85 Kaspersky, Critical Infrastructure Protection, http://www.kaspersky.com/industrial-security-cip, 2015

86 The Economist, Defending the Digital Frontier, http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals, 2014

networks, such as global denial of service attacks on all connected services.[87] New forms of CI such as social media platforms will become a prime target for cybercriminals[88].

Exploitation of existing vulnerabilities, zero days and targeted phishing attacks will increase and continue to pose threats against critical infrastructures owing to the complex mix of legacy systems and new components combined with the need to minimise business disruption and cost, which often delay upgrades and updates. Lack of supplier support and end-of-life policies also have a significant impact on the security of CIs. Employees with privileged system access will remain key targets and subject to social engineering attacks[89,90].

Strengthening cyber security and tackling cybercrime requires a combination of prevention, detection, incident mitigation, and investigation. Addressing critical infrastructures' vulnerabilities necessitates a cooperative approach from the public and private sectors, and connecting the local and international dimension. The challenge of protecting critical infrastructures requires managing competing demands between security and privacy[91,92].

87 Informationweek, The Weaponization of Cyber Vulnerabilities, http://www.informationweek.com/whitepaper/cybersecurity/network-&-perimeter-security/week-to-weak:-the-weaponization-of-cyber-vulnerabilities/360793?gset=yes&, 2015

88 CSO, Pressure Mounts in EU to Treat Facebook and Twitter as Critical Infrastructure, http://www.cso.com.au/article/578271/pressure-mounts-eu-treat-facebook-twitter-critical-infrastructure/, 2015

89 Recorded Future, Real-Time Threat Intelligence for ICS/SCADA Cyber Security, http://go.recordedfuture.com/hubfs/data-sheets/ics-scada.pdf, 2014

90 Techcrunch, The Dinosaurs of Cybersecurity Are Planes, Power Grids and Hospitals, http://techcrunch.com/2015/07/10/the-dinosaurs-of-cybersecurity-are-planes-power-grids-and-hospitals/, 2015

91 Infosecurity Magazine, Destructive Cyber-Attacks Blitz Critical Infrastructure – Report, http://www.infosecurity-magazine.com/news/destructive-cyber-attacks-critical/, 2015

92 Trend Micro, Report on Cybersecurity and Critical Infrastructure in the Americas, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf, 2015

RECOMMENDATIONS

- Policy makers must ensure the swift implementation of the EU Directive on attacks against information systems. The Directive aims to strengthen national cybercrime laws and introduce tougher, consistent and EU-wide penalties for illegal access and system and data interference and criminalising the use of malware as a method of committing cybercrimes[93].
- In the context of the draft Directive on Network and Information Security (NIS), there is a need to improve coordination, active partnership, and relationships between the private sector, law enforcement and CERT community[94].
- Law enforcement and prosecution must be engaged early following cyber security incidents to allow investigation of the criminal aspects of such attacks[95,96,97,98].
- Organisations should consider adopting ENISA guidelines for incident handling in order to minimise operational downtime when investigating incidents.
- Member States should identify which entities should be considered as critical infrastructure within their jurisdiction.
- Law enforcement and agencies dealing with National Security Strategies should ensure there is a single point of contact available to deal with key national critical infrastructure entities.

93 EU Directive on attacks against information systems, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF, 2013

94 ENISA, Critical Infrastructures and Services, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services, 2011

95 CERT-EU, DDoS Overview and Incident Response Guide, http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_09_DDoS_final.pdf, 2014

96 Mandiant, M-Trends 2015, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf, 2015

97 CERT-EU, Data Acquisition Guidelines for Investigation Purposes, http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_04_Guideline_DataAcquisition_v1_4_4.pdf, 2012

98 ENISA, Electronic Evidence – a Basic Guide for First Responders, https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/electronic-evidence-a-basic-guide-for-first-responders, 2015

CRIMINAL FINANCES ONLINE

The digital underground, like any economy, relies on the free flow of funds. The variety of payment mechanisms available to and used by cybercriminals is diverse. It ranges from real world, physical payments to untraceable cryptocurrencies, and everything that falls in between. Many payment mechanisms with a significant or absolute online aspect offer a number of features that make them attractive as a financial instrument for criminal enterprise – anonymity, rapid, cheap and irreversible transfers, and obfuscated financial transactions. In many respects, some payment mechanisms can offer a level of anonymity similar to cash but in an online environment.

The payment mechanisms used by cybercriminals can be broken down into the following categories:

- Traditional financial instruments (e.g. banks accounts, credit cards)
- Money service bureaus (e.g. Western Union, MoneyGram)
- Voucher systems (e.g. Ukash, paysafecard)
- Online payment services (e.g. PayPal, Skrill)
- Centralised virtual currencies (e.g. PerfectMoney, WebMoney)
- Decentralised virtual currencies (invariably Bitcoin)
- Other pre-paid solutions (e.g. pre-paid debit cards)

Furthermore, when considering how and why cybercriminals use any particular payment mechanism it is important to consider the nature of the transaction. In this respect, four distinct scenarios can be identified.

CRIMINAL-TO-CRIMINAL PAYMENTS

This category of payment includes any transaction where one cybercriminal makes a payment to another for purchase of or access to a crime-related product or service – a common scenario within the CaaS business model of cybercrime.

For such payments the nature of the service or product paid for is also an influencing factor. For instance, where the sale of compromised data (such as stolen credit card details) is concerned, the use of Bitcoin or money service bureaus (typically Western Union) is common; however the use of voucher systems (Ukash) or WebMoney is also noted.

Hidden services on the Darknet such as Agora or the now defunct Evolution almost exclusively use Bitcoin for payment, with the mechanisms to handle payment and escrow functions built into the market interfaces.

Overall, Bitcoin is beginning to feature heavily in many EU law enforcement investigations, accounting for over 40% of all identified criminal-to-criminal payments. PayPal is another notable payment system used for transactions of this nature, accounting for almost one quarter of identified payments. To a lesser extent paysafecard, Ukash, Webmoney and Western Union were also used.

PAYMENT FOR LEGITIMATE SERVICES

Transactions in this category represent scenarios where a cybercriminal is required to make a payment to a legitimate, public facing company for such things as hosting, hardware, software or travel and accommodation. The nature of the payment mechanism used in these scenarios indicate that cybercriminals rarely feel the need to hide their identities, or do not have the skill set to do so, as over 60% of transactions use traditional financial instruments such as credit cards or transfers from bank accounts. However, whether these cards or accounts are legitimate, compromised or fraudulently obtained is unknown.

VICTIM PAYMENTS

Where a cybercrime victim is not simply subject to a malicious, destructive attack there will frequently be an attempt to obtain funds from the victim. Cyber-extortion is becoming increasingly common, particularly with the growing pervasiveness of ransomware, however more 'traditional' methods of cyber-extortion such as the threat of DDoS attacks are still commonplace[99]. Again, Bitcoin features as the most common single payment mechanism used in extortion payments, accounting for approximately one third of cases. Voucher systems such as Ukash, paysafecard and MoneyPak also accounted for over one quarter of cases. Direct bank transfers and money service bureaus also accounted for notable volumes of such payments.

Victims also make payments to attackers in less flagrant attacks if they are victims of fraud, either as a result of social engineering or when paying for non-existent or bogus goods or services such as fake anti-virus software. In these instances real world financial services (money service bureaus and bank transfers) account for half of all fraudulent payments, however Bitcoin is also used in almost one third of payments.

MONEY MOVEMENT/LAUNDERING

There are naturally instances where a cybercriminal does not transfer funds to a third party, but simply moves money from one location or payment system to another. This can include the 'cashing out' of compromised financial accounts and credit cards and the use of exchangers to exchange to, from or between virtual, digital and fiat currencies.

As with victim payments, over half of transactions are carried out via money service bureaus and bank transfers. In this scenario however, Bitcoin and other payment mechanisms such as WebMoney only account for a small proportion of transactions.

99 CoinDesk, Bitcoin Extortion Group DD4BC Prompts Warning from Swiss Government, http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks/, 2015

FUTURE THREATS AND DEVELOPMENTS

Although there is no single common currency used by cybercriminals across the EU, it is apparent that Bitcoin may gradually be taking on that role. Bitcoin features as a common payment mechanism across almost all payment scenarios, a trend which can only be expected to increase.

Cryptocurrencies are slowly gaining acceptance at government level, with a number of EU jurisdictions either proposing regulation of cryptocurrencies[100] or already recognising them under existing legislation[101,102]. It is inevitable that more jurisdictions will follow suit although it would appear that there is currently a lack of harmonisation in approaches.

Any regulation of cryptocurrencies would likely only be applicable and enforceable when applied to identifiable users such as those providing exchange services. The inability to attribute transactions to end users makes it difficult to imagine how any regulation could be enforced for everyday users.

It is clear that cybercriminals will continue to use whichever payment mechanism is convenient, familiar or perceived to be safe, including those that are already regulated and maintain anti-money laundering controls.

In the 2014 Internet Organised Crime Threat Assessment it was anticipated that more niche, privately controlled currencies would come to the fore. However these have either yet to be discovered or have simply not materialised. That said, there are currently over 650 recorded cryptocurrencies[103] with new variants being released almost daily.

100 CoinDesk, Will the New UK Government Create a Bitcoin Hub? http://www.coindesk.com/will-the-new-uk-government-create-a-bitcoin-hub, 2015

101 RT, Germany Recognizes Bitcoin as 'Private Money', http://rt.com/news/bitcoin-germany-recognize-currency-641/, 2013

102 JDSUPRA, Virtual Currencies: International Actions and Regulations, http://www.jdsupra.com/legalnews/virtual-currencies-international-action-03024/, 2014

103 Crypto-Currency Market Capitalizations, http://www.coinmarketcap.com, accessed 03/07/2015

Payment Purpose	Payment For	Common Payment Mechanisms	Example
Victim Payment	Extortion	Bitcoins, Bank Transfer, paysafecard	Payment extorted as a result of a ransomware or DDoS attack.
	Fraud	Bitcoins, Bank Transfer, Western Union	Loss to an online fraud/scam.
Criminal to Criminal Payment	Counter AV	PayPal	Testing of malware against commercial AV products.
	Data	Bitcoins, Ukash, Western Union, WebMoney	Purchase of compromised financial data such as credit cards.
	DDoS	Bitcoins	DDoS services for hire.
	Hosting	Bitcoins	Purchase of hosting (including bulletproof).
	Malware	Visa, MasterCard, WebMoney, PayPal	Purchase of malware such as RATS and banking trojans.
	Trade on Hidden Service	Bitcoins, Ukash, paysafecard	Purchase of drugs or weapons.
Payment for Legitimate Service		Bitcoins, Bank Transfer, Visa, MasterCard	Hosting, hardware, software, travel, accommodation, etc.
Money Movement		Bitcoins, Bank Transfer, Western Union	Movement of money to maintain control of funds, or hide/break a financial trail, including 'cashing out' of compromised financial accounts. This also includes exchange to, from or between virtual, digital and fiat currencies.

Many focus on developing features which further enhance their anonymity, thereby making them more attractive for illicit use. However, with so many existing options available to conduct illicit transactions securely online there seems to be little need.

RECOMMENDATIONS

- Investigators must familiarise themselves with the diverse range of account and payment references and file formats of digital wallets used by the different payment mechanisms in order to recognise these in both standard and forensic investigations.
- Law enforcement must continue to cooperate and share knowledge, expertise and best practice on dealing with Bitcoin and other emerging/niche digital currencies in cyber investigations.
- Law enforcement should continue to monitor the alternate payment community for emerging payment mechanisms, to assess their potential or likelihood of being used in cyber-enabled crime.
- It is essential for law enforcement to build and develop working relationships with the financial sector including banks, money transfer agents, virtual currency scheme operators and exchangers in order to promote the lawful exchange of information and intelligence.
- There is a need for harmonised legislative changes at EU level, or the uniform application of existing legal tools such as anti-money laundering regulations, to address the criminal use of virtual currencies.

CRIMINAL COMMUNICATIONS ONLINE

The Internet has changed the way the world communicates. The variety of options for engaging with others online is very diverse. Users can choose to contact one person, or potentially millions at once, sharing information in almost any format or form of media. Moreover, the range of devices and applications which support this level of communication is growing.

CRIMINAL TO VICTIM COMMUNICATION

How a cybercriminal initiates contact with their victim is dependent on the nature, scale and scope of the intended attack. For high volume, untargeted attacks, email is still a preferred method of contacting potential victims, and is easily achievable with automated or well-established criminal services such as spam. Many malware and social engineering attacks are particularly well suited to this scattergun style of approach, compensating for low success rates by targeting potential victims en masse. Following a successful initial contact or attack, email often remains the primary contact method between attacker and victim.

For targeted, campaign-style attacks more direct one-to-one forms of communication are preferred. The use of email is still common (i.e. spear phishing), for both malware-related and social engineering type attacks. Contact in this instance will typically be limited to a select group of victims or even individuals and often only as a stepping-stone to gaining access to a third party. In other instances, there is continuing growth in the use of applications which allow VoIP or text messaging, particularly those available on mobile phones such as Skype, Viber or WhatsApp. In cases relating to online child abuse, Skype is noted as a common communication method in addition to web-based chat rooms.

CRIMINAL TO CRIMINAL COMMUNICATION

When communicating with each other, the range of communication options used by criminals differs considerably. Email is still commonly used, as are web-based chat rooms and applications such as Internet Relay Chat (IRC). The use of forums on either the open or deep web, or Darknets, is also very common, with forums providing meeting- and market-places for criminals to do business and engage with like-minded individuals.

In July 2015, Operation Bugbite saw the successful takedown of the most prolific English-speaking cybercriminal forum to date: Darkode. The popular cybercriminal hub facilitated a wide range of criminal products and services including malware, zero day exploits, hacking, stealing credit card and bank credentials, botnets for rent and DDoS attacks. The operation, which was led by the FBI and supported by Europol's EC3 with the involvement of law enforcement officers from 20 countries in and outside the European Union, resulted in 28 arrests, 37 house searches, and numerous seizures of computers and other equipment.

For real-time, one-to-one communication, Jabber, and to a lesser extent ICQ, are regularly employed, and the use of both is on the increase. With the exception of ICQ, which has a long history of use in cybercrime, there is a notable avoidance of common commercial products in favour of platforms with actual or perceived levels of increased privacy and/or anonymity. The gradual increase in the use of ICQ may be as a result of its ownership moving into the hands of a Russian company (the Mail.ru Group)[104].

THE INCREASING USE OF ENCRYPTION

More than three-quarters of cybercrime investigations in the EU encountered the use of some form of encryption to protect data and/or to frustrate forensic analysis of seized media. Both TrueCrypt and BitLocker are commonly encountered and increasingly so, despite the cessation of TrueCrypt's development in May 2014. Almost half of all Member States also noted an increased use of encrypted email, typically PGP.

While the use of encryption legitimately, for the protection of personal, customer and other business data and intellectual

104 Bloomberg, ICQ Messenger Is Growing for the First Time in Years, http://www.bloomberg.com/news/articles/2014-07-29/icq-messenger-is-growing-for-the-first-time-in-years, 2014

property is to be actively encouraged, the issues for law enforcement arising from its use by criminals and terrorists to similarly protect themselves cannot be overstated.

ANONYMISATION

Any cybercriminal maintaining even the most basic operational security requires some form of IP anonymising solution. The use of simple proxies and virtual private networks (VPNs) has continued to increase over the past 12 months and is now the norm amongst cybercriminals. The adoption of Tor as an anonymising solution has seen the greatest growth in the past 12 months, with half of EU Member States noting an increase in its use for the obfuscation of criminal activity. Instances of I2P being used as an anonymising solution are also on the increase although it is not as widespread as Tor. This may be due to the simplicity of access to Tor, whereas I2P requires some additional user input that may deter less technical users.

FUTURE THREATS AND DEVELOPMENTS

With the actions of Edward Snowden still echoing loudly in the thoughts of governments and the security conscious alike, there is clearly a drive towards greater use of encryption in data storage and also end-to-end encryption in communications. Some major IT manufacturers are slowly moving towards encryption-by-default in their products[105,106]. While the benefits to the public and to the private sector cannot be denied, the question as to where this leaves governments and law enforcement is currently unanswered. The balance between privacy and the protection of data, and the necessity for law enforcement to be able to access data to investigate crime and terrorist activity, is not an easy one to work and government are yet to come forward with a workable solution or compromise.

RECOMMENDATIONS

- Law enforcement would benefit from a central database of VPN and proxy services used by cybercriminals to determine if any are suitable for either information exchange with law enforcement or intervention if criminal in nature.
- Legislators and policy makers, together with industry and academia, must implement a workable solution to the issue of encryption which allows legitimate users to protect their privacy and property without severely compromising government and law enforcement's ability to investigate criminal or national security threats.

105 The Guardian, Apple Defies FBI and Offers Encryption by Default on New Operating System, http://www.theguardian.com/technology/2014/oct/17/apple-defies-fbi-encryption-mac-osx, 2014

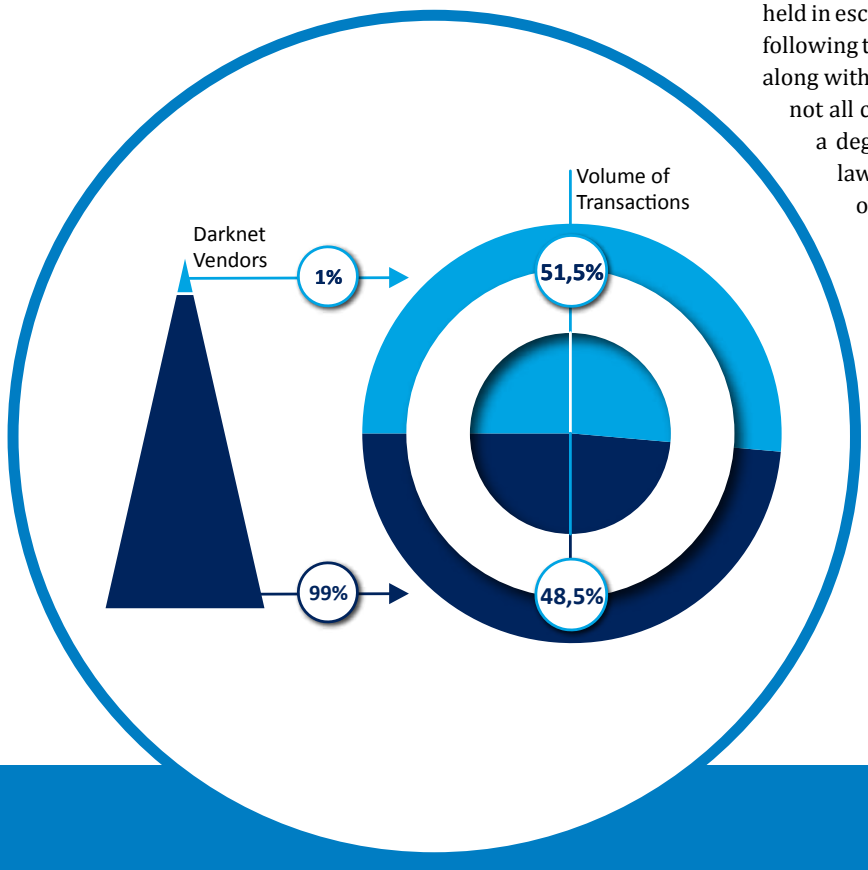
106 The Wall Street Journal, Apple and Others Encrypt Phones, Fuelling Government Standoff, http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801, 2014

DARKNETS

Investigations into hidden services on anonymising overlay networks such as Tor are becoming commonplace for EU cybercrime units. Over half of EU Member States have investigated drug or payment card related activity on the Darknet and over one third have investigated criminal activity related to intellectual property, weapons or compromised bank accounts. Almost a third of EU law enforcement actively monitors marketplaces, although largely in relation to specific operations rather than general intelligence gathering.

A small fraction of criminals active in the Darknet manage to operate successful businesses generating significant profits. Recent research established that the top 1% most successful vendors were responsible for 51.5% of all transactions[107].

107 Carnegie Mellon University, Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf, 2015



2014-2015 has been a turbulent period for criminal services on the Darknet.

In November 2014, 21 countries participated in Operation Onymous which saw the seizure of 619 .onion domains along with bitcoins worth EUR 900 000 and EUR 180 000 in cash, drugs, gold and silver. Thirty-three high profile marketplaces and forums were taken out of action and 17 individuals were arrested. It is estimated that the seized sites represented approximately 37% of the market share on the Darknet.

A consequence of Onymous was the displacement of customers and vendors to the remaining marketplaces, the two largest and most successful of which were Agora and Evolution. Several new marketplaces also opened to fill the vacuum left by the operation. Additionally the prices of illegal goods on many of the remaining services were seen to increase[108].

In March 2015, Evolution shut down as a result of an exit scam. Its administrators left, taking with them over EUR 11 million[109] in Bitcoins belonging to vendors and customers which had been held in escrow. This was the second such major exit scam to occur following the Sheep Marketplace which folded in November 2013 along with over EUR 36 million of members' Bitcoins. On most if not all criminal forums or marketplaces there is undoubtedly a degree of paranoia that the site has been infiltrated by law enforcement. Whether this paranoia is unwarranted or not, exit scams such as these create an additional dimension of distrust that law enforcement could not hope to achieve and further undermines confidence in these marketplaces.

Following the exit of Evolution, the Agora marketplace, along with several smaller markets such as Abraxas, Alphabay, Black Bank, and Middle Earth have absorbed the displaced vendors and

108 The Impact of Operation ONYMOUS; Europol 2015

109 DEEPDOTWEB, Evolution Marketplace Exit Scam: Biggest Exit Scam Ever?, https://www.deepdotweb.com/2015/03/18/evolution-marketplace-exit-scam-biggest-exist-scam-ever, 2015

customers[110]. On top of additional security measures in the wake of Onymous, such sites are now also implementing protocols to help prevent or mitigate potential exit scams such as multi-signature escrow and early finalisation of payments. Together these will not only reduce the amount of Bitcoin sitting in escrow but also prevent a single person having full control over the funds.

Post Onymous, the Agora, Outlaw and Nucleus marketplaces are the highest priority marketplaces for EU law enforcement, with a number of Member States also targeting sites hosted in their native language.

FUTURE THREATS AND DEVELOPMENTS

Between Operation Onymous and the growing number of large scale exit scams, confidence in underground markets has undoubtedly been shaken. Onymous was a strong statement by law enforcement that these services are certainly not beyond their reach. Yet, despite this message, hidden services continue to grow, multiply and evolve.

The prospect of services moving from Tor to I2P is still real, however research carried out to date suggests that Tor is still by far the preferred network[111]. A more concerning prospect (for law enforcement) is the development of decentralised marketplaces such as the OpenBazaar. OpenBazaar is a BitTorrent-style peer-to-peer network which allows direct contact between customers and vendors and uses Bitcoin as a payment mechanism[112]. As the 'market' is peer-to-peer there would be no website or server to be targeted by investigating law enforcement and intervention is a considerable challenge, mirroring the issues law enforcement currently has with investigations involving Bitcoin. Payments on the OpenBazaar use a multi-signature approach involving a third party 'notary' to control the release of funds. This means that there is no possibility of performing an exit scam with customers' and vendors' funds.

110 The Impact of Operation ONYMOUS; Europol 2015
111 TNO research
112 Openbazaar, https://openbazaar.org, 2015

RECOMMENDATIONS

- Law enforcement should proactively gather intelligence relating to hidden services; however this requires a coordinated approach in order to prevent duplication of effort.
- Member States should provide intelligence relating to hidden services to Europol's EC3 to allow it to build a comprehensive intelligence picture of hidden services across Europe. There needs to be greater engagement from non-cybercrime law enforcement in tackling hidden services. The sale of drugs or firearms in these marketplaces is as much, if not more, of an issue for these crime areas as it is for cybercrime.
- Further intelligence gathering is required on the use of I2P and other peer-to-peer networks as hosts for illegal online marketplaces.
- Law enforcement should collaborate with private sector and academia to explore investigative and research opportunities related to emerging technologies such as decentralised marketplaces like OpenBazaar.

BIG DATA, IOT AND THE CLOUD

As highlighted in the 2014 IOCTA, the rise of the Internet of Things (IoT) or the Internet of Everything (IoE) is seen as a major challenge for law enforcement together with Big Data and the Cloud. Being able to keep up with the pace of technological development will require law enforcement to constantly update their digital forensics capabilities.

Based on the feedback received, Big Data for law enforcement usually means a lot of data which is often referred to as the volume challenge. Cases involving several terabytes of data for one suspect are becoming more common, which has a considerable impact on investigations in terms of resources and time, making it more difficult for law enforcement to find the proverbial needle in the haystack. For instance, in one of the cases the amount of data exceeded 100 terabytes. This has stimulated research into tools and methods to improve the handling and analysis of large quantities of data[113].

While the potential benefit of Big Data for more efficient, proactive and preventive police work is generally accepted[114], specifically in relation to predictive policing, it appears that the majority of EU law enforcement agencies are not at a stage where Big Data analytics is being used to its full potential or even considered at all. The potential benefits identified by law enforcement include improved and more targeted analytical capabilities, an increased chance to find relevant evidence, better support for the triage process and the ability to create a denser timeline of events, and the support for the automated analysis of crime-relevant data, including speech and video recognition.

While the IoT is still seen as an emerging threat from a law enforcement point of view[115], the rising number of smart 'things', including smart homes, smart cars[116,117], smart medical devices[118] and even smart weapons[119] are a clear indicator of its growing adoption[120]. This contributes to an increasing digitisation and online presence of personal and social lives, and an increasing level of interconnectivity and automation, which creates a number of challenges in terms of privacy, security, and trust. Law enforcement needs to be prepared to address the criminal abuse of such devices and of the data that is generated or collected via the IoT.

The Cloud is an enabler for IoE and Big Data by providing the distributed and scalable resources needed to handle the data growth and provide the necessary processing services. Data together with entire infrastructures will continue to move to the Cloud, which is already creating technical and legal challenges for law enforcement. Equally, criminals aim to abuse Cloud services such as popular file synchronisation services[121], for instance to host malware or C&C structures, as they are less likely to see any traffic blocked by security systems.

For law enforcement, the top challenges in relation to smart devices and the Cloud are:

113 Elsevier, Fast Contraband Detection in Large Capacity Disk Drives, http://www.dfrws.org/2015eu/proceedings/DFRWS-EU-2015-3.pdf, 2015
114 ISSUU, Predictive Policing: Taking a Chance for a Safer Future – http://issuu.com/rutgerrienks/docs/predictive_policing_rienks_uk, 2015
115 2015 IOCTA Survey; Only one EU law enforcement agency reported a case involving a smart device.
116 Reuters, Daimler to Test Self-driving Trucks in Germany This Year, http://www.reuters.com/article/2015/07/25/us-daimler-autonomousdriving-idUSKCN0PZ0KH20150725, 2015
117 GlobalAutomakers, Vehicle-to-Vehicle Technology, https://www.globalautomakers.org/topic/vehicle-vehicle-technology, 2015
118 FierceHealthIT, IoT to Fuel Revolution in Digital Healthcare, http://www.fiercehealthit.com/story/iot-fuel-revolution-digital-healthcare/2015-07-01, 2015
119 WIRED, Hackers Can Disable a Sniper Rifle – Or Change Its Target, http://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/, 2015
120 Trend Micro, What Smart Device Makers Must Do to Drive the IoT Revolution, http://blog.trendmicro.com/what-smart-device-makers-must-do-to-drive-the-iot-revolution/?linkId=15627100, 2015
121 Imperva, Imperva Hacker Intelligence Initiative uncovers New "Man In the Cloud" Attacks that Use Popular File Synchronisation Services, http://investors.imperva.com/phoenix.zhtml?c=247116&p=irol-newsArticle&ID=2075878, 2015

- Access to data – including determining the location of and timely and lawful access to evidence, determining the relevant legislation, and technical challenges – for instance in relation to encryption;
- Digital forensics and investigation – in relation to live data forensics and cloud forensics, but also in terms of keeping up with the pace of technical development and the variety of new hardware and software components; encryption, attribution and the quantity of data were highlighted under this topic;
- Training and education – specifically in terms of establishing and maintaining the necessary skills and expertise for first responders and forensics experts;
- Privacy and data protection issues linked to a lack of control over data and the risk of data breaches, criminal abuse e.g. in terms of hosting criminal infrastructures and new criminal opportunities due to a lack of security by design, a lack of protective action and a lack of awareness;
- Cross-border/international cooperation issues linked to inadequate legislation and the mutual legal assistance treaty (MLAT) process.

Of the questionnaire responses received from EU law enforcement, three agencies indicated that they were organising or were planning on organising training programmes on the IoT and the Cloud. Three agencies specified that they were cooperating with private industry on this topic. One law enforcement agency supported preventive activities in this area.

However, the feedback provided by law enforcement also identifies several opportunities with regard to the IoT and the Cloud:

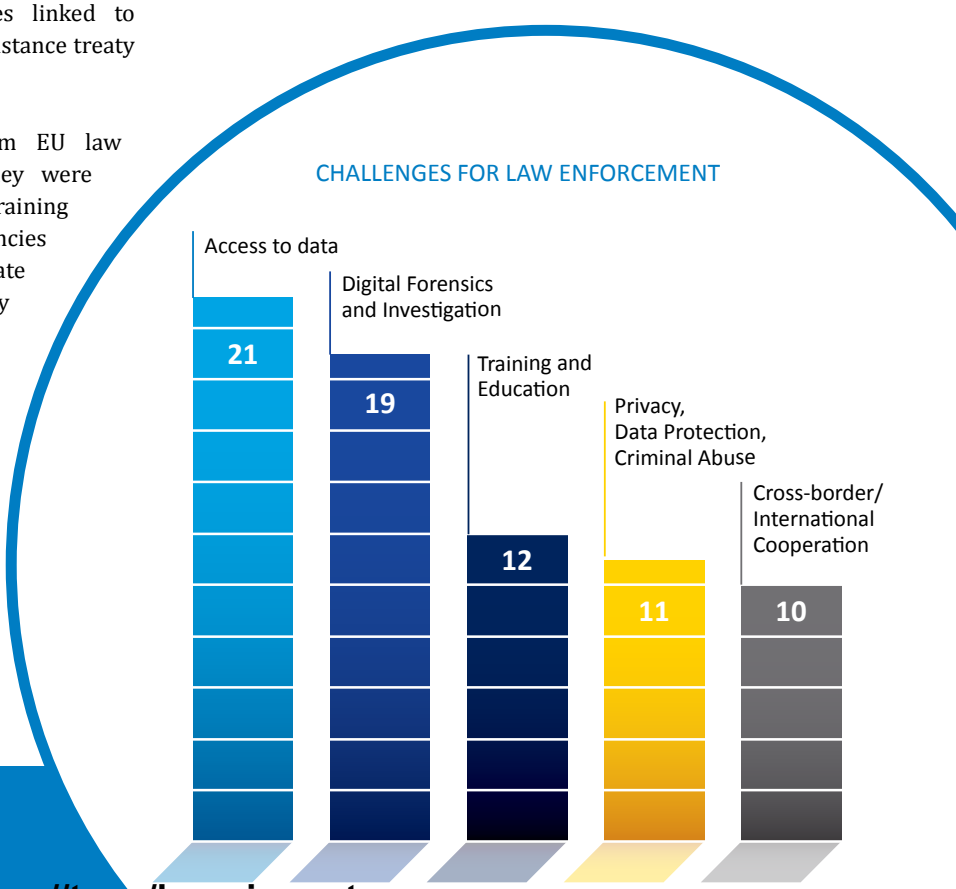
- Digital forensics and investigation – new investigative tools and techniques, new sources and types of evidence, enhanced cross-matching and OSINT opportunities;
- Access to data – centralised access, single point of contact for data requests, possibility for improved exchange of data;
- More opportunities for public-private partnerships and cooperation with private industry.

Future threats and developments

Rapid technological advancements and the increasing (inter) connectivity of people and devices contribute to an ever-rising stream of data and further blur the lines between real life and cyberspace.

While this is making the protection of data and ensuring privacy more challenging, it can also help address the new challenges and threats in cyberspace, for instance in the form of data-driven security or behaviour-based security[122].

122 Techcrunch, Next-Gen Cybersecurity Is All About Behavior Recognition, http://techcrunch.com/2015/08/23/next-gen-cybersecurity-is-all-about-behavior-recognition/, 2015



Data, particularly any personal data, is a commodity that is and will continue to be highly sought-after by private companies to further improve the purchasing experience and the prediction of customer behaviour, but also for security purposes e.g. to implement two-factor authentication – as a key commodity and enabler for cybercrime it is of equal interest to criminals. It is therefore safe to assume that criminals will continue to target companies collecting data, specifically also companies that hold records containing different categories of personal data (e.g. healthcare data) as they can be abused in different ways and for different types of crimes.

The ever-increasing amount of data will increasingly require tool support and automation, including machine learning and artificial intelligence approaches. This will apply to law enforcement and criminals alike and will present its own set of challenges for instance in terms of evidence admissibility.

The rising adoption of the IoT and the Cloud continues to create new attack vectors and increases the attack surface for cybercrime[123,124]. Considering our increasing dependency on connected and smart devices, emerging and future attack scenarios may encompass physical or mental harm, either intentionally or unintentionally. Possible scenarios range from hacked smart cars and hacked medical devices[125,126] to hacked weaponised drones[127].

Cybercriminals will continue to migrate their activities to the Cloud, often abusing legitimate services and combining different techniques to hide their activities[128,129]. The dependencies of the IoT on Cloud services and storage will provide criminals with a broadened range of possibilities to disrupt or manipulate smart devices as well as to extract data[130,131,132].

With criminals being able to potentially access and combine different types and sources of data, one can expect more sophisticated types of attacks (e.g. social engineering) but also new forms of existing crimes (e.g. extortion, ransomware). With novel approaches emerging to secure systems using e.g. behavioural patterns[133] to identify legitimate users, criminals may be forced to expand their data collection activities in order to be able to successfully mimic the behaviour of a user.

Common-mode failures or failures that result from a single fault in software or hardware components used in smart devices will continue to present a mayor cybersecurity risk to the IoT[134,135].

123 ENISA, Threat Landscape for Smart Home and Media Convergence, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-for-smart-home-and-media-convergence, 2015
124 Net Security, Average Financial Services Company Uses 1,004 Cloud Applications, http://www.net-security.org/secworld.php?id=18793, 2015
125 Schneier on Security, Hacking Drug Pumps, https://www.schneier.com/blog/archives/2015/06/hacking_drug_pu.html, 2015
126 MIT Technology Review, Security Experts Hack Teleoperated Surgical Robot, http://www.technologyreview.com/view/537001/security-experts-hack-teleoperated-surgical-robot/
127 Gizmodo, Police in India Will Use Weaponized Pepper Spray Drones on Protesters, http://gizmodo.com/police-in-india-will-use-weaponized-pepper-spray-drones-1696511132, 2015
128 Imperva, Imperva Hacker Intelligence Initiative uncovers New "Man In the Cloud" Attacks that Use Popular File Synchronisation Services, http://investors.imperva.com/phoenix.zhtml?c=247116&p=irol-newsArticle&ID=2075878, 2015
129 Fireeye, Hammertoss: Stealthy Tactics Define a Russian Cyber Threat Group, https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html, 2015
130 HCI, Why Hackers Love Healthcare Organizations, http://www.healthcare-informatics.com/article/why-hackers-love-healthcare-organizations, 2015
131 DARKReading, Spiderbot, Spiderbot, Does Whatever A Hacker Thought, http://www.darkreading.com/partner-perspectives/intel/spiderbot-spiderbot-does-whatever-a-hacker-thought/a/d-id/1321850,2015
132 DARKReading, Vulnerable From Below: Attacking Hypervisors Using Firmware And Hardware, http://www.darkreading.com/partner-perspectives/intel/vulnerable-from-below-attacking-hypervisors-using-firmware-and-hardware/a/d-id/1321834, 2015
133 Techcrunch, Next-Gen Cybersecurity Is All about Behavior Recognition, http://techcrunch.com/2015/08/23/next-gen-cybersecurity-is-all-about-behavior-recognition/, 2015
134 DARKReading, Chrysler Recalls 1.4 Million Vehicles After Jeep Hacking Demo, 2015 http://www.darkreading.com/vulnerabilities---threats/chrysler-recalls-14-million-vehicles-after-jeep-hacking-demo-/d/d-id/1321463, 2015
135 Arstechnica, Researchers Reveal Electronic Car Lock Hack After 2-Year Injunction by Volkswagen, http://arstechnica.com/security/2015/08/researchers-reveal-electronic-car-lock-hack-after-2-year-injunction-by-volkswagen/, 2015

Recommendations

- There is a need to inform law enforcement on a broad basis about Big Data and the challenges and opportunities that come with it.
- With the increasing adoption of the IoT and Cloud computing and services, law enforcement needs to invest in developing and maintaining the necessary skills, knowledge and technical capability to investigate IoT- and Cloud-related crimes.
- Existing initiatives aimed at improving the security of smart devices should be promoted and used to encourage companies to consider security and privacy as part of the design process[136].
- Security-by-design and privacy-by-design should be the guiding principles when developing smart devices and when collecting and processing data. This includes the need to only collect the minimum amount of data necessary, automatically protect personal data by using proactive security measures and means to make individuals less identifiable.
- Based on existing work undertaken in this area for instance by ENISA[137], policy makers should continue to work on effective, efficient and balanced legislation and regulations.

136 Auto Alliance, Automakers Announce Initiative To Further Enhance Cyber-Security In Autos, http://www.autoalliance.org/index.cfm?objectid=8D04F310-2A45-11E5-9002000C296BA163, 2015

137 ENISA, Threat Landscape for Smart Home and Media Convergence, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-for-smart-home-and-media-convergence, 2015

THE GEOGRAPHICAL DISTRIBUTION OF CYBERCRIME

Using the United Nation geoscheme[138], the following is a brief summary of significant industry-reported threats and law enforcement activity impacting on various regions globally, based on 2014-2015 data.

AFRICA

Africa's significance in the cybercrime community continues to grow with blended cyber-attacks of increasing sophistication originating from this region. Indicators suggest that African cybercriminals are benefiting from the same products and services available as-a-service on underground marketplaces as their European counterparts[139].

Nigeria features as a top 10 country for EU law enforcement in terms of the location of offenders or infrastructure related to cybercrime[140].

Furthermore, four out of the five top TLDs (top-level domains) used for phishing are of African origin (.CF, .ZA, .GA and .ML) although with the exception of .ZA (South Africa) these domains were repurposed in 2013 and are now owned by a Netherlands-based company[141].

THE AMERICAS

North America maintains its lead in terms of hosting malicious content and the proportion of global victims resident in that region. In 2014 the United States hosted between 20%[142] and

138 UN Statistics Division, http://unstats.un.org/unsd/methods/m49/m49.htm, 2015

139 Trend Micro, Piercing the Hawkeye: Nigerian Cybercriminals Using a Simple Keylogger to Prey on SMBs Worldwide, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hawkeye-nigerian-cybercriminals-used-simple-keylogger-to-prey-on-smbs, 2015

140 2015 IOCTA Survey

141 APWG, Global Phishing Report 2H 2014, http://internetidentity.com/wp-content/uploads/2015/05/APWG_Global_Phishing_Report_2H_2014.pdf, 2015

142 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015

almost 40%[143] of the world's command-and-control servers. The USA also hosts over 45% of the world's phishing domains[144] and remains one of the world's top spam producers[145,146].

The United States is home to a comparatively high proportion of global bots, harbouring between 16%[147] and 20%[148] of all bots worldwide. In addition, in 2014 almost one third of PoS malware and over 40% of all ransomware detections were in the USA.

20 EU Member States had investigations where criminal infrastructures or suspected offenders were located in the United States and over 70% of SEPA countries reported losses from the use of skimmed payment cards in the USA, though this should decrease over time as the US finally adopts chip and PIN technology[149].

South America featured less in both industry reporting and EU law enforcement investigations in 2014 although both Colombia and Argentina remain in the top 10 countries for sending spam[150,151]. Poor digital hygiene is still an issue with many South American countries (Ecuador, Guatemala, Bolivia, Peru, Brazil) having high malware infection rates[152]. Brazil is also often seen as a key player in malware related to PoS and ATM terminals and skimming devices[153].

South America (Brazil) is also often seen as a key player in malware related to PoS, ATM terminals – and skimming devices.

143 McAfee Labs, Threat Reports May 2015, http://www.mcafee.com/nl/resources/reports/rp-quarterly-threat-q1-2015.pdf , 2015
144 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
145 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
146 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
147 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
148 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
149 EAST, European Fraud Update 02/2015, https://www.european-atm-security.eu/east-publishes-european-fraud-update-2-2015/, 2015
150 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
151 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
152 Panda Labs, Annual Report 2014, http://www.pandasecurity.com/mediacenter/src/uploads/2015/02/Pandalabs2014-DEF2-en.pdf, 2015
153 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015

ASIA

Like the US, China continues to feature heavily in Internet security industry threat reporting. In addition, almost half of EU Member States had investigations where criminal infrastructures or offenders appeared to be located in China. Some sources identify China as the source of over 30% of global network attacks[154]. Along with India[155] and South Korea, China features in top 10 lists of countries hosting botnet C&C infrastructure[156]. China also maintains one of the highest malware infection rates globally[157] and is subsequently home to one of the highest proportions of global bots[158]. India, Indonesia, Malaysia, Taiwan and Japan also host significant bot populations[159,160].

Japan would appear to have an increasingly significant role as both a victim and source of cybercrime, featuring as a source of spam[161] and, in some reports, having the second highest global detection rate for ransomware[162]. Japan is also one of the top three countries in Asia where EU law enforcement investigation has identified perpetrators or criminal infrastructure. Japan, South Korea and the Philippines are the most prominent of countries in East and South-East Asia out of which gangs running commercial sexual extortion campaigns are noted to operate.

Several Asian countries feature as top sources of spam, in particular Vietnam[163,164] and to a lesser extent India[165] and

154 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
155 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
156 McAfee Labs, Threat Reports May 2015, http://www.mcafee.com/nl/resources/reports/rp-quarterly-threat-q1-2015.pdf , 2015
157 Panda Labs, Annual Report 2014, http://www.pandasecurity.com/mediacenter/src/uploads/2015/02/Pandalabs2014-DEF2-en.pdf, 2015
158 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
159 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
160 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
161 McAfee Labs, Threat Reports May 2015, http://www.mcafee.com/nl/resources/reports/rp-quarterly-threat-q1-2015.pdf, 2015
162 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
163 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
164 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
165 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015

China[166]. China also features again as a top jurisdiction within Asia for hosting phishing domains, along with Hong Kong[167]. Although they are not noted for hosting phishing domains, the country code top-level domains (ccTLDs) for both Thailand and Pakistan are commonly used in phishing attacks[168].

The Asia-Pacific region is also the territory where most SEPA members report losses arising from the use of skimmed cards. Five out of the top six countries where losses were identified were in this region, with Indonesia most commonly reported, and then to a lesser extent the Philippines, South Korea, Vietnam and Malaysia[169].

EUROPE

The fast and reliable ICT infrastructure found in much of Europe, particularly Western Europe, is exploited by cybercriminals to host malicious content and launch attacks on targets both inside and outside of Europe. The EU hosts approximately 13% of global malicious URLs (i.e. online resources that contain redirects to exploits or host exploits themselves). Of these the Netherlands accounts for the most significant proportion while Germany, the UK and Portugal make up much of the remainder. Germany, the UK, the Netherlands, France and Russia also feature as significant hosts for both C&C infrastructure and phishing domains globally[170,171]. Italy, Germany, the Netherlands, Russia and Spain are also some of the top sources for global spam[172,173].

Many European regions – especially in Western Europe – feature some of the lowest global malware infection rates. The Scandinavian countries and Finland typically have the lowest rates[174,175].

Within the EU, France, Germany, Italy and to a lesser extent the UK click on the largest number of malicious URLs. This undoubtedly contributes to these states having the highest malware infection rates and the highest proportions of bots found within the EU. This is partly to be expected, however, given that these four jurisdictions have the highest populations in the EU.

In terms of EU law enforcement activity, approximately one half of EU Member States identified infrastructure or suspects in the Netherlands, Germany, Russia or the United Kingdom in the course of their investigations. Moreover, approximately one third found links to Austria, Belgium, Bulgaria, the Czech Republic, France, Hungary, Italy, Latvia, Poland, Romania, Spain or Ukraine.

OCEANIA

Australia retains a presence in a number of industry top 10 league tables related to cybercrime including global bot populations, ransomware detections[176] and as a source of network attacks[177]. Other than this, Oceanic countries do not feature prominently in cybercrime reporting or in EU law enforcement investigations.

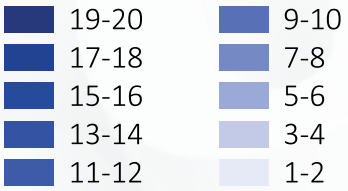
However, the ccTLD for the Micronesian island of Palau features as the TLD with the second highest proportion of its domains used for phishing; being heavily abused by Chinese phishers[178].

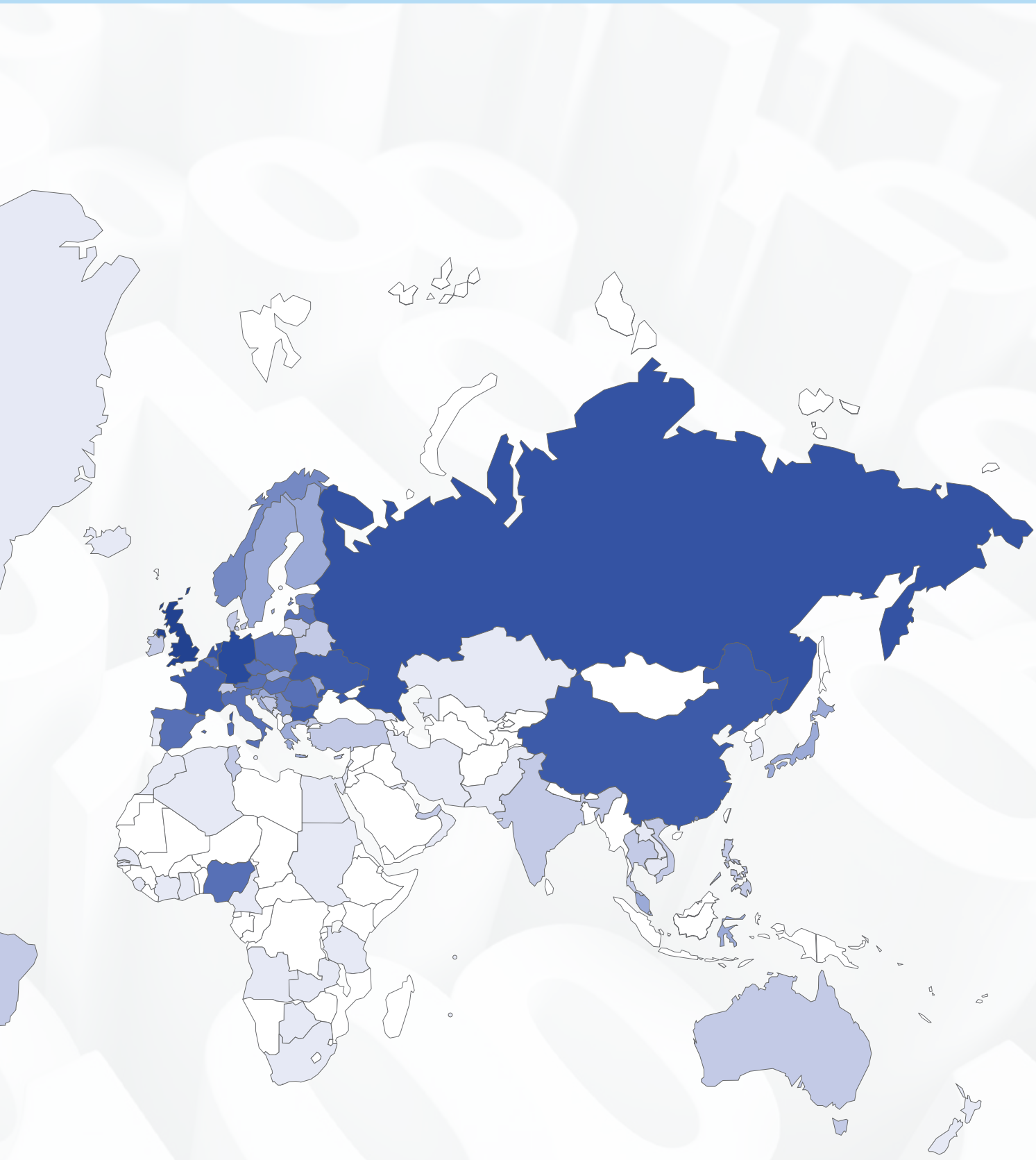
166 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
167 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
168 APWG, Global Phishing Report 2H 2014, http://internetidentity.com/wp-content/uploads/2015/05/APWG_Global_Phishing_Report_2H_2014.pdf, 2015
169 EAST, European Fraud Update 02/2015, https://www.european-atm-security.eu/east-publishes-european-fraud-update-2-2015/, 2015
170 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
171 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
172 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
173 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
174 Panda Labs, Annual Report 2014, http://www.pandasecurity.com/mediacenter/src/uploads/2015/02/Pandalabs2014-DEF2-en.pdf, 2015
175 Microsoft SIR v18, http://download.microsoft.com/download/7/1/A/71ABB4EC-E255-4DAF-9496-A46D67D875CD/Microsoft_Security_Intelligence_Report_Volume_18_English.pdf, 2015
176 Trend Micro, 2014 Annual Security Roundup, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-annual-security-roundup-magnified-losses-amplified-need-for-cyber-attack-preparedness/, 2015
177 Symantec, 2015 Internet Security Threat Report, http://www.symantec.com/security_response/publications/threatreport.jsp, 2015
178 APWG, Global Phishing Report 2H 2014, http://internetidentity.com/wp-content/uploads/2015/05/APWG_Global_Phishing_Report_2H_2014.pdf, 2015

CYBERCRIME HEAT MAP

The heat map below highlights the countries and jurisdictions where EU cybercrime investigations have identified offenders and/or infrastructure. This data relates to both cyber-dependent crime and cyber-enabled fraud and does not include investigations into online child sexual abuse.

With the exception of investigations that led to the US, UK and Germany, fewer than one third of investigations led to an MLAT request being submitted to the country identified as the location of an offender or criminal infrastructure. Whether this reflects alternate means of data sharing, the responsibility of requesting or providing assistance falling to another jurisdiction (including the one in question) as part of a coordinated multi-jurisdictional operation, or simply a lack of confidence in the MLAT system is unclear.





GENERAL OBSERVATIONS

Cybercrime is becoming more aggressive and confrontational. The evolution of cybercrime reported in this document shows that there is a shift from hidden, stealthy interventions by highly competent hackers towards direct, confrontational contact between the criminal and the victim, where the victim is put under considerable pressure to comply with the perpetrator's demands. This is seen in cases of extortion with DDoS attacks, in the deployment of ransomware, and in sextortion. It is also expected in relation to breaches of sensitive personal data, such as dating sites. The psychological impact on victims is much stronger due to the brutal confrontational manner in which the victim is coerced. It can be likened to the difference between a burglary where the victim detects afterwards that things have been stolen, versus an armed robbery where the victim is forced to hand over personal belongings to the criminal. The shift of crime type also suggests a change of perpetrator responsible for such crimes. The traditional, technically skilled hacker is unlikely to match the profile for the types of extortion that require muscles instead of any technical competence. The aggressive confrontation of victims is rather the trademark of traditional crime groups and organised crime gangs that are apparently increasingly turning to the profitable business of cybercrime.

Law enforcement has convincingly demonstrated its competence in dealing with cybercrime. It has achieved great successes in the past 12 months, yet it is fair to state that none of those would have been possible without close cooperation and collaboration with international law enforcement partners and private industry. Such levels of engagement are not simply advantageous, they are paramount. Fighting cybercrime is a shared responsibility and one that cannot be shouldered by law enforcement alone.

An important factor is the alignment of operational activities at EU level as part of the EMPACT policy cycle. This has contributed substantially to the better focussing of law enforcement attention and to jointly investigate and arrest key targets.

The newly established Joint Cybercrime Action Taskforce (J-CAT) was involved in several of the operations outlined in this assessment and contributed significantly to the successes. This J-CAT is a standing operational team of cyber liaison officers from several EU Member States and non-EU cooperation partners, co-located at Europol headquarters and complemented with EC3 staff. It is tasked to conduct, as a team, the most important and complex cybercrime investigations, in close cooperation and coordination with the cybercrime divisions of the seconding States. It serves as an impressive example of efficient and effective global cooperation in fighting cybercrime.

The effect of the positive results is witnessed in an even stronger willingness of partners from law enforcement, the private sector and academia to contribute and cooperate. This report mentions the changes in reporting data breaches and working with law enforcement by victimised companies. The same applies to victims in the financial sector and e-commerce. For law enforcement the need for a truly international orientation has also become more obvious.

Despite these successes, the known difficulties remained and were handled in the best way possible considering the constraints. These included:

- the lack of judicial cooperation possibilities with several countries outside the EU (Eastern European States, including Russia and countries in Southeast Asia);
- inefficient information exchange processes, in particular with private sector parties. For investigations, the use of the JIT framework has proven helpful in the sense that the MLAT procedures are not required between the co-signatory countries;
- unclear or unaligned legal frameworks within the EU, in particular in regard to the application of various coercive measures, undercover work, data retention, online detection, lawful interception, decryption, operational involvement of private sector partners in takedowns and the (lack of) regulation of virtual currencies.

The impact of investigations can be increased by well-considered tactics. In order to effectively tackle cybercrime, it is

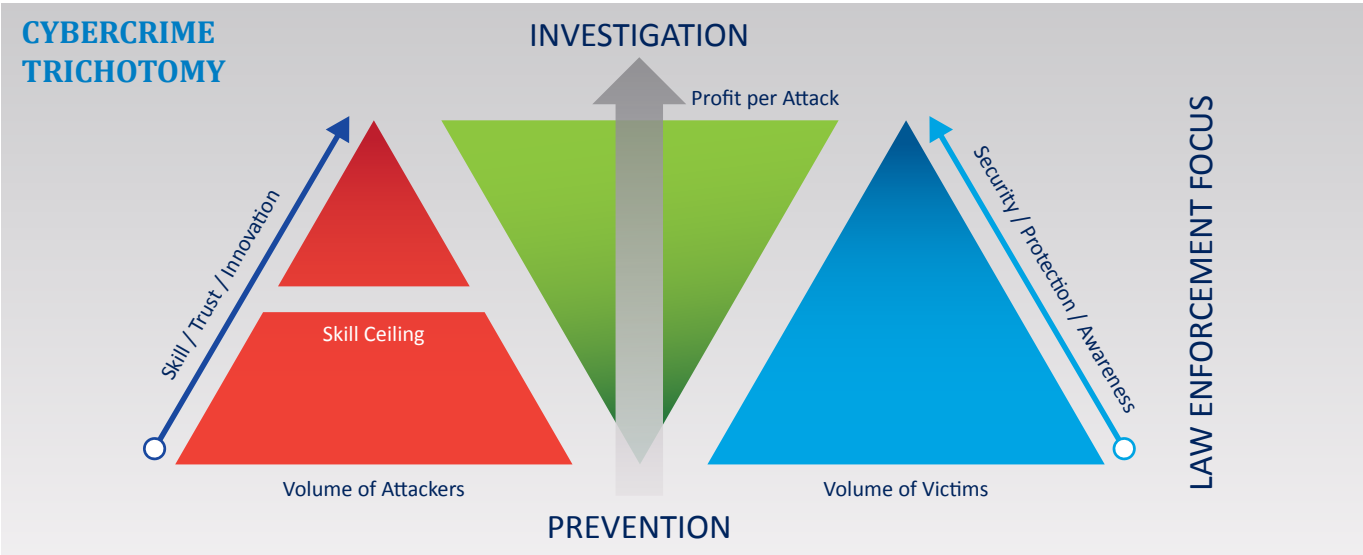
worth considering taking a revised approach. For example, while targeting those developing the current, high-profile malware affecting EU citizens may seem the obvious response, there is no shortage of skilled coders willing and able to take their place. Therefore although such a course of action may result in convictions, it may ultimately have limited long-term impact on the cybercrime community. However, many law enforcement agencies are restricted, and in some cases legally required, to investigate such cases which demand both time and resources.

Law enforcement therefore requires the both the capacity and legal authority to tackle the underlying array of cybercriminals who have enabled that crime to happen and perhaps continue to do so. Crime-as-a-service acts as a multiplier for many facets of cybercrime. Services such as bulletproof hosting, spam, illegal currency exchanges, money mules and counter anti-virus may not be the direct subject of a criminal complaint yet may have been crucial to those offences being committed. Many of these services support a wide range of criminality from malware development to CSE, and often involve a greater human and trust component, making them harder to replace. Similarly, disrupting shared criminal infrastructure can impact on multiple OCGs at once, increasing their costs and effort to operate.

Moreover, cybercrime investigations are often complex and resource intensive. Law enforcement therefore must be granted the latitude it requires in order to conduct long-term, comprehensive investigations for maximum impact without undue pressure to obtain rapid results or arrests.

The fight against cybercrime must encompass more than catching criminals, however. Investment in prevention and protection initiatives is also essential and can guard against many facets of cybercrime at once. Every well-educated and informed child, consumer or organisation is one easy prey less. There will never be an end to criminality; therefore a more prudent response is surely to build a solid defensive foundation.

Further considerations to assess the best tactics for tackling cybercrime can look at the relationships between attackers and their targets in terms of technical complexity of attacks, the level of protection and the value of the criminal profits per attack. These have been schematised in the following Cybercrime Trichotomy:



The above diagram is a simplified model which aligns representations of the volume of attackers by their technical capability against the potential profits of an attack and the volume of potential victims by their asset value/security/awareness levels. The model generalises to some degree as there are likely to be many exceptions.

The red pyramid characterises cybercriminals. Here we recognise a broad base of attackers with a low technical capability who can buy access to the skills and tools they lack (crime-as-a-service). At this level there is little or no innovation and only existing tools and methods are used. As skill levels increase, so do the levels of innovation and with it the trust requirements for cybercriminals to work increasingly collaboratively. Finally at the top of the pyramid there resides the smaller group of highly-skilled individuals that exist within tight circles of trust and where the true potential for innovation lies. This pyramid also highlights the skill ceiling from where cybercriminals can no longer buy progression but must evolve and develop their own skills and specialisations.

The blue pyramid represents victims (citizens/organisations/businesses). Here it is assumed that there is again a broader base of victims who lack the technical competence or security awareness required to sufficiently protect themselves and a smaller number of potential victims who have achieved a high level of security and are therefore harder to target. It is also assumed that the value of the victim's assets at risk increases towards the top and that the victim's willingness to invest in protection therefore also increases.

The green pyramid represents potential profits per attack. As a general rule it is assumed that the more sophisticated the technical competence of the attacker is, and the more valuable the vulnerable assets of the victim are, the higher the profit will be.

The diagram can be read horizontally across the three categories. The high number of attackers with low technical skills are likely to only be able to target the victims with poor security awareness. Such attacks are likely to be less profitable. Conversely, the more sophisticated and organised attackers are able to pursue higher-value targets who typically have greater security in place.

Interestingly, the model also shows why CEO fraud can be perceived as an exception to the rule. Whilst the technical security in place for high-value targets may be high, the technical skills of the offender can be rather low as long as the vulnerable human factor can be successfully addressed to commit the scam in a way that circumvents the technical protection.

The figure also suggests what the most appropriate and effective law enforcement response should be. In the lower part of the diagram, which represents the two broad populations of both cybercriminals and victims, a strategy focussed on prevention and protection would be most effective. Such a strategy is more suited for reaching larger target audiences and could be effective in either preventing novice cybercriminals from becoming further engaged in cybercrime, and in raising awareness of online security amongst potential victims. Progressing up the diagram, prevention strategies will become less effective as cybercriminals are likely to be more steadfast in their activities and potential victims require less education and personal investment in online security. A suitable law enforcement response therefore must include increasingly traditional investigative measures.

Cyber security is lagging behind. Although solutions for many of the exploited vulnerabilities are available, the delay in implementing the remedies or even the absence thereof contributes to the ease with which malware can be re-sold and re-used successfully, even by technically unskilled criminals. An increased awareness of the importance and preventive impact of sound digital hygiene should be envisioned. Also the lack of security orientation in the design of new devices that in one way

or another operate in connection with the Internet, has a major impact on cybercrime. The vulnerabilities of these have already turned these so-called 'smart devices' into important facilitators of botnet attacks. In the absence of proficient self-regulation by the industry, the introduction of minimum security requirements should be considered by the legislator. Similar measures in the automobile industry have had a huge positive effect on the safety of cars. For the various partners in law enforcement, the private sector, the Internet security industry, NGOs and education, there is the continued obligation to create awareness on developing cyber security risks so that citizens and businesses can protect their IT assets and communication devices properly.

There is an increasing eagerness to transfer the losses resulting from cybercrime. In regard to payment fraud it was mentioned previously that EMV technology on payment cards is expected to be introduced in the USA in autumn this year. Interestingly, this EMV implementation is linked to the transfer of liability for fraud-related losses from card issuers to merchants. With cybercrime-inflicted damages on the rise, the development and sales of insurance products to mitigate the risk of cybercrime are likely to grow further in the future. The positive influence that could derive from that development is that the height of the insurance fee may become dependent on the security precautions taken. As such, the cost of cybercrime will eventually end up as an expense to be balanced against the investment in cyber security. By whom that expense will be borne is a different, more complicated question for which the answer will heavily depend on the willingness of the legislator to tie liability to responsibility. Are the manufacturers of 'smart devices' liable for damages resulting from easy breaches by criminals? Does the legislator want those manufacturers to take liability for failing to include security into the equation of their product development?

Responsibility should also be considered in relation to data processing. And especially in this respect there are several questions pending: for instance, who is responsible for facilitating network traffic to and from .onion addresses, in particular those known to facilitate trade in weapons, drugs, payment credentials and counterfeit documents, and the exchange of child abuse material? Is this ICANN? They claim they never issued any .onion extensions. Is this the IETF then, whose architecture of the Internet still supports the processing of domain names that were not officially issued? But they just deal with the technical design and do not process any data. Or does the responsibility then lie with the operators running the major global nodes? The local ISP? Or is the Tor Project eventually responsible? Is it maybe a shared responsibility? More importantly, what are these entities doing to prevent the Tor network from being abused by criminals to mask their identities while exploiting the anonymity for their online criminal activities? What policies do those entities enforce to safeguard the virtues of Tor for genuine freedom of speech? What measures are they taking to discharge themselves responsibly of their respective obligations to contribute to a safe Internet? And if they don't take any measures, can they then be held accountable for the damage caused and liable for the losses suffered?

The right to privacy is gaining ground at the expense of the right to protection. This is seen in the context of data retention of Internet communications and was especially highlighted in recent discussions on encryption. The revelations on electronic mass surveillance seem to have shifted the balance towards maximising the individual's protection against any governmental possibility to interfere with their privacy. The result is that law enforcement services have increasing difficulties to protect citizens against the intrusion of their privacy against hacking, theft of sensitive personal data and other types of cybercrime, because any trace or evidence of such criminal activities are probably not retained and if retained, are increasingly more difficult to access due to sophisticated encryption. It may appear as if these rights are confused here, and therefore it is worth citing Article 12 of the Universal Declaration of Human Rights, which should serve as the basis for the legal principle:

> ***No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.***

The essential difference between hackers intruding the privacy of citizens to commit crimes, versus law enforcement having competences to gain lawful access to the communication data and the content of communications of that hacker in relation to that crime, is the word *arbitrary* in the cited Article. It is up to the legislator to ensure that conditions and modalities under which law enforcement can be explicitly authorised to intrude the privacy of suspects are clearly defined and confined, and systematically observed and audited. However, excluding law enforcement from gaining access under any circumstance, *de*

jure or *de facto*, will neither help to protect the privacy of citizens nor hold in the long run.

The speed at which society and crime 'cyberise' exceed the speed at which law enforcement can adapt. The overall development in which the society becomes increasingly dependent on the Internet has many implications for policing, both in terms of opportunities and challenges. Collecting evidence in relation to a murder is likely to involve forms of digital evidence. Mobile devices, CCTV footage, board computers, cloud storage, online purchases and virtual currencies can all contribute to establishing the whereabouts, contacts and financial transactions of the victim that may lead to finding the killer. Knowing the possibilities will increase the chances of solving crimes, also those that are not related to any form of cybercrime. It will, however, put increasing pressure on the computer forensic capabilities to keep up with the increasing workload.

In addition, there is a continuous shift from traditional crimes to cybercrime, especially since CaaS makes it easy to access for non-tech-savvy criminals, and profits are still attractive. Now, where traditional high-volume crimes, like burglaries and shoplifting, are dealt with in the first instance by local police services, the modern types of simple high-volume crimes, like the use of stolen payment credentials for online shopping, are often too complicated for the local police to deal with. Often, they also lack the geographical relation to the area to make it relevant for the local constabulary. Hence, the cyber-related high-volume crimes also end up with the more specialised cyber divisions that are not resourced to deal with this influx.

The third development worth considering in this context is that the abuse of technology to mask and hide crimes, including obfuscation and encryption, becomes so easy for the non-tech-savvy criminals, that advanced forensic skills and tools need to be developed constantly so that law enforcement can stay in the race.

These considerations call for continued prioritisation of training and resourcing of cyber capabilities at all levels of policing, both technically and in staff quantities.

APPENDICES

A1. THE ENCRYPTION DEBATE

It is axiomatic that if criminals have a means of communicating, which law enforcement agencies cannot understand, then it is a serious impediment to both detection and investigation. The main focus for the debate around this topic has been the use of encryption by criminals: encryption that is so powerful that it is impractical to decipher any communications using these techniques. It is understandable that governments are expressing concern about their ability to both protect people from criminal and extremist behaviour, and to bring those responsible to justice.

The most simplistic approach to the situation is to make the use of encryption illegal for anything other than a specific set of electronic interactions. This is based upon the argument that only criminals would wish to use encryption. The corollary is that law-abiding citizens have no need (or desire) to secure their communications, and that the desire for privacy is not an acceptable end in itself. However, most appear to now accept that is logic is flawed. Data collected by mass surveillance, if retained, may be misused at some future point. Governments change and the reason for the initial action may not be that for which the data is subsequently used, in addition to any 'mission creep'.

Especially in the wake of the information leaked by Edward Snowden, and the associated allegations of mass surveillance, there is greater concern among the wider population about privacy from government, as well as perhaps from the private sector: this is illustrated by the Eurobarometer data. It is argued that privacy is a fundamental human right, as stated in Article 12 of the UN Universal Declaration of Human Rights:

> ***No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.***

Many governments agree, but point out that this is a right to be protected from "arbitrary" interference with a person's privacy. Rather than a desire for arbitrary surveillance, some governments wish there to be a means by which only targeted criminals' communications can be deciphered, under appropriate oversight such as the need for the issuing of specific warrants. This sentiment was perhaps best summed up by a statement made by the UK Prime Minister, David Cameron:

> ***"Do we want to allow a means of communication between two people which even in extremis with a signed warrant from the home secretary personally that we cannot read?***
>
> ***My answer to that question is no, we must not. The first duty of any government is to keep our country and our people safe."***

Whilst this is a sentiment with which many, if not most, would agree, the problem is in the detail of how this is implemented. The possible means of achieving such a situation have been discussed many times and were well rehearsed in the late 1990s when several countries were attempting to deal with encryption whilst introducing legislation to cover investigatory powers. The reasons these mechanisms were rejected then remain valid today. In summary they are:

OUTLAW ENCRYPTION FOR GENERAL USE:

This is a technology that governments can no longer control. Unlike weapons of mass destruction, there is no large infrastructure needed to produce and distribute encryption technology. The technology is already widely and freely available. Trying to put it under control now would be impractical. In any event, even if legislation were passed in all EU Member States to outlaw encryption, and the wider population abided by this, it would not stop criminals using the technology. It would have the unfortunate effect of making those who abide by any such law more vulnerable to the very criminals who it is designed to handicap. This is exacerbated by the fact that if the EU Member States were to pass such a law, there is no guarantee that other countries would do the same. As organised crime is often committed across borders, it would be another dimension in which to frustrate the detection

and prosecution of criminals, not least via arguments about the propriety of mutual legal assistance.

Trying to restrict the distribution of encryption software is impractical. Even if one could prevent it leaving a country once produced there is nothing to stop the ideas travelling and being re-implemented in another country. We saw exactly this happen with PGP when the US government attempted to control its distribution outside of the US: it was simply reincarnated as PGP International.

It may be possible to enforce a blanket ban on encryption. If all the Internet service providers established technology to detect and block encrypted traffic it would be impractical to use encrypted communications into, out of, or within a country. However, attempting to differentiate between legitimate use of encryption and that being used by criminals would be a non-trivial task, and likely to be flawed unless all providers did exactly the same. It would also be relatively easy to circumvent by using virtual private networks, Tor, or some similar mechanism.

It also does not address the problem of using steganography. It is perfectly possible for criminals, again using widely and freely available technology, to disguise communications, and to encrypt those communications. Likewise the use of dead letter box style email accounts and similar covert means of communication would go undetected.

In the modern world we are increasingly dependent upon the Internet yet it was never designed to be a secure network. Layering encryption on top of the Internet is currently the only practical means of ensuring confidentiality, integrity and authenticity of our Internet based interactions.

KEY ESCROW:

It was mooted early on in the debate that anyone using encryption should be obliged to file a copy of their encryption key with either a government agency or possibly a trusted third party. If an authorised agency then needed to decrypt communications the key could be retrieved. There are several significant problems with this approach:

1. Modern encryption typically employs 'forward secrecy': the encryption key is changed for every new interaction. This is obviously not the case for something such as encrypted email using, say, PGP or an encrypted file using, say, TrueCrypt. However, increasing use is being made of communications services that can be both end-to-end encrypted, and are ephemeral. As a direct response to the concerns raised by the allegations of mass surveillance by the US and UK governments, companies with international users have sought to reassure them by constructing systems where even the service provider cannot decrypt the communications as they pass through their infrastructure: the key is known to no-one except the participants of the interaction.

2. The practicalities of ensuring that all encrypted communications are using a key that has been placed in escrow are, to all intents and purposes, insurmountable. It would only be when the authorities come to attempt to decrypt some criminal communications that they would discover that they did not have access to the key after all. If this were to work, an infrastructure would need to be developed that enabled only those communications for which a key was in escrow, and to block all others. We do not believe this is possible.

3. Recent history has taught us that connected databases are prime targets for hackers. There is a real danger that any datastore could be compromised by hackers, which would lay anyone who has placed their keys in escrow open to abuse by criminals. The massive breaches on the US Office of Personnel Management and DigiNotar, amongst others, demonstrate that both government and private trusted third parties are not immune from compromise, with devastating results to trust in government as well as practical consequences for some individuals thus harmed. There is also the very real danger of intentional misuse internally or simple incompetence leading to a breach.

4. The cross-border nature of modern organised crime means that a law enforcement agency in one country may need to apply to another government to retrieve a key. This would require international agreement. Whilst this is entirely possible amongst the EU Member States, and possibly between other like-minded governments, it is difficult to see how this might work across less friendly borders.

WEAKENED ENCRYPTION:

Many have suggested that only encryption which law enforcement agencies can 'crack' should be allowed. It has been suggested that this might be through the use of, for example, a weakened algorithm, restricted key lengths or the inclusion of a back door. All of these have the same issues: if you weaken encryption for your enemies, you do so for your friends. It no longer takes vast computing facilities to break weakened encryption, nor would it take a determined group of criminals long to find a back door.

The security community has been imploring users to ensure they use the latest encryption and extend their key lengths, precisely because the arms race between encryption and the ability of computing power to break it is continuous. Organised criminals have access to significant finances and some of the best technologists in the world so it would naïve to assume that governments would enjoy any form of advantage in breaking deliberately weakened encryption.

This approach was typified when the US government attempted to introduce the Clipper chip, which had a backdoor. It was announced in 1993 and was totally defunct by 1996 as it had been rendered impractical for all of the reasons discussed above.

The use of weakened encryption has a long-term impact as well. A recent vulnerability in Transport Layer Security (TLS) was discovered where hackers were able, in some implementations, to force an encrypted link to use an older 'export' grade encryption which was breakable by modern computers. Once such weakened encryption enters the wider environment, in order to maintain compatibility, especially backward compatibility, it has to be always possible to request that an interaction uses the weaker form of encryption: there will always be someone who is still using it and the way in which these interactions are established (between those who may not have communicated before) means that the initial dialogue moves to the lowest common denominator. Whilst these flaws are blocked off when disclosed, the applications that use them are very complex and it is almost inevitable that further such flaws will emerge based upon legacy weakened encryption. It would appear to compound the issue by reintroducing newly weakened encryption.

OBLIGATION TO DISCLOSE:

This appears to be the only practical method of handling encryption where the keys are held by individual users. Rather like refusing to take a breath test to see if you are over the drink driving alcohol limits, it is possible to make it an offence to disclose an encryption key that allows law enforcement agencies to examine encrypted data. This has the advantage of enabling a criminal to be prosecuted if he reveals his encrypted data or refuses to do so.

Internationally there are some courts that have been asked to consider such an action as tantamount to self-incrimination. However, on the whole it has been seen by the courts as justified as part of criminal investigations.

Unfortunately, this tends to be effective only when data remains on the suspect/criminal's computer. If the keys are transient, especially if they are system generated, it can be practically impossible to recover these. This is then compounded by the fact that the communication itself may be transient and not recorded, i.e. even if they key could be recovered, there is nothing to decrypt unless it has been captured through surveillance and recorded by the law enforcement agencies.

As mentioned above, this situation is complicated by the re-architecting of communications services for the likes of WhatsApp, iMessage, Facebook and Facetime, and the email services provided by Google and Yahoo, by enabling end-to-end encryption.

If there were a practical place where encryption could be tackled, it would be through achieving agreement with these service providers to implement security architectures that did not enable end-to-end encryption; if the communications were encrypted from each participant to the service provider but potentially readable on the service providers' systems, it would be possible for law enforcement agencies to present a suitable warrant to read the communications.

The issue that service providers have expressed is that their users are internationally based, and they would find it difficult to know which law enforcement agencies they should cooperate with. The companies providing these services are predominantly US based and their users have expressed concern that the US and its allies would be able to use such an architecture to conduct

mass surveillance. Similarly a US based company might be placed in an invidious position if law enforcement agencies from unfriendly countries made such requests, perhaps for politically motivated surveillance.

It was this dilemma that resulted in the introduction of end-to-end encryption in the first place.

The debate currently underway is one that quite rightly is being held in public. Whilst most would agree with the sentiments of wanting their law enforcers to have access to criminals' communications, the dilemma is the negative impact of the ways in which this would be achieved. However, one significant piece of data is missing from the debate: the scale of the problem. What is currently not in the public domain is the degree to which criminal detection and investigation is being hampered by the use of encryption by criminals.

It would seem that if a proper public debate is to be forthcoming, if legislators are to be trusted in what they wish to place into law, and if decisions on what inevitably will be compromises in security and privacy are to be evidence based, it is important that the problem is quantified in a way that earns the trust of most if not all members of the public. EC3 will be asking Member States if they will cooperate in providing the data to enable the nature of the problem (current and future potential) to be established.

A2. AN UPDATE ON CYBER LEGISLATION

The 2014 IOCTA emphasised that it is essential for law enforcement to closely observe developments in the field of law. Without criminal legislation the hands of law enforcement agencies are bound – and without adequate procedural law, the prosecution of high-tech offenders can be close to impossible.

UPDATE 1: EU CYBERCRIME LEGISLATIVE FRAMEWORKS

Since the publication of the last IOCTA, the European Union has not introduced a new legislative framework to harmonise the cybercrime legislation of the Member States. However, 4 September 2015 is an important date with regard to the 2013 EU Directive on Attacks against Information Systems[179]. Article 16 requires Member States to bring their legislation, regulations and administrative procedures in line with the requirements of that Directive by that date. With regards to criminalisation, the Directive does not go beyond the 2001 Council of Europe Convention on Cybercrime, which was implemented by most EU Member States; therefore the chances of an EU-wide transposition of the Directive are high.

UPDATE 2: COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

By August 2015, the number of ratifications/accessions to the 2001 Council of Europe Convention on Cybercrime increased to 47 countries, including eight non-members of the Council of Europe. Outside of Europe, Australia, Canada, the Dominican Republic, Japan, Mauritius, Panama, Sri Lanka and the United States are listed as non-Member States that ratified the Convention. The ratification of the Convention worldwide is an ongoing process with an average of more than three countries joining per year. Some of the fastest growing and most relevant economies outside of Europe, such as the BRIC countries (Brazil, Russia, India and China), with which European law

179 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

enforcement agencies frequently deal, have not yet been invited to accede to the Convention. Involvement of those countries would be a significant advantage for international law enforcement cooperation.

UPDATE 3: DATA BREACHES

Data breaches remain a major challenge and are certainly one of the fastest moving forms of what is widely seen as criminal activities. During the first half of 2015, millions of data records were obtained by attackers. CareFirst, Kaspersky Lab, Premera BlueCross, Harvard University and the US Government were just a few prominent victims of this type of attack. Unchanged since the 2014 IOCTA, a strong, harmonised legal approach towards this type of offence – one that includes the criminalisation of trading compromised identities – is still absent in Europe. Neither the 2001 Council of Europe Convention on Cybercrime, nor the existing EU legislative approaches specifically criminalise identity theft and the related transfer of identities. Consequently, the prosecution of such activities depends on the existence of national legislation.

UPDATE 4: INVALIDATION OF DATA RETENTION DIRECTIVE

Access to traffic and location data is of great relevance for law enforcement agencies, especially when it comes to the identification of perpetrators. The basis of the harmonisation of legislation with regard to the process of retaining such data was for some years the 2006 EU Data Retention Directive[180]. It contained an obligation for the providers of publicly available electronic communications services or of the public communications networks to store data, i.e. traffic data and location data and the related data necessary to identify the subscriber or user for the purpose of investigation, detection and prosecution of serious crime, as defined by each EU Member State in its national law. Despite different national approaches within the transposition process of the Directive, especially with regard to the duration of retention, it was an interesting legal harmonisation foundation.

However, on 8 April 2014, the European Court of Justice (ECJ) declared the Directive invalid[181]. The Court concluded that the retention of data as required by the Directive may be considered to be appropriate for attaining the objective pursued, but the wide-ranging and particularly serious interference of the Directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary. In this respect, the Directive did not comply with the principle of proportionality. As a consequence, the Member States are no longer bound by the Directive. National provisions implementing the Directive are nonetheless not automatically invalid, which lead to very significant discrepancies among EU national data retention provisions. The reactions of Member States have varied very much from one another. Some States have annulled their transposing legislation (e.g. Austria, Belgium, Slovakia and Slovenia), some have not changed their legislation since the ECJ ruling (e.g. Ireland, Spain and Sweden) and some, such as the United Kingdom, have reacted drastically by enacting a new legislation providing for a new legal basis for data retention by service providers[182].

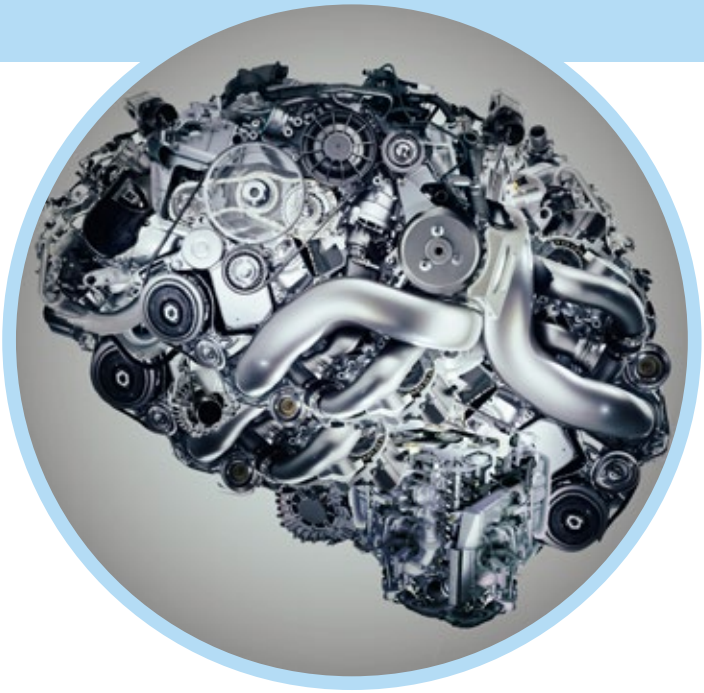
Generally, Member States are waiting for the EU to adopt a new Directive. However, it is currently uncertain whether and when the European Union will adopt a new legal instrument on this issue. It is clearly unlikely to happen very soon.

The usefulness of traffic data and location data for criminal investigations is defended by law enforcement agencies and prosecutors. It is true that accessing data after the commission of the offence, when it was not retained originally by service providers, may be more difficult or impossible if the data was

180 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks and amending directive 2002/58/EC, OJ L105.

181 ECJ, Digital Rights Ireland and Seitlinger and Others case, Joined Cases C-293/12 and C-594/12, 8 April 2014

182 The Data Retention and Investigation Act (2014) was declared invalid on 17 July 2015 by the High Court of Justice Queen's Bench Division, Divisional Court, *The Queen* v. *The Secretary of State for the Home Department*.



deleted in the meantime. Indeed, law enforcement agencies underline that the effectiveness of their work relies increasingly on the availability of data that is already collected, retained and made available by the service providers in a lawful manner. In particular, investigations related to serious crime typically require a more long-term approach as they may be longer than the average time of any other criminal investigation.

The magnitude of the impact of the ECJ ruling on investigations cannot be understated as the detection and investigation of cyber-enabled and cyber-facilitated crime relies extensively on the collection and analysis of telecommunications data. At least seven Member States stated that their data retention regime provides for up to six months of retention. Member States expressed that the inability to access case-relevant telecommunications data has affected a significant part of recent cybercrime investigations, leading to unsuccessful investigations in areas such as computer intrusion, hacking and child abuse.

As criminals are increasingly using the Internet and/or technologies at their disposal, data retention is certainly an interesting means to gather information on typically Internet-related crime such as computer intrusion, hacking and child pornography online.

In addition to the retention period and from a more practical perspective, service providers often take a dysfunctionally long time to satisfy the request. Five Member States reported that a typical waiting period was more than one month. In addition, there is little standardisation in the format of the response. Some States indicated that data may not be provided in electronic format, which leads to a waste of resources spent on the collation and interpretation of hard copy data.

A3. COMPUTER CRIME, FOLLOWED BY CYBERCRIME FOLLOWED BY .... ROBOT AND AI CRIME?

AN OUTLOOK INTO CRIMINAL OFFENCES RELATED TO ARTIFICIAL INTELLIGENCE

It is currently difficult to say if the ongoing process of automation and the increasingly rapid advances in and application of artificial intelligence (AI) present more of a challenge or an opportunity for law enforcement – the underlying problem from a crime development perspective was already briefly addressed in the 2014 IOCTA.

Artificial intelligence and Big Data analysis have the potential to provide significant input to the work of law enforcement[183] – if it is possible to overcome legitimate concerns related to data protection and fundamental human rights. However, as with all new developments, there is potential for abuse as is evident, for instance, in the increasing number of targeted attacks against automated systems, such as modern, computer-controlled factories.[184] Stuxnet was certainly only the first widely discussed example of the capability of such attacks.[185] Taking into account that AI is ultimately a complex automated system, the threats are applicable to AI systems as well. Therefore the current situation can be aptly described as a combination of both opportunity and challenge.

In addition to the need to address the recent challenges of automation and AI it would be worthwhile to look a few years ahead with a view to trying to predict the impact of realistic and more mainstream AI applications on the work of law enforcement[186]. Artificial intelligence is an area that offers immense potential for new services and innovative products.

183 Alzou'bi/Alshibly/Ma'aitah, Artifical Intelligence in Law Enforcement, A Review, International Journal of Advanced Information Technology, Vol. 4, No. 4

184 Cardenas/Amin/Lin/Huang/Huang/Sastry, Attacks Against Process Controll Systems: Risk Assessment, Detection, and Response

185 Albright/Brannan/Walrond, Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 22.12.2010; Broad/Markoff/Sanger, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times, 15.01.2011; Kerr/Rollins/Theohary, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010; Timmerman, Computer Worm Shuts Down Iranian Centrifuge Plant, Newsmax, 29.11.2010

186 For a discussion on the application of AI in the context of the objectives and purposes of the Geneva Convention, specifically in relation to lethal autonomous weapons systems, http://www.unog.ch/80256EE600585943/

The success of AI-based systems in beating humans at playing video games by applying deep learning and deep reinforcement learning underlines, in a very illustrative way, the progress of this field[187]. The fact that the AI system was able to quickly pick up the rules of the game without being taught in advance attracted a lot attention even outside the scientific community[188]. Other visible signs of the integration of AI are for example Google's successful tests with self-driving cars[189] or the successful Turing test in 2014, which was seen as a major breakthrough in computer history[190]. What may sound like a nightmare vision to some is hope for major progress in road safety to others. Similar to 'airbags' and 'Collision Prevention Assist', self-driving vehicles could lead to a decrease in traffic accident-related injuries and fatalities. Google's monthly report for May 2015 indicates that, in six years of the project, more than a million miles of self-driving cars had been involved in 12 minor accidents – none of them caused by a self-driving car[191].

It would be naive to believe that these developments will not have an impact on society by introducing a number of potential challenges. For example, some statistics indicate that 'truck driver' remains the most common job in 29 out of 50 of the United States.[192] Recent reports predicting that self-driving trucks are only two years away could have a truly disruptive impact on this market[193].

When thinking about law enforcement implications, the discussion about 'hacked' cars might be one of the obvious responses. However, this topic is far away from being visionary as the integration of computer and network technology in cars continues at high speed. Already back in 2002 Forbes brought this issue to the attention of a wider public[194]. In 2013 Volkswagen tried to stop the publication of research on how to hack anti-theft systems[195]. And Wired reported about potential and real attacks in 2014 and in 2015[196]. This is of course not limited to smart cars but applies to smart devices in general.

The practical relevance of these developments for law enforcement is primarily related to the ability to prevent such crimes and to have the forensic capabilities to investigate them. The advantage is that these attacks are covered by up-to-date legal systems. With regard to the potential impact there are certainly differences between hacking a desktop computer and a computer system in a car – however, from a legal point of view, both are quite similar.

Therefore it might be worth looking ahead to the developments that we could expect in the coming years. One issue that could become a true challenge for law enforcement is the involvement of AI-based machines in the commission of crime. Machines are already widely used to automate production processes[197]. This has also led to automation-related accidents and incidents, a recent example being the case of a worker 'killed' by a robot in a car manufacture company in Germany, which stimulated a public debate[198]. Unfortunately this is not the first time that somebody lost his life due to a malfunction of a robot – the first reported incidents were filed more than 30 years ago[199]. And, as old, is the debate about legal and ethical implications.

But the relevance of the debate might quickly change. While

187 Mnih/Kavukcuoglu/Silver/Rusu/Veness/Bellemare/Graves/Riedmiller/Fidjeland/Ostrovaski/Petersen/Beattie/Sadik/Antonoglou/King/Kumaran/Wierstra/Legg/Hassabis, Human-level control through deep reinforcement learning, Natur, 2015

188 McMillan, Google's AI is now smart enough to play Atari like the Pros, Wired Magazine, 2015

189 KMPG, Self-driving Cars: The Next Revolution, https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/self-driving-cars-next-revolution.pdf, 2012

190 University of Reading, Turing Test Success Marks Milestone in Computing History, http://www.reading.ac.uk/news-and-events/releases/PR583836.aspx, 2014

191 Google Self-Driving Car Project, Monthly Report, May 2015

192 Balance Sheet Solutions, Weekly Relative Value, http://www.balancesheetsolutions.org/stored/pdf/WRV062915.pdf, 2015

193 *Prigg*, Self-Driving trucks are just two years away says Daimler as it is set to get go-ahead for trials on German roads within months, Daily Mail, 27.07.2015

194 Fahey, How to Hack Your Car, Forbes, 7.8.2002

195 Volkswagen sues UK university after it hacked sports cars, The Telegraph, 30.7.2013

196 Greenberg, Hackers could take control of your car. This device can stop them, Wired 22.7.2014; Greenberg, Hackers remotely kill a jeep on the highway – with me in it, Wired, 21.7.2015

197 Singh/Sellappan/Kumaradhas, Evolution of Industrial Robots and their Applications, International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Issue 5, 2013

198 Robot kills worker at Volkswagen plant in Germany, The Guardian, 2.7.2015

199 Dennet, When HAL Kills, Who's to Blame? Computer Ethics, in Stork, Hal's Legacy: 2001's Computer as Dream and Reality, 1997

the malfunction of a machine can rather easily be handled as an accident that does not require intensive criminal investigations, the increasing use of AI could be a game changer. While a concluding discussion would go well beyond the scope of this Appendix, four main issues of relevance to the debate should be briefly mentioned. Before doing so, however, the fact that this is already of practical relevance today can be easily demonstrated by the following example[200]: an AI-based self-driving car is driving along a narrow road with concrete bollards on both sides. All of a sudden a child jumps right on the street. In response, the AI system may identify several different options. Without any action or even by performing an emergency stop the car would hit the child and may seriously injure or even kill her/him. To avoid the collision the car's AI system may instead decide to make a right or left turn. The crash into the concrete bollards could seriously injure or even kill the passenger. The same or similar situations have been discussed in criminal law for decades – with the difference being that it is a human being who takes the decision in those conflict situations.

- The first question arising is the general question of liability. Who will be made responsible? The hardware production company? The AI software company? The implementer? This question, which has been discussed in literature to some extent[201], will require further attention, especially with regard to the required capacities to analyse the underlying reasoning process – which can be challenging taking into account the complexity of the systems and algorithms.

- But the challenge for law enforcement is going beyond this. The story about AI beating humans in video games by learning the rules of the game without pre-programming them shows that one essential component of AI is that that the system is going beyond what was programmed. Therefore the differentiation between action and omission will become even more relevant in the future. Not having implemented measures to restrict possible action of AI-based systems could in the future be the focus of law enforcement investigations against manufacturers of such systems. And it might even be necessary to customise their 'ethical and legal value system' to differing ethical and legal systems.

- The third element that will need to be further discussed is *mens rea* or the 'guilty mind'. Just like general aspects of liability and the differentiation between action and omission, *mens rea* is a fundamental element of criminal law[202]. It is ultimately the concurrence of intelligence and violation[203]. The question is if this includes artificial intelligence. This is certainly not the traditional understanding of *mens rea*. The application of traditional criminal law provisions to crimes involving AI could therefore go along with unique challenges and raises the question if we need a specific legal regime for AI or if it is favourable or even essential to apply one legal framework to AI and non AI-base criminal activities.

- Finally what will be the consequences and penalties that will be applied? Imprisonment will most likely not be a suitable option. The challenge is not new; within the debate about criminal liability of legal persons, similar challenges were discussed. But in this context even applying fines and financial penalties goes along with unique challenges204.

This brief overview underlines some of the challenges for law enforcement that might be worth observing already at this early stage. It certainly includes rather philosophical questions like: Do we expect AI to act better than humans? But ultimately it also includes questions related to the core work of law enforcement: The application of law and enforcement.

200 http://www.bloomberg.com/news/articles/2015-06-25/should-a-driverless-car-decide-who-lives-or-dies-in-an-accident-

201 Bloomberg, Should a Driverless Car Decide Who Lives or Dies?, http://www.bloomberg.com/news/articles/2015-06-25/should-a-driverless-car-decide-who-lives-or-dies-in-an-accident-, 2015

202 Llewelyn/Edwards, Mens rea in statutory offences, 1955

203 *Hall*, General Principles of Criminal Law, 2005

204 A recent report by the RAND Corporation provides an interesting overview of how emerging and future Internet technologies can strengthen the work of law enforcement and the judiciary. In relation to smart or driverless cars, the report suggest developing policies, procedures and technical interfaces that take into account law enforcement requirements. http://www.rand.org/content/dam/rand/pubs/research_reports/RR900/RR928/RAND_RR928.pdf

PHOTO CREDITS

Pictures © Shutterstock, 2015,
Page 51: © ChameleonsEye / Shutterstock.com

2015 — 76 pp. — 21 × 29.7 cm

ISBN 978-92-95200-65-4
ISSN 2363-1627
DOI 10.2813/03524

EUROPOL

EUROPEAN LAW ENFORCEMENT AGENCY

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands
PO Box 90850
2509 LW The Hague
The Netherlands

Website: www.europol.europa.eu
Facebook: www.facebook.com/Europol
Twitter: @Europol_EU @EC3Europol
YouTube: www.youtube.com/EUROPOLtube

QL-AL-15-001-EN-N