

# ■ IOCTA 2016

## INTERNET ORGANISED CRIME THREAT ASSESSMENT





Internet Organised Crime Threat Assessment  
(IOCTA) 2016

European Police Office (Europol)  
P.O. Box 908 50  
2509 LW The Hague  
The Netherlands

This publication and more information on Europol  
is available online:

[www.europol.europa.eu](http://www.europol.europa.eu)  
[www.facebook.com/Europol](https://www.facebook.com/Europol)  
[www.youtube.com/EUROPOLtube](https://www.youtube.com/EUROPOLtube)  
Twitter: @Europol and @EC3Europol

All images © Shutterstock  
except pages 5, 8, 31, 53, 54 and 57 © Europol.

ISBN 978-92-95200-75-3  
ISSN 2363-1627  
DOI 10.2813/275589  
QL-AL-16-001-EN-N

© European Police Office, 2016

Reproduction is authorised provided the source is  
acknowledged. For any use or reproduction of individual  
photos, permission must be sought directly from the  
copyright holders.



# ■ CONTENTS

<b>5</b>	FOREWORD
<b>6</b>	ABBREVIATIONS
<b>7</b>	EXECUTIVE SUMMARY
<b>10</b>	KEY FINDINGS
<b>12</b>	KEY RECOMMENDATIONS
<b>15</b>	SUGGESTED OPERATIONAL PRIORITIES
<b>16</b>	INTRODUCTION
<b>17</b>	MALWARE
<b>24</b>	ONLINE CHILD SEXUAL EXPLOITATION
<b>28</b>	PAYMENT FRAUD
<b>32</b>	SOCIAL ENGINEERING
<b>35</b>	DATA BREACHES AND NETWORK ATTACKS
<b>39</b>	ATTACKS ON CRITICAL INFRASTRUCTURE
<b>42</b>	CRIMINAL FINANCES ONLINE
<b>45</b>	CRIMINAL COMMUNICATIONS ONLINE
<b>47</b>	DARKNETS AND HIDDEN SERVICES
<b>49</b>	THE CONVERGENCE OF CYBER AND TERRORISM
<b>52</b>	BIG DATA, IOT AND THE CLOUD
<b>56</b>	INTERNET GOVERNANCE
<b>59</b>	THE GEOGRAPHIC DISTRIBUTION OF CYBERCRIME
<b>64</b>	APPENDICES





## ■ FOREWORD

I am pleased to introduce the 2016 Internet Organised Crime Threat Assessment (IOCTA), the annual presentation of the cybercrime threat landscape by Europol's European Cybercrime Centre (EC3).

The 2016 report provides a predominantly law enforcement focused assessment of the key developments, changes and emerging threats in the field of cybercrime over the last year. It is based on valuable contributions by EU Member States and the expert input of Europol staff, which has been further enhanced and combined with input from our partners in private industry, the financial sector and academia.

The assessment confirms that cybercrime remains a real and significant threat. It also highlights how those criminal techniques and methods which have traditionally been associated with cybercrime are extending into other crime and threat areas. A growing range of threats, from trafficking in human beings to terrorism, are becoming increasingly cyber-facilitated. Other cross-cutting issues, such as the growing misuse of legitimate anonymity and encryption services and tools for illegal purposes pose a serious impediment to detection, investigation and prosecution of criminals.

The report provides a number of key recommendations to address the issues and challenges outlined, 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 clear actions under the three main mandated areas of the EC3 – cyber attacks, child sexual exploitation online, and payment fraud – such as: targeting criminals providing essential services and developing key tools which facilitate the activities of their criminal counterparts; eliminating communities which promote the production and sharing of child sexual exploitation material; and co-ordinated action to combat money mules.



The 2016 IOCTA will inform the setting of priorities and help streamline resources within the EU and internationally to respond to cybercrime in an effective and concerted manner, supported by Europol. Despite the increasing challenges, the last 12 months have demonstrated that a coordinated approach by EU law enforcement that includes all relevant partners can result in significant successes in the fight against cybercrime, including in the important areas of prevention and awareness. I am confident that this will continue and improve in the years to come.

**ROB WAINWRIGHT**  
**DIRECTOR OF EUROPOL**

# ABBREVIATIONS

ADSL	Asymmetric Digital Subscriber Line	IPv4	Internet Protocol version 4
AI	artificial intelligence	IPv6	Internet Protocol version 6
API	Application Programming Interfaces	IRC	Internet Relay Chat
APT	Advanced Persistent Threat	IRU	Internet referral unit
ATM	automated teller machine	ISP	Internet service provider
AV	anti-virus	IT	information technology
BPH	bullet proof hosting	J-CAT	Joint Cybercrime Action Taskforce
C&C	command and control	KYC	Know Your Customer
C2C	Criminal to Criminal	LEA	law enforcement agency
C2V	Criminal to Victim	MIT	Massachusetts Institute of Technology
CaaS	Crime-as-a-Service	MLAT	mutual legal assistance treaty
CEO	chief executive officer	MTIC	missing trader intra-community (fraud)
CERT	computer emergency response team	NAT	Network Address Translation
CGN	Carrier-Grade Network Address Translation	NCA	National Crime Agency
CI	critical infrastructure	NCT	National Childbirth Trust
CNP	card-not-present	NFC	Near Field Communication
CSE	child sexual exploitation	NGO	non-governmental organisation
CSEM	child sexual exploitation material	NIS	network and information systems
CSI	criminal suspects and/or infrastructure	NIST	National Institute of Standards and Technology
CSIRT	Computer Security Incident Response Team	OCG	organised crime group
CTB	Curve-Tor-Bitcoin	OPSEC	operations security
DCPCU	Dedicated Cheque and Plastic Crime Unit	OSINT	open-source intelligence
DD4BC	Distributed Denial of Service for Bitcoin	P/P	privacy/proxy
DDoS	Distributed Denial of Service	P2P	peer to peer, or people to people
DLT	Distributed Ledger Technology	PBX	Private Branch Exchange
DNS	Domain Name System	PDP	Policy Development Process
EBF	European Banking Federation	PIN	personal identification number
EC3	European Cybercrime Centre	PoS	point-of-sale
EMAS	Europol Malware Analysis System	RAT	Remote Access Tool
EMMA	European Money Mule Actions	SCADA	supervisory control and data acquisition systems
EMPACT	European Multidisciplinary Platform Against Criminal Threats	SEPA	Single Euro Payments Area
EMV	Europay, MasterCard and Visa	SGIM	self-generated indecent material
EUCTF	European Cybercrime Task Force	SOCTA	Serious and Organised Crime Threat Assessment
EWG	Expert Working Group	SQL	Structured Query Language
gTLD	Generic Top Level Domain	TCP/IP	Transmission Control Protocol/Internet Protocol
I2P	Invisible Internet Project	THB	trafficking in human beings
ICANN	Internet Corporation for Assigned Names and Numbers	TLD	top-level domain
ICT	information & communications technology	Tor	The Onion Router
IOCTA	Internet Organised Crime Threat Assessment	URL	uniform resource locator
IoT	Internet of Things	V2C	Victim to Criminal
IP	Internet protocol	VoIP	Voice-over-Internet Protocol
		VPN	virtual private network
		VR	virtual reality



# EXECUTIVE SUMMARY



The 2016 Internet Organised Crime Threat Assessment (IOCTA) reports a continuing and increasing acceleration of the security trends observed in previous assessments. The additional increase in volume, scope and financial damage combined with the asymmetric risk that characterises cybercrime has reached such a level that in some EU countries cybercrime may have surpassed traditional crime in terms of reporting<sup>1,2</sup>. Some attacks, such as ransomware, which the previous report attributed to an increase in the aggressiveness of cybercrime, have become the norm, overshadowing traditional malware threats such as banking Trojans.

The mature Crime-as-a-Service model underpinning cybercrime continues to provide tools and services across the entire spectrum of cyber criminality, from entry-level to top-tier players, and any other seekers, including parties with other motivations such as terrorists. The boundaries between cybercriminals, Advanced Persistent Threat (APT) style actors and other groups continue to blur. While the extent to which extremist groups currently use cyber techniques to conduct attacks appears to be limited, the availability of cybercrime tools and services, and illicit commodities such as firearms on the Darknet, provide ample opportunities for this situation to change<sup>3</sup>.

Many of the key threats remain largely unchanged from the previous report. Ransomware and banking Trojans remain top malware threats; a trend unlikely to change for the fore-

seeable future. While the same data stealing malware largely appears year-on-year, ransomware – a comparatively more recent threat – is in greater flux and may take several more years before it reaches the same level of equilibrium.

Peer-to-peer networks and the growing number of forums on the Darknet continue to facilitate the exchange of child sexual exploitation material (CSEM); while both self-generated indecent material (SGIM) and content derived from the growing phenomenon of live-distant child abuse, further contribute to the volume of CSEM available.

EMV (chip and PIN), geoblocking and other industry measures continue to erode card-present fraud within the EU, forcing criminals to migrate cash out operations to other regions. Logical and malware attacks directly against ATMs continue to evolve and proliferate. The proportion of card fraud attributed to card-not-present (CNP) transactions continues to grow, with e-commerce, airline tickets, car rentals and accommodation representing the industries hit hardest. The first indications that organised crime groups (OCGs) are starting to manipulate or compromise payments involving contactless (NFC) cards have also been seen.

The overall quality and authenticity of phishing campaigns has increased, with targeted (spear) phishing aimed at high value targets - including CEO fraud - reported as a key threat by law enforcement and the private sector alike.

<sup>1</sup> Office for National Statistics, Crime in England and Wales: year ending Mar 2016, <https://www.gov.uk/government/statistics/crime-in-england-and-wales-year-ending-mar-2016>, 2016

<sup>2</sup> NCA Strategic Cyber Industry Group Cyber Crime, Cyber Crime Assessment 2016, <http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file>, 2016

<sup>3</sup> European Union Terrorism Situation and Trend Report (TE-SAT) 2016, <https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-te-sat-2016>, 2016

DDoS attacks continue to grow in intensity and complexity, with many attacks blending network and application layer attacks. Booters/stressers<sup>4</sup> are readily available as-a-service, accounting for an increasing number of DDoS attacks. While other network attacks aimed at exfiltrating data continue to focus on financial credentials, there is a growing trend in the compromise of other data types, such as medical<sup>5</sup> or other sensitive data or intellectual property for other purposes.

Cryptocurrencies, specifically Bitcoin, remain the currency of choice for much of cybercrime, whether it is used as payment for criminal services or for receiving payments from extortion victims. Even so, key members of the Bitcoin community, such as exchangers, are increasingly finding themselves the victim of cybercriminals.

The growing misuse of legitimate anonymity and encryption services and tools for illegal purposes poses a serious impediment to detection, investigation and prosecution, thereby creating a high level of threat cutting across all crime areas. For law enforcement in particular, this creates a dichotomy of value. Strong encryption is highly important to e-commerce and other cyberspace activity, but adequate security depends on police having the ability to investigate criminal activity.

This report highlights some areas of innovation within the cybercriminal community, but also how much of cybercrime ex-

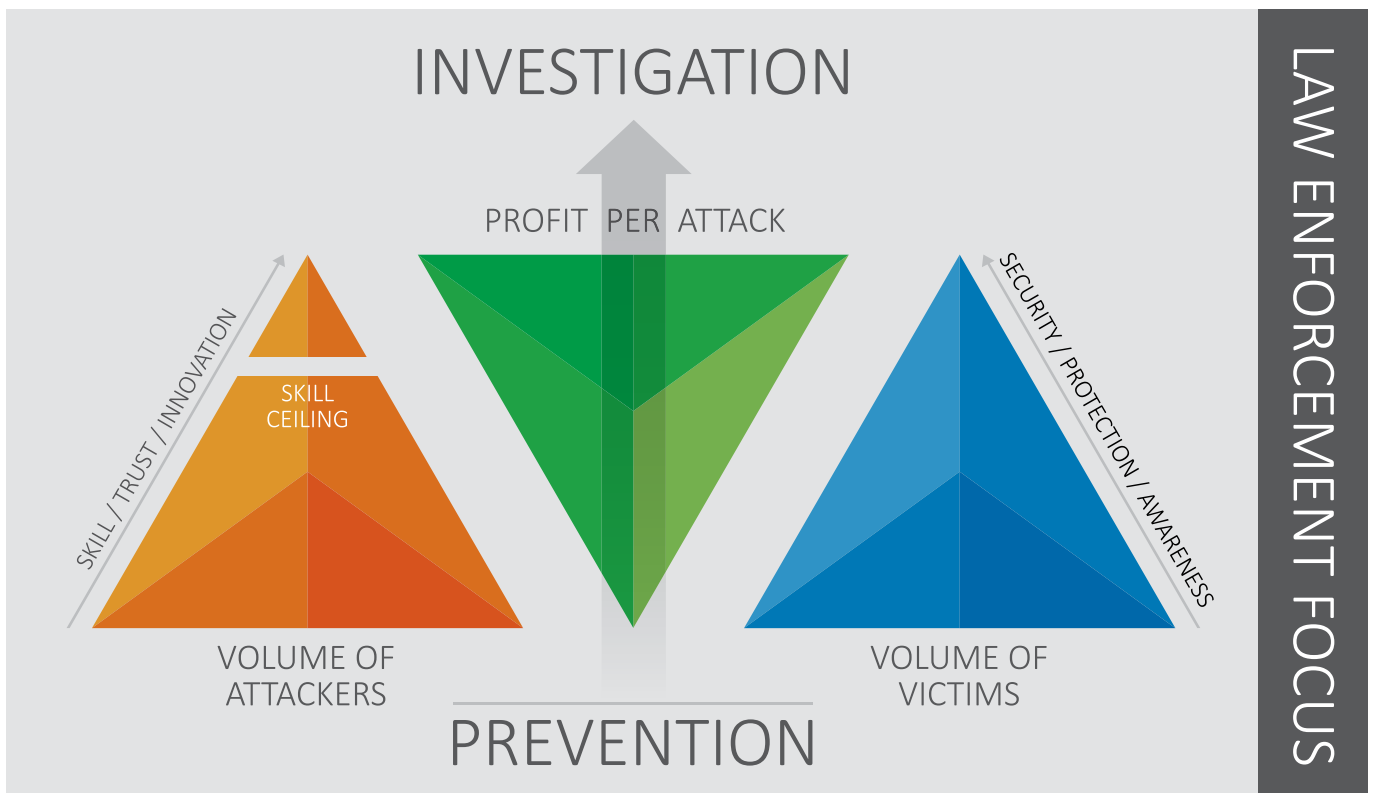
ploits well-known, and in some cases decade-old, techniques and vulnerabilities. Some historic attack vectors, such as malicious Microsoft Office macros<sup>6</sup>, have come full circle and are once more increasingly popular among cybercriminals.

It should be noted that the majority of reported attacks are neither sophisticated nor advanced. While it is true that in some areas cybercriminals demonstrate a high degree of sophistication in the tools, tactics and processes they employ, many forms of attack work because of a lack of digital hygiene, a lack of security by design and a lack of user awareness.

Nevertheless, a variety of new and innovative modi operandi have been discovered, combining existing approaches, exploiting new technology or identifying new targets. The proliferation and evolution of malware attacks directly against ATMs, indications of compromised payments involving contactless (NFC) cards and the recent attacks against the SWIFT system are examples of this development.

Using the Cybercrime Trichotomy introduced in last year's report, it is proposed to put an even stronger focus on awareness and prevention when it comes to high volume crimes that can be effectively stopped by increasing the general level of cybersecurity. This should be done in close cooperation at EU level and via public-private partnerships (PPPs). Moreover, law enforcement, together with all relevant partners needs to

## THE CYBERCRIME TRICHOTOMY



<sup>4</sup> Booters/stressers are tools for stress testing servers which can be misused to conduct DDoS attacks.

<sup>5</sup> Forbes, Data Breaches In Healthcare Totalled Over 112 Million Records In 2015, <http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015>, 2015

<sup>6</sup> WindowsSecurity.com, The Return of Macro Attacks, [http://www.windowsecurity.com/articles-tutorials/viruses\\_trojans\\_malware/return-macro-attacks.html](http://www.windowsecurity.com/articles-tutorials/viruses_trojans_malware/return-macro-attacks.html), 2016



step up efforts to demonstrate that criminal behaviour online is met with real consequences. This should involve a stronger focus on and prioritisation of investigation and improved attribution in relation to key criminal actors, tools and services as well as identifying preventive actions and working proactively with young individuals who may be at risk of conducting criminal activity online<sup>7</sup>.

The networking model employed by Europol's EC3 continues to provide tangible results in the fight against cybercrime at EU level and beyond. In the last year the number of successful high-level operations supported by the EC3 (which rose from 72 operations during 2014, to 131 in 2015), with EU and non-EU law enforcement and judicial partners, as well as partners in industry, the financial sector, the CERT community and academia demonstrate the power of the network.

However, law enforcement, policy makers, legislators, academia and training providers need to become even more adaptive and agile in addressing the phenomenon. Existing frameworks, programmes and tools are often too slow and bureaucratic to allow for a timely and effective response. Rather than multiple partners investing in and developing the same highly specialised skill-sets and expertise, perhaps a more effective, high-level model would be for law enforcement and relevant partners to focus on distinct core competencies and to make them available to others 'as a service'.

In addition to leveraging existing networks further, the EC3, and law enforcement in general, need the resources required to not only maintain but further increase response capacities to keep up with the expanding cybercrime threat within the EU and beyond. This should include the necessary resources to recruit and retain law enforcement personnel with the specialised skills, knowledge and expertise required to examine, analyse and investigate cybercrime as well as to develop or acquire special purpose tools for digital forensics, Big Data analytics and Blockchain investigations.

In order to minimise unnecessary overlap and duplication of efforts by connecting existing initiatives and partnerships, the development of a 'cyber-security ecosystem' is needed at EU level and beyond to identify all the relevant partners and stakeholders, map out networks, identify interfaces and links to legal and regulatory frameworks, facilitate easier capacity building and visualise opportunities for the further strengthening of cyber security in the EU. This should include organisations such as EC3, INTERPOL, Eurojust, ENISA, CERT-EU, CEPOL, the International Cyber Crime Coordination Cell (IC4), the National Cyber-Forensics and Training Alliance (NCFTA) and the Cyber Defence Alliance (CDA), to mention some.

It is important to consider law enforcement as one of the key partners in ensuring cybersecurity in the EU. An important aspect in this regard is the systematic and official involvement of law enforcement in cooperation with EU agencies such as ENISA and CERT-EU as well as national/governmental Computer Emergency Response Teams (CERTs) on law enforcement relevant aspects of cyber security. Law enforcement can provide investigative support and valuable information on the methodologies and groups behind cyber-attacks.


In the context of the Network and Information Systems (NIS) Directive, law enforcement should be fully engaged, given that the investigation and prosecution of cybercrime is essential for the kind of cross-domain and sector cooperation that is required to effectively and efficiently address cyber threats.

<sup>7</sup> UCD Geary Institute for Public Policy, Young People and Pathways into CyberCrime, <http://www.ucd.ie/geary/research/humandevlopment/pathwaysintocybercrime/>, 2016

# KEY FINDINGS

- Cryptoware (encrypting ransomware) has become the most prominent malware threat, overshadowing data stealing malware and banking Trojans. With cryptoware becoming a key threat for citizens and enterprises alike, law enforcement and the internet security industry have responded rapidly and in concert, with prevention and awareness campaigns and technical support, and operations targeting the criminal groups and infrastructure involved.
- As mobile devices increasingly operate less as simple phones and more as mobile computers, the nature and complexity of malware attacking mobile devices and the methods of infecting those devices are beginning to more closely mirror those of 'conventional' desktop malware.
- There is a notable difference in the malware threat landscape as perceived by both law enforcement and the financial sector on one side, and the internet security industry on the other, with each encountering different ends of the attack chain. Law enforcement largely encounters the 'payload' malware, which results in actual damage or financial loss, whereas the internet security industry has greater awareness of 'upstream' malware threats, such as droppers and exploit kits that enable such attacks to occur.
- Following grooming or social engineering, victims of child sexual exploitation are increasingly subjected to coercion and extortion. Offenders apply this influence to obtain further child abuse material, financial gain or physical access to the victim.
- While peer-to-peer (P2P) networks continue to represent a popular platform for the exchange of child sexual exploitation material (CSEM), a growing number of Darknet forums facilitating the exchange of CSEM, coupled with the ease of access to these networks, is leading to an increase in the volume of material being exchanged on the Darknet.
- The use of end-to-end encrypted platforms for sharing media, coupled with the use of largely anonymous payment systems, is facilitating an escalation in the live streaming of child abuse. Offenders target regions where there are high levels of poverty, limited domestic child protection measures and easy access to children.
- EMV(chip and PIN), geoblocking and other industry measures continue to erode card-present fraud within the EU, forcing criminals to migrate cash out operations to other regions, mainly the Americas and South East Asia. Meanwhile, logical and malware attacks directly against ATMs continue to evolve and proliferate.
- The proportion of card fraud attributed to card-not-present (CNP) transactions continues to grow. Levels of fraud have increased across almost all sectors, with the purchases of physical goods, airline tickets, car rentals and accommodation causing the heaviest losses.
- There are indications that organised crime groups (OCGs) are starting to manipulate or compromise payments involving contactless (NFC) cards. This demonstrates how quickly criminals can adapt to and abuse emerging technologies.
- An increase of targeted phishing aimed at high value targets was reported by law enforcement and the private sector alike. A rising quality and apparent authenticity of phishing campaigns was also observed, making these increasingly difficult to tell apart from the genuine communication.
- A refined variant of spear phishing, CEO fraud, has evolved into a key threat as a growing number of businesses are





targeted by organised groups of professional fraudsters. Successful CEO frauds often result in significant losses for the targeted companies.

- DDoS attacks continue to grow in intensity and complexity, with many attacks blending network and application layer attacks. Booters/stressers are readily available “as-a-service”, accounting for an increasing number of DDoS attacks.
- Companies that store financial credentials remain a key target for financially motivated cybercriminals carrying out network attacks and data breaches. As such, the accommodation and retail sectors are common targets. There is, however, a growing trend in the compromise of further data types for other purposes, such as medical records. This additionally highlights a need for such businesses to store data in an encrypted format.
- Data remains a key commodity for cybercriminals, however data is no longer just procured for immediate financial gain. Increasingly it is acquired for the furtherance of more complex fraud, encrypted for ransom, or used directly for extortion. When considering intellectual property, the illegal acquisition of this data can reflect the loss of years of research and substantial investment by the victim.
- For criminal to criminal (C2C) payments, payment systems which ensure that both parties can maintain a high level of anonymity are preferred, with Bitcoin being the payment system of choice for many C2C transactions. Bitcoin has also become the standard solution for extortion payments, whether as a consequence of ransomware or DDoS attacks.
- Cybercriminals use whatever communication method they deem to be the most convenient and/or that which they

perceive to be sufficiently secure. The communication channels used by any particular cybercriminal may be indicative of their level of sophistication, and range from simple email to end-to-end encrypted channels such as Jabber. Forums within either the deep web or Darknet remain an important communication platform for criminals.

- The use of encryption by criminals to protect their communications or stored data represents a considerable challenge for law enforcement, denying access to essential intelligence and evidence. This is a cross-cutting issue that affects all crime areas. The growing regularity of native encryption on mobile devices compounds this problem.
- While law enforcement strives to disrupt criminal forums and marketplaces on the Darknet, the natural volatility of these hidden services acts as an internal control. In 2015/2016 a number of high profile markets either closed down or were abandoned as their administrators exited with their customers’ money. Such activity has the additional disruptive effect of spreading distrust and uncertainty throughout the community.
- The extent to which extremist groups currently use cyber techniques to conduct attacks appears to be limited. While such factions make extensive use of the internet, particularly social media, for the purposes of recruitment, propaganda and incitement, there is currently little evidence to suggest that their cyber-attack capability extends beyond common website defacement. The availability of cyber-crime tools and services, and illicit commodities (including firearms) on the Darknet provide ample opportunities for this situation to change.

# KEY RECOMMENDATIONS



## INVESTIGATION

- Law enforcement needs to have the tools, techniques and expertise to counter the criminal abuse of encryption and anonymity.
- Law enforcement should continue to focus on attribution and intelligence development in order to identify, locate and prosecute key criminal individuals to achieve more permanent impact on the criminal community.
- It is essential for law enforcement to continue to allocate sufficient resources to investigate the malware and services that enable other cyber-attacks.
- Law enforcement needs to have the tools, techniques and expertise to counter the criminal abuse of encryption and anonymity.
- Booter/stresser tools are responsible for a growing proportion of DDoS attacks. A concerted and coordinated effort is required by law enforcement to tackle this threat.
- Following the success of the European Money Mule Action (EMMA) initiatives in 2015 and 2016, more European countries should endeavour to contribute and engage in the related operational and prevention activity. This will result in a greater and more widespread impact on this key area of criminality.
- Given the additional challenges investigations on the Darknet present to law enforcement, effective deconfliction, collaboration and the sharing of intelligence is essential. This will help to prevent duplication of effort, facilitate the sharing of tactics and tools, and increase understanding of the threat.
- Law enforcement should make greater use of the Europol Malware Analysis System (EMAS) by submitting ATM and PoS malware samples, in order to identify links to other cases and improve a community-wide understanding of the threat.
- There should be a continuous effort from all parties to prioritise the victims in the investigation of CSE. That includes law enforcement investing human and IT resources to improve the opportunities for victims to be identified. Such strategies are regularly demonstrated to be valuable in locating children harmed by abuse and preventing further abuse.
- Taking a phenomenon-centred approach rather than an incident-centred one, successful initiatives targeting fraud in the airline industry should be replicated to cover additional sectors. Operations to target offenders arriving at a physical location to benefit from fraudulent transactions, such as car rentals or other pre-ordered services, may be particularly effective.

## CAPACITY BUILDING & TRAINING

- To cope with the criminal use of encryption, law enforcement must ensure it has the training and resources it requires

to obtain and handle digital evidence in situ using techniques such as live data forensics, while mindful of the need to avoid weakening cybersecurity in general<sup>8</sup>.

- Law enforcement must continue to develop and invest in the appropriate specialised training required to effectively investigate highly technical cyber-attacks. A foundation level understanding of cyber-facilitated and cyber-enabled crime, including the basics of digital forensics (e.g. how to secure/seize digital evidence) should be required by all law enforcement officers, especially first responders.
- Given the rapidly changing nature of cybercrime and the pace at which technology evolves, there is a need for a more adaptive and agile approach to research and development, including funding opportunities, with a view to delivering relevant results in a more timely manner.
- As the criminal use of virtual currencies continues to gain momentum, it is increasingly important for law enforcement to ensure that cybercrime and financial investigators have adequate training in the tracing, seizure and investigation of virtual currencies.
- A coordinated effort should be made by law enforcement to engage with countries where compromised cards are cashed out and where goods purchased with compromised cards are reshipped.
- Darknets are an environment where cyber-facilitated crime is becoming firmly established. This is a cross-cutting issue that requires support from specialists in multiple crime types. It is not feasible or practical that all such crime is dealt with by cybercrime units when the predicate crime is related to drugs, firearms or some other illicit commodity. It is essential therefore that appropriate training and tool support is extended to those working in these areas to provide them with the required knowledge and expertise.

## PREVENTION

- When it comes to addressing volume crimes, investing resources in prevention activities may be more effective than investigation of individual incidents. In addition to raising awareness and providing crime prevention advice the campaigns should advise the public on how to report the crimes.
- Prevention campaigns should not focus solely on preventing citizens and businesses from becoming victims of cybercrime, but also on preventing potential cybercriminals becoming involved in such activity. Such campaigns must highlight the consequences of cybercrime for both the victim and perpetrator.

- Prevention campaigns should be coordinated with other national and international organisations.
- Law enforcement should to maintain the current momentum on prevention and awareness campaigns relating to mobile malware.
  - Encouraging the use of security software and the reporting of attacks gives law enforcement and the security industry an overall clearer picture and a greater capacity to mitigate the threat.
- Alongside NGOs and private industry, law enforcement must maintain its focus on the development and distribution of prevention and awareness raising campaigns. Such campaigns must be updated to encompass current trends such as sexual extortion and coercion and self-generated indecent material.
  - Raising awareness and providing children, parents, guardians and carers with the appropriate knowledge and tools are essential to reduce this threat.

## PARTNERSHIPS

- Law enforcement must continue to forge and maintain collaborative, working relationships with academia and the private sector.
  - The comparison of law enforcement, industry and internet security perspectives on malware threats highlights how small a piece of the overall picture law enforcement actually sees. Law enforcement must continue to investigate reported attacks, but must also be informed by the views of other sectors.
- Additional effort is required, through more focused information sharing within law enforcement and/or partnership with private industry, to link cases of card fraud. This would facilitate the identification of organised crime groups involved in card fraud.
- Law enforcement must continue to cooperate with private industry and other law enforcement partners to conduct large-scale operations, both to disrupt cybercrime and to reassure the public and business that law enforcement are actively seeking to protect them.
  - This should also include clear rules of engagement, so that digital evidence acquired through private entity action is admissible in judicial proceedings.
- In cases where authorities have to report incidents to the national Cyber Security Incident Response Team (CSIRT), agreements should be undertaken to make sure that law enforcement is able to follow up with criminal investigations when needed<sup>9</sup>.

<sup>8</sup> Europol and ENISA Joint Statement, On Lawful Criminal Investigation that Respects 21st Century Data Protection, <https://www.europol.europa.eu/content/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint->, 2016

<sup>9</sup> EU Member State, Law enforcement recommendation, 2016

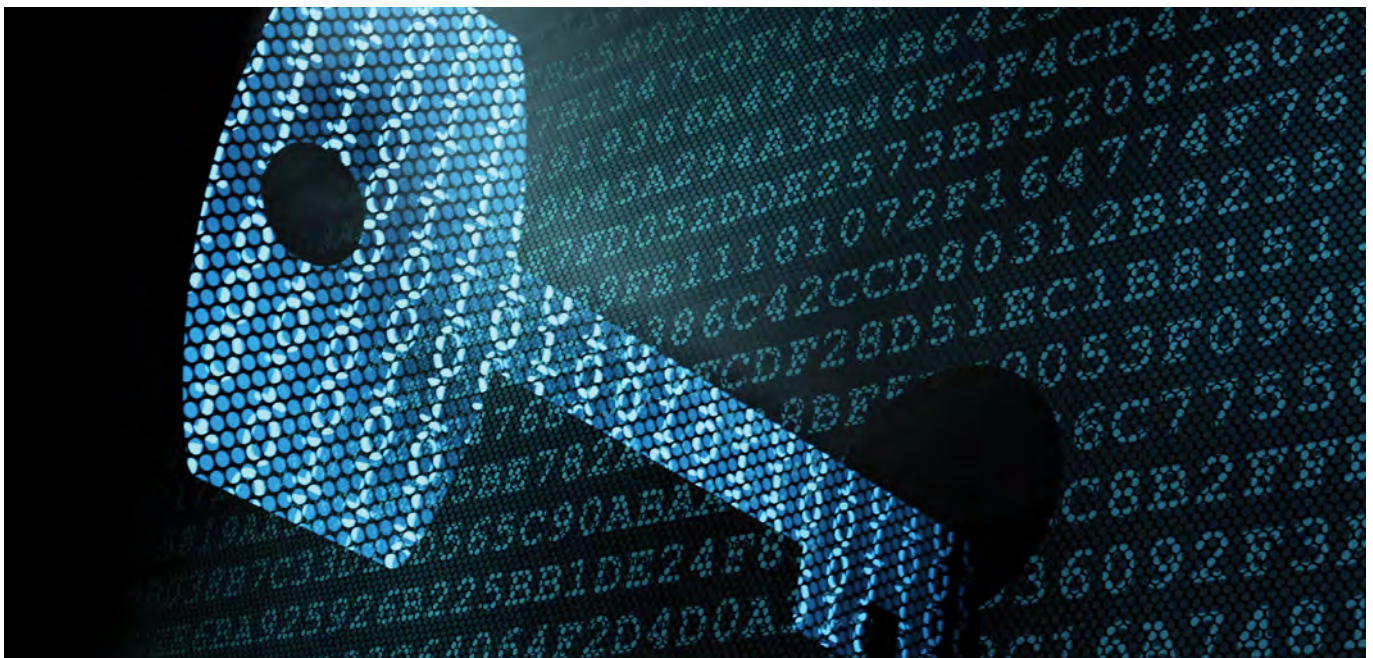


- Law enforcement should make themselves aware of any packet station services<sup>10</sup> operating in their jurisdictions in order to build working relationships with them to mitigate the abuse of these services.
- As the criminal use of virtual currencies continues to gain momentum, it is increasingly important for law enforcement to build and maintain relationships with the virtual currency community, in particular virtual currency exchangers.

## LEGISLATION

- The difficulties faced by law enforcement operating lawfully in the Darknet are clear, with many jurisdictions restricted by their national legislation. A harmonised approach to undercover investigations is required across the EU.
- While securing critical infrastructures remains a private sector responsibility, attention should be given by regulators to the compliance of IT systems and mandatory security-by-design.
  - There needs to be a baseline of security standards for those operating systems that manage critical industrial systems, transportation, power grids or air traffic<sup>11</sup>.
  - There is a need for provisions aimed at protecting critical infrastructures<sup>12</sup> and securing network and information systems<sup>13</sup> in order to align cyber security capabilities in all the EU Member States and ensure efficient exchanges of information and cooperation.

- In order to improve criminal justice in cyberspace, existing domestic procedures for the acquisition of electronic evidence should be harmonised. This would include a common approach to the cooperation with ISPs, streamlining existing MLA procedures<sup>14</sup> and a possible rethinking of how to establish jurisdiction in cyberspace.
- In order to avoid safe havens where criminals can avoid investigation and prosecution, harmonisation of the criminalisation of certain conduct is required<sup>15</sup>.
- The Budapest Convention should be implemented in full by all signatories, including EU Member States. Assessments performed by the Cybercrime Convention Committee (T-CY)<sup>16</sup> have shown that not all Parties to the Convention make full use of the opportunities offered. They also show that implementation of it in the national legal frameworks of some of its members is incomplete or not in line with the Convention.
- Steps should be taken to facilitate intensified cooperation across government (predominantly law enforcement, intelligence services and armed forces), to allow information sharing and a coordinated approach to response to serious cyber attacks.



<sup>10</sup> Unmanned stations where packages can be delivered and stored securely.

<sup>11</sup> Hewlett Packard Enterprise, IT Spend Slowdown Puts the Squeeze on Innovation, <http://hpe-enterpriseforward.com/spend-slowdown-puts-squeeze-innovation/>, 2016

<sup>12</sup> European Commission, Communication from the Commission on a European Programme for Critical Infrastructure Protection, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN>, 2016

<sup>13</sup> European Commission, <https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive>, 2016

<sup>14</sup> Modernizing International Procedures against Cyber-enabled Crimes, <https://www.eastwest.ngo/info/modernizing-international-procedures-against-cyber-enabled-crimes>, 2016

<sup>15</sup> The rapid evolution of cyber threats has led to a situation in which certain conduct is criminalised in some countries, but not in others. An example is the live streaming of child sexual abuse. Even within the EU, there are countries where the act of streaming is not separately criminalised, while at the same time it cannot be captured under 'possession'. Similarly, wilful facilitation of the hosting of illicit content is not criminalized in a number of countries, effectively creating a safe haven for bulletproof hosters.

<sup>16</sup> Assessing the Implementation of the Budapest Convention, <http://www.coe.int/en/web/cybercrime/assessments>, 2016

# SUGGESTED OPERATIONAL PRIORITIES

A key role for the IOCTA is to inform the priority setting for the operational action plans in the framework of the European Multidisciplinary Platform Against Criminal Threats (EM-PACT)<sup>17</sup>. In this regard, and considering the information presented in this report, the following priorities are proposed for the forthcoming operational actions for EU law enforcement for 2017.

## CYBER ATTACKS

As an overarching, horizontal goal, law enforcement should prioritise actions against the providers of the key criminal services and tools that support other areas of cybercrime. Removal of these highly specialised services and will have significant impact on the cybercrime community.

- Developers, vendors and buyers of payload malware such as ransomware, RATs and banking Trojans;
- Developers, vendors and buyers of enabling/facilitating malware such as exploit kits, droppers and spam;
- Providers of DDoS attack services (Booters/Stressers);
- Counter anti-virus services;
- Botnet takedowns, with particular focus on those deployed to distribute other malware and carry out DDoS attacks.

## PAYMENT FRAUD

- Execution, enabling and facilitation of card-present fraud:
  - Developers and vendors of ATM/POS malware and skimming devices;
  - Logical and malware attacks designed to obtain cash or sensitive data from ATMs and/or POS (Black Boxing, Jackpotting, Man-in-the-Middle or Skimming 2.0);
  - The compromise of EU citizen card data;
  - Illegal transactions in non-EMV compliant regions (fraud migration outside the EU).
- Online fraud/card-not-present fraud:
  - E-commerce fraud with a focus on the transport (airlines), retail and accommodation sectors.
- The acquisition and trading of compromised financial data and credentials:
  - Data breaches;
  - Take-down of carding sites and prosecution of their operators and users.

## ONLINE CHILD SEXUAL EXPLOITATION

- Combating the live streaming of on-demand abuse;
- Eradication of groups that stimulate active CSEM production, in particular on the Darknet;
- Victim identification and rescue;
- Tackling the misuse of legitimate online platforms for CSE related crimes (such as the dissemination of CSEM, grooming and child sexual extortion).

## CROSS-CUTTING CRIME ENABLERS

- Vendors, buyers and administrators of illegal trading sites on the Darknet;
- Criminal providers of anonymising and hosting solutions:
  - Bulletproof hosting;
  - Criminal VPN/proxy providers.
- Money mules and money laundering services;
- Criminals facilitating the abuse of Bitcoin and other virtual currencies;
  - Criminal exchangers;
  - Criminal mixing services.

Many criminal tools and services cut across several crime areas to some degree; their disruption would therefore have an impact on a broader range of cyber-enabled crime than simply the crime area it is primarily associated with. Tackling these areas would however require greater levels collaboration between investigators from cyber attacks, payment fraud and online child sexual extortion to efficiently prioritise and coordinate investigations and prevent the need for deconfliction.

The operational objectives suggested above must be considered in parallel with adequate provision for intelligence sharing and analysis. Furthermore, they should be matched by more strategic priorities around training and capacity building and complemented by prevention and awareness initiatives.

<sup>17</sup> EU Policy Cycle – EMPACT, <https://www.europol.europa.eu/content/eu-policy-cycle-empact>, 2016



# ■ INTRODUCTION

## AIM

The Internet Organised Crime Threat Assessment (IOCTA) is produced by the European Cybercrime Centre (EC3) at Europol. It aims to inform decision-makers at strategic, policy and tactical levels in the fight against cybercrime, with a view to directing the operational focus for EU law enforcement. The 2016 IOCTA will steer the setting of priorities for the 2017 EMPACT operational action plan in the three sub-areas of the cybercrime priority: cyber attacks, payment fraud and child sexual exploitation.

## SCOPE

The 2016 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 which influence or impact upon the cybercrime ecosystem, such as social engineering and money laundering.

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

In addition to the topics covered in previous years, the 2016 IOCTA examines the use of cyber techniques by terrorist groups and the latest developments in internet governance.

## METHODOLOGY

The 2016 IOCTA was drafted by a team of strategic analysts within EC3 drawing predominantly on contributions from Member States, the European Union Cybercrime Taskforce (EUCTF), Europol's Focal Points Cyborg, Terminal and Twins, as well as the Cyber Intelligence team and SOCTA team, via structured surveys, interviews and moderated workshops. This has been enhanced with open source research and input from the private sector, including EC3's advisory groups, Eurojust<sup>18</sup>, ENISA, CERT-EU, the EBF and the CSIRT community. These contributions have been essential to the production of the report.

## ACKNOWLEDGEMENTS

Europol would like to extend special thanks to Prof. Marco Gercke, Prof. Michael Levi and Prof. Alan Woodward of the IOCTA Advisory Board for their contributions. Special thanks are also due to Bruce Nikkel from UBS AG for his contribution on the positive changes in the fight against cybercrime from a finance industry perspective.

<sup>18</sup> The Netherlands EU Presidency 2016, General EJ EC3 Joint Paper Version 1.0 Final, <https://english.eu2016.nl/documents/publications/2016/03/7/general-ej-ec3-joint-paper-version-1.0-final>, 2016



# MALWARE



Malicious attacks on public and private networks are relentless. In order to carry out such attacks, cybercriminals need access to the right tools and services. The development and propagation of malware therefore continues to be the cornerstone for the majority of cybercrime. Although different malware have a range of overlapping capabilities, the two dominant threats encountered by EU law enforcement are ransomware and information stealers.

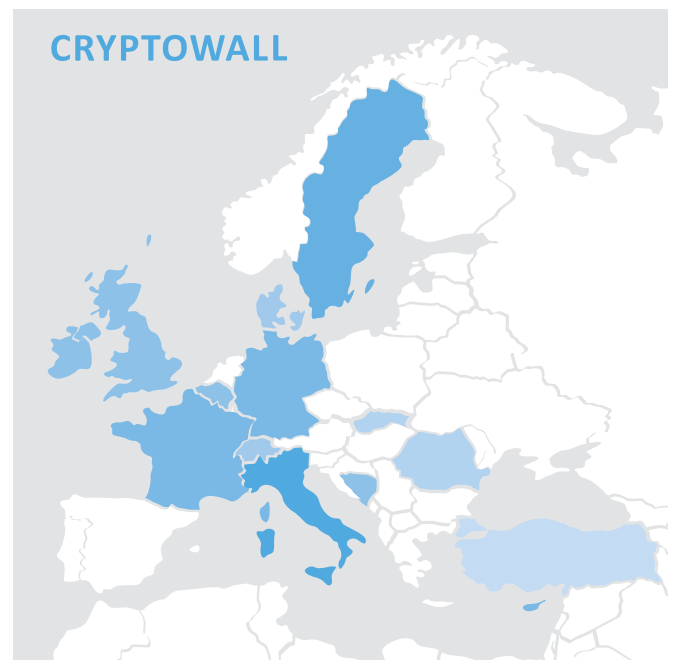
## KEY THREAT - RANSOMWARE

Ransomware continues to be the dominant concern for EU law enforcement. While police ransomware appears to have dropped off the radar almost completely, the number of cryptoware variants has multiplied. Whereas each variant has its own unique properties, many are adopting similar anonymisation strategies such as using Tor or I2P for communication, and business models offering free test file decryptions to demonstrate their intentions. Ransom payment is almost exclusively in Bitcoins. While most traditional and “commercially available” data stealing malware typically targets desktop Windows users, there are many more applicable targets for ransomware, from individual users’ devices, to networks within industry, healthcare or even government.

No More Ransom ([www.nomoreransom.org](http://www.nomoreransom.org)) is a new initiative in cooperation between law enforcement and the private sector to fight ransomware together<sup>19</sup>. This new online portal launched in 2016 aims to inform the public about the dangers of ransomware and helps victims to recover their data without having to pay ransoms to cybercriminals.

## CRYPTOWALL

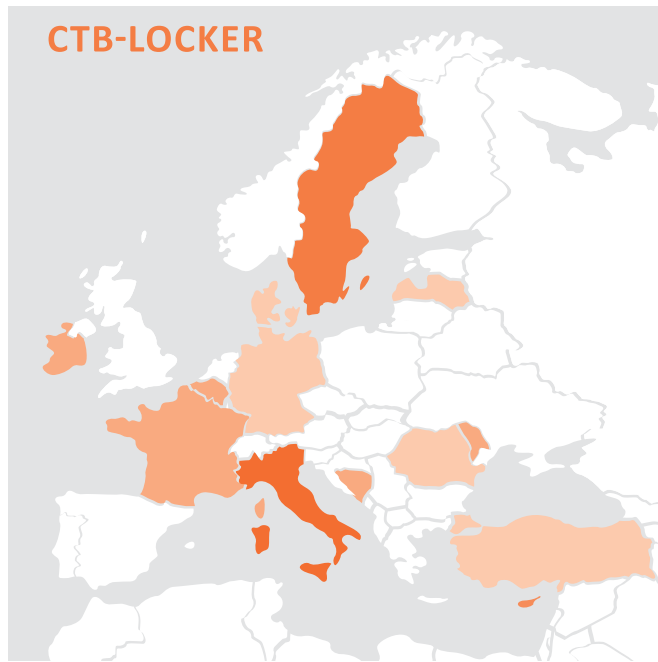
First appearing in 2013, Cryptowall has appeared under a number of pseudonyms, including Cryptodefense and Cryptorbot, and at the time of writing is running under version 4.0. Cryptowall is typically installed by an exploit kit or malicious email attachment. The malware makes use of both Tor (for handling Bitcoin payments from victims) and I2P (for communicating with its C&C servers) P2P networks. Half of EU Member States report cases of Cryptowall.



<sup>19</sup> Europol, Press Release on No More Ransom Initiative, <https://www.europol.europa.eu/content/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-fight-ransomware>, 2016

## ■ CTB-LOCKER

Emerging in mid-2014, Curve-Tor-Bitcoin (CTB) Locker (also known as Critroni) was one of the first ransomwares to use Tor to hide its C2 infrastructure. While active during 2015, CTB-Locker activity has dropped off in 2016. However, a more recent variant has been targeting web-servers and is uniquely using the Bitcoin blockchain to deliver decryption keys to victims<sup>20</sup>. Marginally less prominent among EU law enforcement investigations compared to Cryptowall, CTB-Locker represented the top malware threat for the financial industry.



indicate that Germany, France, Italy and Spain are all top 10 targets for the new campaign<sup>22</sup>. Locky encrypts over 160 different file types, including virtual disks, databases and Bitcoin wallet (wallet.dat) files<sup>23, 24</sup>.

Due to similarities in the campaigns for both malware distribution methods (malicious macro spiked email attachments distributed via mass spam campaigns) and several aspects of the coding, it is speculated that the Locky malware is produced by the same developers as the Dridex malware<sup>25</sup>.

### *The legacy of Cryptolocker*

*Throughout 2014, the Cryptolocker ransomware was one of the top ransomware threats within the EU in terms of scope and impact. In May 2014, Operation Tovar significantly disrupted the infrastructure distributing Cryptolocker and by the end of 2014 Cryptolocker was effectively finished. The name 'Cryptolocker' now appears to have become a synonym for any unidentified ransomware. Consequently, reports of 'Cryptolocker' infections are still high within Europe.*

## ■ TESLACRYPT

Teslacrypt was another cryptoware variant reported by EU law enforcement as a significant threat in 2015. However, in May 2016, the developers apparently discontinued the malware, apologised for their actions and released a master decryption key<sup>21</sup>. There is no indication as to why they did this. Residual investigations remain in a number of Member States.

## ■ LOCKY

While the Locky cryptoware did not appear until mid-February 2016, and consequently does not feature heavily in the reporting period, it is expected to become one of the dominant cryptoware threats throughout 2016. Some reports

<sup>20</sup> Sucuri Blog, Website Ransomware – CTB-Locker Goes Blockchain, <https://blog.sucuri.net/2016/04/website-ransomware-ctb-locker-goes-blockchain.html>, 2016

<sup>21</sup> BleepingComputer, TeslaCrypt Shuts Down and Releases Master Decryption Key, <http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/>, 2016

<sup>22</sup> SecurityWeek, Germany, France Hit Most by Locky Ransomware: Kaspersky, <http://www.securityweek.com/germany-france-hit-most-locky-ransomware-kaspersky>, 2016

<sup>23</sup> Naked Security, "Locky" Ransomware – What You Need to Know, <https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/>, 2016

<sup>24</sup> Avast Blog, A Closer Look at the Locky Ransomware, <https://blog.avast.com/a-closer-look-at-the-locky-ransomware>, 2016

<sup>25</sup> Symantec Official Blog, Locky Ransomware on Aggressive Hunt for Victims, <http://www.symantec.com/connect/blogs/locky-ransomware-aggressive-hunt-victims>, 2016

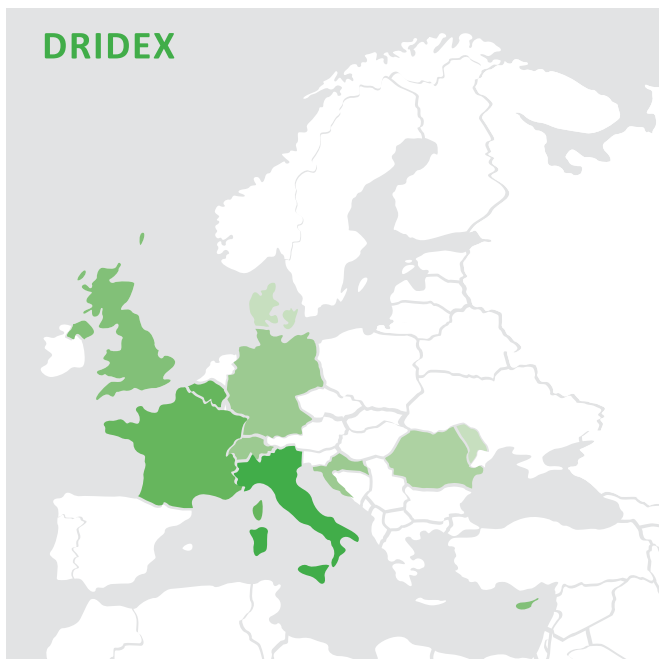
# KEY THREAT – INFORMATION STEALERS

While ransomware provides easy money for cybercriminals, the data which information stealing malware can harvest can be of significantly greater value, even though it requires additional effort to monetise. While information stealers can target any data of potential value from social media logins to digital currency wallets, the majority focus on harvesting banking and credit card credentials.

The malware landscape - with regards to information stealers - remains largely unchanged from the previous year. While information stealing malware is no less prevalent or relentless than in previous years, the perceived lower threat level by law enforcement perhaps reflects that, along with support from private industry, law enforcement is now better equipped and better prepared to both investigate and mitigate this threat.

## ■ DRIDEX

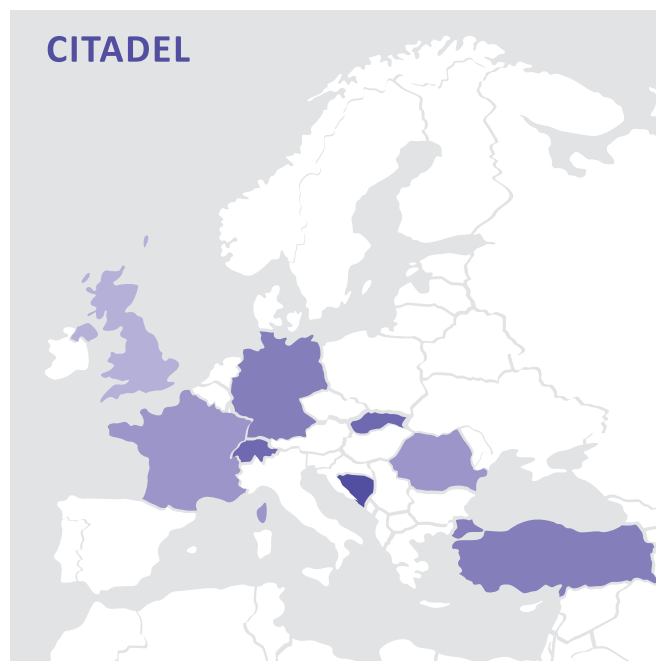
While only just emerging as a threat for law enforcement in 2015, Dridex has, as predicted, become one of the main financial threats for EU law enforcement over the last year. Dridex is distributed almost exclusively via spam campaigns, disguised as financial emails such as invoices, receipts, and orders. Dridex targets nearly 300 different organizations in over 40 regions, focussing on financial institutions in the US and Western Europe, as well as a range of Asia-Pacific states<sup>26</sup>. Dridex uses a distributed P2P command and control infrastructure that makes it more resistant to takedown. Dridex was the top threat in this category for both law enforcement and the financial sector.



*In August 2015, the UK's NCA and the US FBI, with the support of EC3 and the J-CAT and a number of international law enforcement agencies and key private partners, conducted an operation to 'sinkhole' the Dridex malware, stopping infected computers from communicating with the cybercriminals controlling them. Additionally a key player in the development of Dridex was arrested. The operation was a success, but by November 2015 there was a resurgence in activity as new variants began to propagate.*

## ■ CITADEL

A Zeus variant that first appeared in 2012, the sale and use of Citadel is limited to select groups of cybercriminals and run as-a-service. Several Member States continue to report low numbers of Citadel cases. In April 2016, a new variant of Citadel, dubbed Atmos, began targeting financial institutions in France. The Trojan is noted as having C&C servers based in Vietnam, Canada, Ukraine, Russia, the US and Turkey<sup>27</sup>. It is unknown how many of the law enforcement reports reflect the appearance of this new variant.



## ■ ZEUS

First appearing in 2006, the source code for Zeus was leaked in 2011. Subsequently, the code has been re-used by coders to create both new variants of Zeus itself and whole new malware families, such as Ice IX and Citadel. While Zeus still affects some Member States, it is likely that the statistics represent an amalgamation of all the current variants rather than any single coordinated campaign.

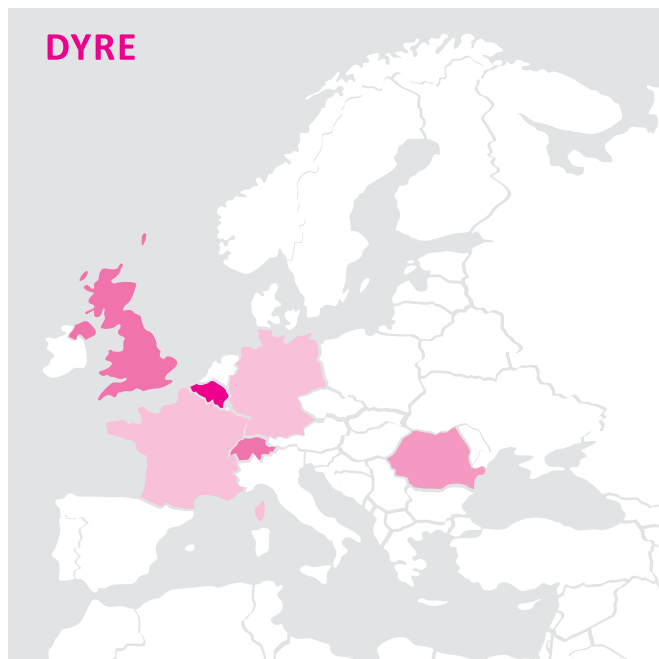
<sup>26</sup> Symantec, Dridex: Tidal Waves of SPAM Pushing Dangerous Financial Trojan, [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/dridex-financial-trojan.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf), 2016

<sup>27</sup> SC Magazine, Atmos, Citadel Malware Variant, Hitting French Banks, <http://www.scmagazine.com/atmos-citadel-malware-variant-hitting-french-banks/article/489104/>, 2016



## ■ DYRE

In the 2015 IOCTA it was predicted that Dyre (also known as Dyreza) would be one of the top malware threats throughout 2015. Run privately by its developers, Dyre targeted over 1000 banks and other payment and financial services. However, while it did indeed enjoy significant successes, in November 2015 Russian authorities arrested a number of suspects believed to be part of the Dyre crew<sup>28</sup>. Following these arrests, Dyre activity dropped to negligible levels. A number of Member States report low numbers of Dyre investigations but these are predominantly follow-up investigations and not based on new infections.



## KEY THREAT – MOBILE MALWARE

Identified by law enforcement as little more than a likely future threat in previous years' reports, mobile malware now features firmly in law enforcement investigations in 14 European countries, particularly non-EU states. While the number of cases per state typically is still low (under 10), this is a clear indication that mobile malware is finally breaking into the public domain with regards to both the reporting and subsequent criminal investigation of mobile malware attacks. Moreover, industry continues to report the proliferation of mobile malware, much of which is now as complex as PC malware. This growth in complexity also reflects the change in the purpose of mobile malware. Historically mobile malware has been dominated by premium service abusers, i.e. exploiting the device in its capacity as a phone with access to (limited) credit. As mobiles are increasingly of the 'smart' variety, the current generation of mobile malware instead targets devices in their capacity as mobile computers. Consequently the infection pathways and intent of mobile malware are beginning to mirror that of the desktop PC – drive-by downloads<sup>31</sup>, RATs, ransomware, click fraud<sup>32, 33</sup> and banking Trojans are all common features for mobile malware today.

Whereas police ransomware appears to have almost disappeared from desktop PCs, mobile platforms (both Android and iOS) appear to be one of the few environments where it is still active<sup>34</sup>. In some cases, however, the requested payment method (e.g. iTunes vouchers<sup>35</sup>) ridicules any pretence that it represents a legitimate law enforcement agency. Mobiles otherwise represent key targets for ransomware and, coupled with the lower likelihood of mobile device users running security software, mobiles are increasingly at risk.

## ■ OTHER INFORMATION STEALERS

A variety of other information stealing malware featured in EU investigations throughout 2015, however the numbers of these were sufficiently low to suggest they did not represent a significant threat to the EU. Of these, Spyeeye and Carberp (particularly in South East Europe) were the most prominent, but only rare cases involving malware such as Vawtrack (Neverquest), Ice IX, Nymain or Dorkbot were reported. While Tinba was only reported as a low lying threat by law enforcement, some internet security partners<sup>29</sup> and media reporting indicated that it is a more significant threat<sup>30</sup>.

<sup>28</sup> The Hacker News, Hackers Behind Dyre Malware Busted in Police Raid, <http://thehackernews.com/2016/02/hacking-dyre-malware.html>, 2016

<sup>29</sup> Check Point Software Technologies, <http://www.checkpoint.com>, 2016

<sup>30</sup> SecurityWeek, Fifth Tinba Variant Targets Financial Entities in Asia Pacific, <http://www.securityweek.com/fifth-tinba-variant-targets-financial-entities-asia-pacific>, 2016

<sup>31</sup> Blue Coat Labs, Android Towelroot Exploit Used to Deliver "Dogspectus" Ransomware, <https://www.bluecoat.com/security-blog/2016-04-25/android-exploit-delivers-dogspectus-ransomware>, 2016

<sup>32</sup> WeLiveSecurity, Porn Clicker Trojans Keep Flooding Google Play, <http://www.welivesecurity.com/2016/02/24/porn-clicker-trojans-keep-flooding-google-play/>, 2016

<sup>33</sup> Check Point, From HummingBad to Worse: New In-Depth Details and Analysis of the HummingBad Android Malware Campaign, <http://blog.checkpoint.com/2016/07/01/from-hummingbad-to-worse-new-in-depth-details-and-analysis-of-the-hummingbad-android-malware-campaign/>, 2016

<sup>34</sup> Trend Micro, Flocker Mobile Ransomware Crosses to Smart TV, <http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/>, 2016

<sup>35</sup> Blue Coat Labs, Android Towelroot Exploit Used to Deliver "Dogspectus" Ransomware, <https://www.bluecoat.com/security-blog/2016-04-25/android-exploit-delivers-dogspectus-ransomware>, 2016

## OTHER MALWARE THREATS – REMOTE ACCESS TOOLS (RATS)

In the 2015 IOCTA, RATs were highlighted as an additional key threat area. The volume of investigations into RATs dropped considerably throughout 2015, however. The two most prominent RATs, providing attackers with backdoors to victims' systems, are again Blackshades and DarkComet, but the number of countries reporting Blackshades investigations continues to decline and, while approximately one quarter of Member States still have investigations involving DarkComet, individual case numbers are low.

## OTHER MALWARE THREATS – ENABLERS

Whereas law enforcement investigations highlighted in previous reports were entirely dominated by 'payload' malware (e.g. ransomware, information stealers and RATs), 2015 has seen a progression in tackling malware threats that operate 'behind the scenes', i.e. those used to disseminate or install other malware.

### ■ EXPLOIT KITS

Over one fifth of European countries reported active investigations involving the Angler exploit kit. First seen in 2013, Angler – known for its rapid adoption of new vulnerabilities – became one of the most popular exploit kits in the digital underground following the demise of the Blackhole exploit kit. Cryptowall 4.0 and new ransomware CryptXXX<sup>36</sup> feature amongst the payloads installed by Angler. The Nuclear and Neutrino exploit kits have also attracted the attention of European law enforcement. The Nuclear exploit kit was also noted to be spreading Cryptowall<sup>37</sup>. At the time of writing, following law enforcement action by the Russian authorities, both the Angler and Nuclear exploit kits appear to be inactive.

*Following the arrest of 50 individuals linked to the Lurk malware in June 2016 by Russian law enforcement, the operation of several other malware campaigns was severely disrupted – including Dridex, Locky, Angler, Nuclear and Necurs<sup>38</sup>, indication that some of the suspects were involved in providing a key support service for these campaigns, likely the distribution channels. While most recovered, both Angler and Nuclear remain inactive.*

### ■ DROPPERS

Both Andromeda and Conficker feature in 2015 law enforcement investigations, albeit in only a small number of countries. Andromeda's primary function is to drop other malware onto infected machines but its modular nature means its functionality can be modified to perform a variety of other tasks. Conficker (also known as Downadup) is a worm that

primarily downloads other malware but can also provide remote access and steal data<sup>39</sup>.

It is important to recognise that the view of law enforcement in terms of identifying malware threats only represents the tail end of the entire threat landscape. It often only encompasses the attacks which are detected by victims or third parties and are subsequently reported as a crime. The following table highlights the top malware threats within the EU as seen by law enforcement. Alongside this we have displayed the same view from the financial sector, which appears to be largely aligned. We would expect this, as banks and banking customers are likely to be complainants who initiate law enforcement investigations.

Notably however, over the same time period there was almost no overlap between the threats seen by law enforcement and the financial sector and those by industry. One of the few exceptions to this is Conficker (aka Downadup), which was identified as a significant threat by the internet security industry, albeit only low level by law enforcement. Some data stealing malware such as Zeus also features in the internet security threat list.

One explanation for the discrepancy between the two viewpoints is that internet security companies will typically encounter (and prevent) the malware operating 'behind the scenes' such as droppers, and are therefore less likely to see the payload malware that would have subsequently attacked the intended target. Conversely, law enforcement is more likely to encounter payload malware that has neither been detected nor prevented by an anti-virus solution. Furthermore, it is likely that only payloads that have resulted in actual, noticeable loss or damage to a victim are reported to law enforcement. Consequently, the threat list of law enforcement is dominated by banking Trojans and ransomware, and that of the internet security industry is dominated by droppers, backdoors and other unobtrusive, stealthy malware.

<sup>36</sup> Check Point, CryptXXX Ransomware: Simple, Evasive, Effective, <http://blog.checkpoint.com/2016/05/27/cryptxxx-simple-evasive-effective/>, 2016

<sup>37</sup> SecurityWeek, CryptoWall 4.0 Spreading via Angler Exploit Kit, <http://www.securityweek.com/cryptowall-40-spreading-angler-exploit-kit>, 2016

<sup>38</sup> SecurityWeek, Did Angler Exploit Kit Die With Russian Lurk Arrests?, <http://www.securityweek.com/did-angler-exploit-kit-die-russian-lurk-arrests>, 2016

<sup>39</sup> Check Point, Top 10 Most Wanted Malware, <http://blog.checkpoint.com/2016/06/21/top-10-most-wanted-malware/>, 2016

MALWARE	ALIAS	PRIMARY FUNCTION	PRIMARY INFECTION VECTOR	LAW ENFORCEMENT RANK	FINANCIAL SECTOR RANK
CRYPTOWALL	Cryptodefense, Cryptorbit	Ransomware	Exploit kit	1	5
CTB-LOCKER	Critroni	Ransomware	Email attachment (.zip)	2	1
DRIDEX	Bugat, Feodo, Cridex	Data stealer	Email attachment (.Word macros)	3	2
TESLACRYPT	-	Ransomware	Exploit kit	4	3
ANGLER*	-	Exploit kit	-	5	4
CITADEL	-	Data stealer	Exploit kit	6	-
DARKCOMET	-	RAT	Exploit kit	7	-
ZEUS	Zbot, Gameover (GOZ)	Data stealer	Exploit kit	8	6
DYRE	Dyreza	Data stealer	Dropper	9	7
NEUTRINO	-	Exploit kit	-	10	9
VAWTRACK	Neverquest, Snifula	Data stealer	Email attachment	24	8
NUCLEAR*	-	Exploit kit	-	15	10

\* At the time of writing both the Angler and Nuclear exploit kits appear to be inactive



## FUTURE THREATS AND DEVELOPMENTS

There will always be a demand for data grabbing malware, but the market for these is notably less volatile, with a handful of often persistent “consumer favourites” dominating the markets. The cryptoware scene is currently where the most flux exists, with a myriad of new variants identified in industry and media reporting in the past year. Many of these such as Cerber, CryptXXX and Locky appear to be gaining momentum. It is therefore a safe bet that 2016 will see further diversification in the range of cryptoware available, with likely only a select few surviving into 2017. Police ransomware will likely fade into obscurity as the pretence of representing law enforcement becomes obsolete - an unnecessary complication to a simple demand for money.

Cryptoware will also continue to expand its attack surface. Now firmly established as a daily desktop malware threat, the profile of ransomware as a threat on mobile devices will grow as developers hone their skills in attacking those operating systems and platforms. Given the scale of mobile device ownership (with many more mobile devices than people<sup>40</sup>) there is no shortage of fertile ground for the proliferation of mobile ransomware. Moreover, we will also see ransomware evolving to routinely spread to other smart devices. There are already indications that some ransomware is capable of infecting devices such as smart TVs<sup>41</sup>. Following the pattern of data stealing malware, cryptoware campaigns will likely become less scattergun and more targeted on victims of greater potential worth.

More recently, a new strain of server-side ransomware called SAMSAM predominately target the healthcare industry. SAMSAM, does not require user interaction but exploits the vulnerabilities of web servers and encrypts folders typically associated with web site files, images, scripts, etc<sup>42</sup>.

While there is clear indication that other malware - with a degree of magnitude more sophisticated than that openly available on any criminal market - exists either already in the wild or as a proof of concept, none appears to be “commercially available”. Its use therefore remains either limited to closed criminal groups, or out of the reach of criminality altogether. Those using it are likely to be out of the scope of a typical law enforcement investigation.

One such indicator of sophistication would be the use of information hiding techniques, such as steganography. These techniques, once solely a tool for espionage, are now increasingly being used by malware to hide its existence, communications and data exfiltration, by incorporating data in other traffic flows or media<sup>43</sup>. While this technique has only been used by a handful of malware variants so far, its very nature means that any future or existing malware using this technique may be extremely hard to detect.

## RECOMMENDATIONS

- It is essential for law enforcement to continue to allocate sufficient resources to investigate the malware and services which enables other cyber-attacks.
  - The impact the removal of a key service can have is clear<sup>44</sup>.
- Law enforcement should maintain the current momentum on prevention and awareness campaigns relating to mobile malware.
  - Encouraging the use of security software and the reporting of attacks gives both law enforcement and the security industry an overall clearer picture and thereby a greater capacity to mitigate the threat.
- Law enforcement must continue to forge and maintain collaborative, working relationships with academia and the private sector.
  - The comparison of law enforcement, industry and internet security perspectives on malware threats highlights how small a piece of the overall picture law enforcement actually sees and to some degree questions the relevance of law enforcement priorities. While there is no question that law enforcement must continue to investigate reported attacks, it must also be guided partly by the views of other industries.
- Law enforcement and industry should continue to contribute and make use of the Europol Malware Analysis Service (EMAS). Moreover, the tool needs to continue to evolve and develop to address the growing needs for malware analysis.
- The disclosure of relevant information to the public, found within the course of criminal investigations, should be encouraged and facilitated. For instance, when a server with decryption keys is found, it should be possible (or easier) for LEA to disclose this information to the public, through a cooperation with private entities. In some cases however, this may require legislative action as some countries, including EU MS, are prohibited from disclosing information during criminal investigations outside the law enforcement community.

<sup>40</sup> The Radicati Group, Mobile Statistics Report 2014-2018, <http://www.radicati.com/wp/wp-content/uploads/2014/01/Mobile-Statistics-Report-2014-2018-Executive-Summary.pdf>, 2014

<sup>41</sup> Trend Micro, FLocker Mobile Ransomware Crosses to Smart TV, <http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/>, 2016

<sup>42</sup> Trend Micro, Server-side Ransomware SAMSAM Hits Healthcare Industry, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/server-side-ransomware-samsam-hits-healthcare-industry>, 2016

<sup>43</sup> CUIng, Criminal Use of Information Hiding (CUIng) Initiative, <http://cuing.org/>, 2016

<sup>44</sup> SecurityWeek, Did Angler Exploit Kit Die With Russian Lurk Arrests?, <http://www.securityweek.com/did-angler-exploit-kit-die-russian-lurk-arrests>, 2016

# ONLINE CHILD SEXUAL EXPLOITATION



The use of the internet as a platform for child sex offenders to communicate, store and share child sexual exploitation material (CSEM) and to hunt for new victims continues to be one of the internet's most damaging and abhorrent aspects. In this chapter, we explore the current trends in the use of tools and techniques by online offenders and how they can identify, and exert their influence on, potential victims.

We welcome the adoption of the 'Luxembourg Guidelines' (the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse)<sup>45</sup> as an important document to build consensus on key concepts and strengthen collaboration between relevant stakeholders, including investigators, judicial authorities and child protection agencies.

## KEY THREAT – SEXUAL COERCION AND EXTORTION ONLINE

Online sexual coercion and extortion of children is the targeting and commoditisation of the child and/or their sexual image for the procurement of sexual gains, such as sexually explicit images of that child and/or sexual activity with the child, or for financial gain. This process is supported by a range of manipulative strategies, typically involving the use of coercion, through threats and intimidation, but also the use of deceptive strategies such as impersonation, hacking, or the theft of the child's image.

There are two main types of sexual coercion and extortion: content driven, for sexual purposes, and financially driven, with an economic motivation.

This activity is usually characterised by grooming the child or impersonating another in order to gain their trust. Once this is established the offenders exploit the child's vulnerabilities to obtain a photo or video of a sexual nature, which leads to the third phase – extortion. With content driven extortion the offender demands more photos/videos, commonly of an even more explicit nature. There can additionally be requests to involve a third person, such as a sibling or a friend, and to have offline meetings for sex. With financially driven extortion – as the name indicates – after obtaining the CSEM the child is asked for money to prevent further dissemination.

Both content and financially driven extortion is based on the threat to disclose the images on the internet and/or send it directly to family, friends, school, etc. Some research suggests that around 45% of offenders carry out their threats<sup>46</sup>.

The platforms used for sexual coercion or extortion are often social networks, online games and forums, all abundantly populated by minors. This is where the grooming process starts. Once they have gained the child's attention or trust they can migrate the communications to other platforms that allow not only chat but also video and photo sharing. Today, many of these apps have end-to-end encryption enabled by default.

<sup>45</sup> Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, [http://www.ilo.org/wcmsp5/groups/public/---ed\\_norm/---ipecc/documents/instructionalmaterial/wcms\\_490167.pdf](http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---ipecc/documents/instructionalmaterial/wcms_490167.pdf), 2016

<sup>46</sup> Janis Wolak, David Finkelhor, Sextortion: Findings from an Online Survey about Threats to Expose Sexual Images, <https://www.wearethorn.org/wp-content/uploads/2016/06/Sextortion-Report-1.pdf>, 2016



Many countries report that self-generated indecent material (SGIM) accounts for a growing volume of the CSEM in circulation. According to helpwanted.nl, 18% of SGIM is distributed further online by an unknown third party. Sexting is often used in the grooming process and by the offenders to threaten/blackmail the child; it is also seen today as an established trend amongst teenagers leading to higher quantities of CSEM available online.

Even though it is acknowledged by law enforcement worldwide as a rapidly growing problem, the growing trend of sexual coercion and extortion is still an understudied and underreported phenomenon, mostly due to the nature of the crime, including the shame and guilt felt by the victims. There are growing levels of complaints from parents against persons who attempt to obtain CSEM from their children. The accessibility of children is also higher than ever as a result of unprotected social media profiles, online games and greater access to broadband internet and mobile devices.

Some studies indicate that 100 million children will be coming online for the first time between 2012-2017, and that 80% of those will be connecting via mobile devices<sup>47</sup>. A significant proportion of these children will be connecting from African and South-East Asian countries.

There can be serious consequences for victims of this type of crime, including long-term psychological damage and an elevated risk of self-harm including suicide or suicide attempts. Therefore, the development of preventive campaigns to raise awareness and provide children with tools to protect

themselves, and the knowledge to detect and deal with this phenomenon, are essential, especially in light of the fact that around 50% of victims prefer to discuss it with their peers.

## KEY THREAT – MISUSE OF LEGITIMATE ONLINE PLATFORMS

Online access to CSEM has been facilitated by the expansion, greater accessibility and ‘user friendliness’ of tools that provide anonymisation and encryption of devices and communications. This allows an increasing number of offenders to access, download and trade CSEM more securely over the internet. This trend is reflected by the increased volume of seized material for forensic analysis in most recent cases.

One of the most popular platforms to exchange such material continues to be peer-to-peer (P2P) networks, although there has been an increase in the volume of exchanges carried out on platforms that allow anonymised access like Darknet networks (e.g. Tor).

There is also an increasing number of forums available on the Darknet that facilitate the exchange of CSEM, reflecting ongoing recovery from previous setbacks. This trend may be due to the growing popularity of Darknets which are no longer exclusive to more ‘sophisticated’ offenders but now easily accessible to those who are less technology savvy.

<sup>47</sup> Telenor Group, Telenor Group Supports ‘Stop Cyberbullying Day 2016’ Across its Markets in Asia, <http://www.telenor.com/media/press-releases/2016/telenor-group-supports-stop-cyberbullying-day-2016/>, 2016



The continuing misuse of online social networking and other platforms on the surface net cannot be disregarded either. These continue to be used by offenders in innovative and devious ways to meet, discuss and propagate the creation and distribution of child abuse material.

Child sex offending is mostly based on a deviant sexual tendency<sup>48</sup> and the currency amongst offender networks is CSEM. Unseen CSEM is of the highest value, therefore offenders with access to new material and those prepared to record or otherwise make available their abuse of children for distribution are the ones with higher status and influence within the community.

Reports from law enforcement stress that increasing numbers of victims are originating from geographic regions where previously there was little known activity. Non-Caucasian victims increasingly feature in the CSEM being exchanged by offenders. This trend can be at least partly explained by the increased penetration of broadband internet in regions such as Africa and South-East Asia and the consequential increased access to and misuse of online platforms.

There are also reports suggesting that the average age of the victims continues to fall and that CSEM continues to reflect more violent sexual abuse being inflicted on those children. In addition, activity in the areas of sexting and self-generated indecent material (SGIM) are also leading to an increase of CSEM online. A subset of this material is being generated in the context of sexual coercion and extortion as noted above.

To a lesser degree, there is also some evidence that forms of commercial child sexual exploitation such as on-demand live streaming of abuse is also contributing to the rise of the amount of CSEM online.

## KEY THREAT – FORENSIC AWARENESS OF CHILD SEX OFFENDERS

In parallel with other cybercriminals, child sex offenders increasingly favour the use of defensive measures that provide anonymisation and encryption of their online illegal activities in order to evade law enforcement. While this is partly due to the ready availability of such tools, it is also to some extent the result of knowledge sharing amongst offenders.

Common tools used by offenders include IP anonymisation tools, encryption for both devices and communications, wiping software or operating systems, virtualisation and cloud storage. Such techniques have been reported by some countries to be found in ‘almost all cases’. Historically the use of these techniques was associated with the more ‘sophisticated’ offenders. Today this is not the case, and it is becoming the norm.

Darknet and surface net platforms not only allow exchanging the newest CSEM but also allow the exchange of techniques to elude and hamper law enforcement activities. This mutu-

al support and camaraderie is a worrying trend. Through the exchange of this knowledge offenders reduce their risk of discovery thus diminishing the seriousness of the offences, which may encourage previously reluctant offenders into ‘hands-on’ offending.

The use of encryption is an established trend and the use of encrypted communications has recently been heavily associated with sexual coercion and extortion cases. The use of encrypted devices is also growing, and poses a significant problem for evidence gathering as the content in the physical devices is not accessible to law enforcement or can be ‘wiped out’ by pre-installed software.

## KEY THREAT – LIVE STREAMING OF CHILD SEXUAL ABUSE

Live distant child abuse is still being reported as a growing threat. The live streaming of child sexual abuse on the internet involves a perpetrator directing the live abuse of children on a (pre-arranged) specific time-frame through video sharing platforms. The abuse can be ‘tailored’ to the requests of the soliciting offender(s) and recorded to further disseminate on Darknet sites and/or P2P networks. This dissemination contributes to the growth of CSEM available on the internet.

Live streaming abuse of children is facilitated by end-to-end encrypted platforms where not even the service providers can access what is being shared amongst their users, hampering the evidence collection and also weakening preventive approaches to tackling this crime. There are a great variety of payment methods available to the offenders, including digital currencies. Usually the amounts being transferred are low, and are therefore unlikely to generate alerts even if regulated financial services are used to transfer payments.

Traditionally the victims of live distant child abuse were based in South-East Asia, in particular the Philippines. More recent reports indicate that it is now spreading to other countries. Regions of the world with high levels of poverty, limited domestic child protection measures and easy access to children are being targeted by offenders for all types of CSEM, including live streaming.

There is evidence that supports the link between the live streaming of child sexual abuse and subsequent travelling for the purpose of child sexual exploitation – so-called hands-on offending. Following the live streaming abuse, the soliciting offender can travel to the country/place where the original abuse occurred so they themselves can sexually abuse the child. Equally, those who have travelled to abuse children may engage in live streaming activity on their return, having made the arrangements while in the country.

Live distant child abuse has the most obvious links with commercial distribution of CSEM. As new and/or unseen CSEM is valuable currency within the offending community, live distant abuse is therefore a way to not only acquire more CSEM, but

<sup>48</sup> Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, [http://www.ilo.org/wcmsp5/groups/public/---ed\\_norm/---ipecc/documents/instructionalmaterial/wcms\\_490167.pdf](http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---ipecc/documents/instructionalmaterial/wcms_490167.pdf), p85., 2016

to simultaneously generate material with a high 'value'. It is a perverse way of converting money into the accepted currency and simultaneously gratifying their sexual urges. It is also linked to offenders' forensic awareness as the activity leaves less traditional evidence on digital media.

## FUTURE THREATS AND DEVELOPMENTS

In the last decade cybercrime and cyber-enabled crime have grown in parallel with rapid developments in technology, and show no signs of decelerating anytime soon. In the next few years, we can optimistically expect a shift in policies, on a national and international level, to better tackle these crimes, including online CSE. For instance, a new legal definition and criminalisation of online sexual coercion and extortion, rather than one that falls under the existing definition of extortion.

We can expect to encounter an increase in the use of anonymous payment systems such as digital currencies. Such payment systems, which are already integral to ransomware, may become the currency of choice for financially driven sexual extortion or for the payment of the live streaming of child sexual abuse.

The growing availability of internet-enabled mobile devices and their ownership amongst minors, coupled with the development of new and existing communication apps which focus on security, will create further areas of risk for potential victims and added challenges for law enforcement.

Advances in facial recognition software may lead to offenders using this technology to identify and/or locate potential victims in the real world through their social media by matching existing images in their possession to those published in the social media profiles<sup>49</sup>. Similarly, developments within apps and social media platforms in relation to geolocation may also make it easier for offenders seeking hands-on contact to locate their victims.

2016 has seen the release of several consumer virtual reality (VR) devices, with a number of other virtual and augmented reality products on the near horizon. It is possible that such devices could be used to simulate abuse on a virtual child or view CSEM. While there is currently no evidence that they are being used for such a purpose, the VR pornography industry is already well established in Asia and all it would require is someone with sufficient programming skills and intent to produce the appropriate content. Previous adoption of technologies by offenders and those with a commercial interest in this area would indicate this as a likely development.

## RECOMMENDATIONS

- There should be a continuous effort from all parties to prioritise the victim in the investigation of these crimes. That includes law enforcement investing human and IT resources to improve the opportunities for victims to be identified. Training in and use of victim identification methodologies, increased use of VID databases and the fine analysis of the seized CSEM at local, national and international level are essential steps in this. Such strategies are regularly demonstrated to be valuable in locating children harmed by abuse and preventing that abuse from continuing.
- Law enforcement needs to have the tools, techniques and expertise to counter the criminal abuse of encryption and anonymity by networks of online offenders and in the distribution and storage of CSEM.
- Law enforcement needs to develop the required tools, tactics and EU-wide measures to address the abuse of peer-to-peer networks and the Darknet to distribute CSEM.
- Alongside NGOs and private industry, law enforcement must maintain its focus on the development and distribution of prevention and awareness raising campaigns. Such campaigns must be updated to encompass current trends such as sexual extortion and coercion and self-generated indecent material.
  - Raising awareness and providing children, parents and caretakers with the appropriate knowledge and tools is essential to reduce this threat.
- Law enforcement should continue to strengthen cooperation with the private sector, specifically content and service providers, to encourage the integration of mechanisms which allow the early detection, blocking and removal of CSEM online.
- Law enforcement needs to further improve the existing NCMEC information flow and establish similar information flows with other relevant partners.
- Investigators, judicial authorities and child protection agencies should familiarise themselves with the 'Luxembourg Guidelines'<sup>50</sup> (the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse) to strengthen collaboration between relevant stakeholders.
- Increased capacity building and training among the judiciary is needed to better understand the technical merits of a case and to better deal with technically geared defences.

<sup>49</sup> The Guardian, Face Recognition App Taking Russia by Storm May Bring End to Public Anonymity, <https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte>, 2016

<sup>50</sup> Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, [http://www.ilo.org/wcmsp5/groups/public/---ed\\_norm/---ipecc/documents/instructionalmaterial/wcms\\_490167.pdf](http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---ipecc/documents/instructionalmaterial/wcms_490167.pdf), 2016

# PAYMENT FRAUD

Despite facing competition from instant payments based on the SEPA credit transfer, non-bank payment institutions and relatively low, yet gradually increasing adoption of virtual currencies, payment cards remain a very popular payment method<sup>51</sup>. In 2014, the number of payment card transactions including debit and credit cards rose by 8.8% to 47.5 billion, with a total value of €2.4 trillion<sup>52</sup> while other payment services including credit transfers, direct debits or cheques remained stable or decreased.

As many as 85% of internet users feel that the risk of becoming a victim of cybercrime is increasing<sup>53</sup>. The increases in both actual crimes and the perceived risk of potential crime cause significant costs to the EU economy both in terms of direct costs as well as lost opportunities.

## KEY THREAT – CARD – PRESENT FRAUD

While skimming still represents a major threat it was reported to be in downturn in the majority of jurisdictions with no EU Member States experiencing an increase in number of investigations last year.

EMV (Chip and Pin) compliance has reached almost 100% across the EU, which prevents card-present fraud from becoming a more significant issue. Increasingly efficient preven-

tion measures have gradually forced criminals to adapt and migrate their 'cash out' operations to non-EMV compliant jurisdictions. Skimmed data is mostly uploaded to blank cards and cashed out overseas, mainly by OCGs having a permanent presence in the Americas and South East Asia, with the USA, Indonesia and Philippines identified as the top three destinations. Skimming losses relating to the usage of compromised European card data outside Europe have risen to the highest level seen since 2008<sup>54</sup>. This geographical displacement has had negative repercussions for EU law enforcement as it is often more complex and slower to obtain evidence.

However, card-present fraud can also be bi-directional in nature as demonstrated by several OCGs, which send their members to EU countries in order to purchase high value goods with forged cards using compromised details harvested overseas.

The abuse of cards overseas can be effectively mitigated by geoblocking<sup>55</sup>, as evidenced in the countries where the majority of issuers put this into practice. However, geoblocking is far from being universally applied and consequently criminals may still abuse cards issued by non-compliant entities.

Several Member States reported other forms of card present fraud, including shoulder surfing or card- and cash-trapping, as a recurring issue. However the general impact of the crime as well as the overall trends have a decreasing tendency throughout Europe.



<sup>51</sup> Yves Mersch, ECB Executive Board, <https://www.ecb.europa.eu/press/key/date/2016/html/sp160118.en.html>, 2016

<sup>52</sup> European Central Bank, Press Release on October 15, 2015, Payment Statistics for 2014, <https://www.ecb.europa.eu/press/pdf/pis/pis2014.en.pdf>, 2015

<sup>53</sup> Eurobarometer 423 on Cyber Security, [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_423\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf), 2015

<sup>54</sup> European ATM Security Team (EAST), Card Skimming Losses Continue to Rise Outside Europe, 2016

<sup>55</sup> Geoblocking is the practice of restricting access or use - in this case the use of payment cards - to specific geographic regions.



## ■ DEEP INSERT SKIMMING ATTACKS

As anti-skimming protection gets more efficient, criminals adapt their attack approaches. Standard ATM skimming protection and detection measures can be circumvented through the use of deep insert skimmers that are invisible to the users of the machine. Both law enforcement and ATM manufacturers across Europe have reported the discovery of such devices<sup>56</sup>. This threat may be partially mitigated through the application of an ATM firmware update with a version that detects insertion of deep insert devices. However, adoption of this protection measure is not a simple task as there are 411 243 ATMs throughout Europe as of 2015<sup>57</sup>.

## ■ STAGES OF ORGANISED ATM SKIMMING:



## KEY THREAT - ATM MALWARE

The emergence and proliferation of ATM malware is a reminder that OCGs are developing new criminal opportunities by constantly shifting their attack vectors. There has been a confluence of factors resulting in the shift from skimming to more advanced attacks. Anti-skimming and other preventive measures, such as EMV and geoblocking, have rendered traditional card-present fraud more difficult. However, outdated and insecure ATM operating systems, coupled with a shift

from custom to standard PC hardware components, has left ATMs more vulnerable to malware attacks.

Additionally, a large number of proprietary technologies in ATMs have been replaced with standardised APIs (Application Programming Interfaces) that allow interaction with ATM hardware regardless of model and type. While the hardware and software standardisation has brought a number of benefits for the financial institutions, it has made ATMs more attractive targets, as the same malware can be reused on multiple devices<sup>58</sup>.

Although ATM malware has frequently been discussed as a growing problem, and the number of attacks has significantly increased since 2013, it is still vastly outnumbered by the number of skimming attacks. This is also reflected by the fact that only a limited number of countries reported active investigations into digitally facilitated ATM Attacks. Furthermore, the majority of these investigations related to the black boxing technique, where the attacker's computer connects directly to the cash dispenser and issues dispensing instructions, and were not malware attacks.

Many of these attack vectors could be designed out in close cooperation with industry.

## KEY THREAT - E-COMMERCE FRAUD

Statistics provided by the ECB indicate that 66% of total card fraud value is the result of card-not-present (CNP) transactions<sup>59</sup>. This figure represents yet another increase on the previous year and is echoed by law enforcement experience.

The use of compromised credit card details is an increasingly high volume crime, with tens of thousands of criminal complaints in many EU countries. An increase in CNP fraud is apparent across almost all sectors; the purchases of physical goods, airline tickets, car rentals and accommodation with compromised cards have generally seen an increase throughout the EU.

In some cases, the offenders identify a vulnerability within a merchant's payment process and exploit it before the merchant can identify and address the issue. Such an approach has led to huge losses for individual merchants.

The monetisation of fraudulently purchased goods has seen little variation compared to previous years. Once high value items are purchased, they are often reshipped through several layers of packet mules abroad, frequently to Eastern Europe and monetised through buy-and-sell websites.

*The UK's DCPCU and Visa Europe, supported by Europol, carried out the first ever Retail Week of Action, a joint operation targeting e-commerce fraud. The operation saw the financial industry and retailers share live data with law enforcement which was used to target suspects using stolen card details to purchase high value goods including electronics, designer clothes and household equipment. Eleven people were arrested during the operation and goods worth more than €280 000 were seized.*

<sup>56</sup> NCR, Expansion of Deep Insert Skimming Attacks:

<http://www.ncr.com/wp-content/uploads/NCR-Security-Alert-2016-05-Expansion-of-Deep-Insert-Skimming-Attacks.pdf>, 2016.

<sup>57</sup> European ATM Security Team (EAST), ATM in Europe, 2016.

<sup>58</sup> Trend Micro and EC3: ATM Malware on the Rise: A comprehensive Overview of the Digital ATM Threat, 2016.

<sup>59</sup> European Central Bank: Fourth Report on Card Fraud, [https://www.ecb.europa.eu/pub/pdf/other/4th\\_card\\_fraud\\_report.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf), 2015.

## ■ AIRLINE TICKET FRAUD

Airline companies are among the most affected by CNP fraud. The airline industry is estimated to lose over one billion dollars per year<sup>60</sup> as a result of the fraudulent online purchases of flight tickets. Furthermore, individuals travelling on fraudulently purchased airline tickets are often involved in terrorism or other forms of serious organised crime or including trafficking in human beings (THB) or drugs smuggling.

For most airline ticket fraud, the interval between ticket purchase and travel time is typically less than two days<sup>61</sup>. Often criminals will book a flight in the afternoon in order to fly the next day. Airlines are under pressure to develop efficient mechanisms to identify fraudulent transactions while keeping the impact on legitimate customers as low as possible. False positives resulting in mistaken cancellations are costly for airlines, as the denied travellers are entitled to compensation ranging from between €250 and €600<sup>62</sup>, with potential reputational damage on top of this.

*In June 2016, the seventh Global Airline Action event was held, involving over 74 airlines and 43 countries, taking place in over 130 airports around the world over two days. With coordination centres at Europol in The Hague, INTERPOL Singapore and Ameripol in Bogota, and further support from Canadian and US law enforcement authorities, the operation resulted in 140 individuals being detained under suspicion of fraud following the reporting of over 250 suspicious transactions<sup>63</sup>.*

## FUTURE THREATS AND DEVELOPMENTS

In last year's report we highlighted the first functional ATM equipped with facial recognition, unveiled in China. Weeks later, a major financial institution tested ATMs capable of performing retinal scans<sup>64</sup>. It is unclear yet, however, how much need or appetite there is for such authentication technologies on ATMs, and therefore to what extent they will be adopted globally.

The increasing implementation of geoblocking and 3D Secure<sup>65</sup>, apart from their obvious positive impact, is likely to further displace fraud to countries and businesses that have not yet implemented these preventive measures. The 2015 IOCTA highlighted the liability shift of losses to merchants following the migration to EMV in the US. Consequently the top 100 merchants in the US, who collectively generate 80% of all face-to-face transactions, are now EMV enabled<sup>66</sup>.

As the financial institutions increasingly issue EMV cards to their respective card bases, we can expect US merchants to be fully EMV compliant within two years. This will likely push card-present fraud to other jurisdictions or make criminals turn to CNP in search of the path of least resistance. However, this also increases the risk of attacks on the EMV technology, so further innovations are needed to keep that platform secure.

The possibility of compromising NFC transactions was explored by academia years ago and it appears that fraudsters have finally made progress in the area. Several vendors in the Darknet offer software that uploads compromised card data onto Android phones in order to make payments at any stores accepting NFC payments. Moreover, at least one Member State reports instances of OCGs using contactless cards purchased from individuals who then report the card as lost. The OCGs were able to reset the cards once they had reached the purchase limit thereby allowing continued spending.

Fraudulent use of NFC payments would have a number of unexpected consequences including the inability of merchants to confiscate the compromised card. Currently, when merchants detect a fraudulent transaction they are requested to seize the card. However, the confiscation may not be feasible when the compromised card data are recorded on the buyer's smartphone.

## RECOMMENDATIONS

- Successful initiatives targeting fraud in the airline industry should be replicated to cover additional sectors. Operations where offenders have to arrive at a physical location to benefit from fraudulent transactions, such as car rentals or other pre-ordered services, may be particularly effective.

<sup>60</sup> IATA, 2016.

<sup>61</sup> CEPOL Webinar on Airline Fraud Notification Tool, 2016

<sup>62</sup> Regulation (EC) No 261/2004 of the European Parliament and of the Council, <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32004R0261>, 2004

<sup>63</sup> Europol Press Release, More Than 140 Detained in Global Action Against Airline Fraud, <https://www.europol.europa.eu/content/more-140-detained-global-action-against-airline-fraud>, 2016

<sup>64</sup> The Wall Street Journal: The Eye-Scanning ATM Is Here, <http://www.wsj.com/articles/the-eye-scanning-atm-is-here-1445815637>, 2015

<sup>65</sup> 3D Secure is an online fraud prevention measure familiar through Verified by Visa or MasterCard SecureCode.

<sup>66</sup> Stephen W. Orfei, PCI Security Standards Council, 2016

- Where resources permit, law enforcement should consider embedding staff temporarily within the private sector and vice versa. This would improve cooperation and collaboration and provide law enforcement with valuable insights into how the industry operates, which may be beneficial for preventative and investigative purposes.
- Additional effort is required, through more focused information sharing within law enforcement and/or partnerships with private industry, to link cases of card fraud. This would facilitate the identification of organised crime groups involved in card fraud.
  - Looked at in isolation, the fragmented nature of card fraud means that it is often given a low priority.
- A coordinated effort should be made by law enforcement to engage with countries where compromised cards are cashed out and where goods purchased with compromised cards are reshipped.
- Law enforcement should make greater use of the Europol Malware Analysis System (EMAS) by submitting ATM and PoS malware samples in order to identify links to other cases and improve a community-wide understanding of the threat.
- Investigators focusing on ATM crime should familiarise themselves with a comprehensive overview of the digital ATM threats called “ATM Malware on the Rise”, a joint EC3 and Trend Micro report on malware threats and specific types of malware in circulation.
- Industry should take action to design out security flaws from new and existing software and hardware.

**EUROPOL**

**Airline industry** (Airplane icon) | **Law Enforcement** (Police badge icon) | **Losses of USD 1 billion** for the airline industry

**Credit card industry** (CARD icon) | **Travel industry** (PASS icon) | **The International Air Transport Association (IATA)** took part in the action, providing important fraud intelligence from its database

**Europol** deployed specialists and equipment to locations across Europe.

A dedicated team of analysts working from the **Europol operational centre** provided live access to centralised criminal intelligence databases.

**Credit card fraud linked to:** drug trafficking, fraud with counterfeit payment cards, organising illegal immigration

**Aim of action**

- Target the criminal online services offering credit card credentials and fake plane tickets
- Protect consumers from being duped by these criminal enterprises

**140** detained under suspicion of fraud

**252** suspicious transactions reported



# SOCIAL ENGINEERING



As an attack vector social engineering has been utilised in many different crime areas and cybercrime is no exception. In fact, many internet security companies continuously highlight the human factor as the weakest link in cyber security. Influencing people into acting against their own interest or the interest of an organisation is often a simpler solution than resorting to malware or hacking.

Both law enforcement and the financial industry indicate that social engineering continues to enable attackers who lack the technical skills, motivation to use them or the resources to purchase or hire them. Additionally, targeted social engineering allows those technically gifted to orchestrate blended attacks bypassing both human and hardware or software lines of defence.

2015 saw more replication than invention in this area. Law enforcement observed that techniques that used to work in the past continue to be recycled, polished and reintroduced. Nevertheless, several Member States noticed an improving overarching quality of phishing attempts and other scams.

## KEY THREAT - CEO FRAUD

There are several terms used to describe CEO fraud, including business email compromise and mandate fraud. The fraud involves an attacker contacting the victim and requesting an urgent bank transfer or a change of bank account details for upcoming transactions. This may be carried out through pure social engineering but the advanced forms of the compromise may be combined with hacking or even the deployment of malware.

Attacks are often preceded by a substantial amount of research and reconnaissance, mapping the organisations' structure and behaviour of potential victims. Criminals target senior staff to take advantage of organisational hierarchies and the fact that more junior staff are less likely to challenge senior management. The perpetrators assume the identity of the CEO, president or a managing director to send a targeted email to a person in charge of making financial decisions, such as a CFO, financial controller or accountant. Letters, emails or phone calls also may come from outside the company, when a payment request is sent by someone purporting to be a trusted business partner or a lawyer.

The request is usually time-sensitive and often coincides with the close of business hours to make verification of the request difficult. Such attacks often take advantage of publicly reported events such as mergers, where there may be some degree of internal flux and uncertainty.

To avoid raising doubt, attackers will follow corporate procedure, using language that is often specific to the company. The payment method is also consistent with victim's usual business practices, which is typically a bank transfer.

Several countries reported a notable increase in CEO fraud in the last year and identified it as a key social engineering threat, a view supported by the financial sector. Businesses of all sizes in both the private and public sector are targeted.

The fraud continues to affect tens of thousands of victims worldwide resulting in the loss of billions of euros<sup>67</sup>. The losses for individual companies were often in the hundreds of thousands or even millions. Despite the often considerable financial damages, victims do not always report such crimes to avoid reputation damage. This prevents law enforcement from obtaining a clear picture of the scale and scope of the threat. Where law enforcement has been able to investigate, it has been noted that some OCGs formerly engaged in MTIC fraud now appear to be involved in CEO fraud.

*Sixty suspects, mainly from Spain, Nigeria and Cameroon, were arrested as part of Operation Triangle, coordinated by Europol and Eurojust and led by Italian, Spanish and Polish authorities with the support of the UK, Belgium and Georgia. The suspects utilised a combination of hacking and social engineering to monitor internal communication within medium and large European companies before requesting a bank transfer to accounts controlled by the criminal group.*

## KEY THREAT - PHISHING

Phishing has developed into one of the most widespread attack vectors, and can either be used on its own or as a preliminary step to a further attack. Some industry reporting indicates that phishing rates in general continued to gradually decline throughout 2015<sup>68</sup>, although it had something of a resurgence in the first quarter of 2016<sup>69</sup>. However, the overall decrease in 2015 is not consistent with the trends observed by the Member States, most of whom reported an increased number of investigations.

An explanation for this may be that while the use of scattergun, mass phishing campaigns may be in decline, the number of targeted, spear phishing attacks is increasing; a trend confirmed by industry. Such attacks, which are more likely to target higher value targets, are perhaps more likely to be reported to law enforcement.

The quality of phishing messages and websites is also increasing. It is not always possible for an intended victim to rely on poor grammar, spelling and punctuation, or simply poor drafting as an indication that a particular message may be fraudulent. Professional looking phishing websites continue to be generated by easy-to-obtain phishing kits that require little technical skill to be installed and customised on a remote server. To complement the theft of login credentials, phishing may also be used as an effective way to bypass two-factor authentication<sup>70</sup>.

The most common vishing<sup>71</sup> scheme, commonly known as

the “Microsoft support scam” appears to be limited to a relatively small number of Member States, although those affected continue to report a large number of incidents. In some cases, the scam has evolved from cold-calling unsuspecting victims to the attacker fooling victims into calling them directly<sup>72</sup>. Member States have observed that OCGs have increasingly recruited or outsourced native speakers.

Phishing is not limited to desktop users. Phishing smartphone apps, particularly on the Android platform, often slip through the Google Play review process. These malicious apps collect credentials and other information and deliver it to the attackers. These applications are often downloaded from trusted locations and the phishing website is accessed from the app so that users do not see the malicious URL. E-banking and bitcoin wallet apps in particular are targeted<sup>73</sup>.

## KEY THREAT - ADVANCED FEE FRAUD

A wide variety of advanced fee frauds continue to be reported to law enforcement. Of these, romance scams, which can result in both monetary losses and psychological damage, are one of the most commonplace. Despite media coverage and prevention activity in many countries, this type of crime has increased across several Member States.

Another common method highlighted by law enforcement includes scams that react to the latest geopolitical developments, for example fraudsters presenting themselves as US soldiers serving in Afghanistan or similar locations. Alternatively, criminals may assume the identity of a female refugee requiring financial support.

Many perpetrators of these offences seem to originate in developing countries. The multi-jurisdictional element of the advanced fee frauds in combination with their high quantity contributes to a generally low detection rate for these offences.

<sup>67</sup> FBI, Public Service Announcement, Business E-mail Compromise: The 3.1 Billion Dollar Scam, <https://www.ic3.gov/media/2016/160614.aspx>, 2016

<sup>68</sup> Symantec, Internet Security Threat Report Volume 21, <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>, 2016

<sup>69</sup> APWG, Phishing Activity Trends Report, [http://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2016.pdf](http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf), 2016

<sup>70</sup> Firstpost, Hackers Using Social Engineering To Bypass Two Factor Authentication, <http://tech.firstpost.com/news-analysis/hackers-using-social-engineering-to-bypass-two-factor-authentication-321121.html>, 2016

<sup>71</sup> Vishing refers to voice phishing, typically occurring over the telephone.

<sup>72</sup> Symantec, Internet Security Threat Report Volume 21, <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>, 2016

<sup>73</sup> PhishLabs Blog, Fraudster Phishing Users with Malicious Mobile Apps, <https://info.phishlabs.com/blog/fraudster-phishing-users-with-malicious-mobile-apps>, 2016

## FUTURE THREATS AND DEVELOPMENTS

As the quality and authenticity of phishing tools and services continues to increase, we can expect the increase in targeted spear phishing attacks to continue. With the availability of such tools, we can perhaps expect the mass, scattergun phishing campaigns to become more associated with low skilled cybercriminals, new to the arena, while experienced and more skilled attackers focus on targeted attacks. However, it is as likely that any attack method that generates profit will be used by all levels of criminality.

As existing and emerging social networks and social apps consider the incorporation of some form of payment, perhaps through virtual currencies<sup>74</sup>, we can expect criminals to take advantage of these platforms which efficiently combine both the stage upon which they can socially engineer their victims and obtain payment from them.



## RECOMMENDATIONS

- Member States should consider implementing more efficient reporting channels for high volume crime. Online reporting that allows the victim to report the crime without the need to contact local police is particularly fit for purpose.
- When it comes to addressing volume crimes, investing resources into prevention may be more effective than investigation of individual incidents. In addition to raising awareness and providing crime prevention advice, the campaigns should advise the public on how to report the crime.
- Education and awareness on cyber-security and safety should be introduced as 'life skills' from an early age.
- Prevention campaigns should be coordinated with other national and international organisations to avoid duplicating initiatives that may already be in place.
- Successful operational results demonstrate that when joining forces, affected businesses and law enforcement authorities can successfully investigate cross-border CEO fraud. Timely reporting and sharing of relevant information forms a solid basis for such investigations.
- Implementation of a "four-eyes" or "two-signature" principle is recommended by international accountants and advisory companies/organisations. Such principles add additional controls to prevent large fraudulent transactions such as those found in CEO fraud.

<sup>74</sup> For example <https://www.ipayyou.io> or <http://www.coinia.fi>



# DATA BREACHES AND NETWORK ATTACKS

It is increasingly clear that any internet facing entity, regardless of its purpose or business, must consider itself and its resources to be a target for cybercriminals. When taking into account the safety and security of these networks, there are a number of key threats that must be considered.

## KEY THREAT – DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

Among the wide range of services offered in the digital underground, DDoS is one of the most popular. This particular type of attack can be used by cybercriminals, not only launch to attacks on public and private organisations and businesses, but also on their own competitors and rivals<sup>75,76</sup>.

In our last report it was indicated that attacks over 100 Gbps<sup>77</sup> were uncommon. Later in 2015 there were reports of attacks exceeding 300 Gbps. 2016 has already seen record attacks allegedly exceeding 600 Gbps, targeting the global website of the BBC and US presidential candidate Donald Trump's website<sup>78</sup>. These attacks were intended to demonstrate the effectiveness of a new DDoS-as-a-service tool BangStresser. Indeed, tools such as these, commonly referred to as 'booters' or 'stressers' and readily available as-a-service on the internet, accounted for a significant proportion of DDoS attacks reported to law enforcement.

Half of EU Member States reported investigations into DDoS attacks. While a significant proportion of these attacks were attempts at extortion, these attacks were often either purely malicious or had an unclear motive.

Throughout 2015 two names dominated the DDoS attack scene – DD4BC (DDoS for Bitcoin) and the Armada Collective, receiving wide coverage in the media.

*In December 2015, law enforcement agencies from Austria, Bosnia and Herzegovina, Germany and the United Kingdom joined forces with Europol and the J-CAT for Operation DD4BC, targeting the cybercriminal group DD4BC. The operation resulted in the arrest of a main target and resulted in the cessation of attacks from both DD4BC and the Armada Collective<sup>79</sup>.*



The Armada Collective was suspected to be a copy-cat, as their tactics bore many similarities and both stopped their activities following the arrests in December 2015. Both groups have spawned scammers who continue to extort enterprises based on the reputation of the original criminal gangs, demanding ransoms or 'protection money' when they in fact lack both the intention and capability to launch such an attack<sup>80</sup>.

## KEY THREAT – NETWORK INTRUSIONS

Almost half of Member States indicated that they had been involved in investigating attacks on private networks. The primary criminal intent for these attacks was to steal data, although there were additionally half as many attacks that related to VoIP<sup>81</sup> fraud or were simply malicious. Over a third of Member States also reported investigations into attempts specifically to gain unlawful access to intellectual property. Both industry<sup>82</sup> and law enforcement see similar patterns in the techniques used to obtain such unauthorised access, with hacking and exploiting network vulnerabilities as the

<sup>75</sup> SecureWorks, Underground Hacking Markets Report, <https://www.secureworks.com/resources/wp-underground-hacking-markets-report>, 2014

<sup>76</sup> DeepDotWeb, Meet the Market Admin Who Was Responsible for the DDoS Attacks, <https://www.deepdotweb.com/2015/05/31/meet-the-market-admin-who-was-responsible-for-the-ddos-attacks/>, 2015

<sup>77</sup> Gigabits per second.

<sup>78</sup> The Hacker News, 602 Gbps! This May Have Been the Largest DDoS Attack in History, <http://thehackernews.com/2016/01/biggest-ddos-attack.html>, 2016

<sup>79</sup> Europol Press Release, International Action Against DD4BC Cybercriminal Group, <https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group>, 2016

<sup>80</sup> ArsTechnica, Businesses Pay \$100,000 to DDoS Extortionists who Never DDoS Anyone, <http://arstechnica.com/security/2016/04/businesses-pay-100000-to-ddos-extortionists-who-never-ddos-anyone/>, 2016

<sup>81</sup> Voice over Internet Protocol

<sup>82</sup> Verizon, 2016 Data Breach Investigation Report, <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>, 2016

most common technique, followed by malware and then social engineering. It has been suggested that Dridex, one of the key malware threats identified in this year's report, was likely a major factor in these attacks<sup>83</sup>.

## ■ DATA BREACHES

While there are no specifics from law enforcement, other reporting indicates that industries such as accommodation and retail account for a significant percentage of breaches as the data from these sources are highly valued by financially motivated criminals<sup>84</sup>. Virtual currency exchangers, as well as traders on these platforms are particularly attractive targets for hacking attacks. 2016 has seen a number of exchanges being successfully hacked with both company and customer funds directly transferred to the attackers, via pseudonymous payment mechanisms (usually Bitcoin) which prevents retrieval of the funds. Some reports indicate that up to 89% of data breaches have a financial or espionage motive<sup>85</sup>.

It is not only financial credentials or intellectual property that is desirable however. 2015 saw the healthcare industry heavily targeted by attackers<sup>86,87</sup>. Moreover, following the breaches of Ashley Madison and AdultFriendFinder earlier in 2015, there appears to be a trend in targeting online services catering to 'consenting adults', with further breaches occurring in 2016. Criminals targeting these services can gain not only financial data for using in financial fraud, but also potentially compromising sensitive customer data which can additionally be used for extortion<sup>88</sup>.

Cryptsy, Shapeshift, Gatecoin and Bitfinex all suffered large scale hacks in 2016. The Bitfinex breach in particular, resulting in loss of almost 120,000 bitcoins<sup>89</sup> represents the largest loss of funds since the notoriously known Mt. Gox incident in early 2014 when over 744,000 bitcoins was lost. Unlike most attacks in early years of the technology, many companies affected by recent criminal activity have reported the incidents to law enforcement and actively support investigation efforts.

Interestingly, a number of services in the criminal underground were also breached<sup>90,91</sup>, disclosing credentials and other attributable data used by cybercriminals during their online activity. The identity of the perpetrators of these attacks is unknown, but whether coming from a 'white hat', rival criminal or cyber-vigilante, such disclosures provide law enforcement with a wealth of invaluable information.

## ■ VOIP/PBX FRAUD

Private Branch Exchange (PBX) or Dial Through fraud is by no means a new crime, having been around for more than 20 years, however the shift to IP-based networks has created new opportunities for criminals. PBXs are telephone systems used by businesses to communicate both internally and externally. PBX fraud is the routing of calls to premium rate or special service numbers through a compromised exchange. Attackers running these premium phone lines can make significant profits<sup>92</sup>, while the hacked company is liable for the call charges, which can escalate rapidly. Unlike other types of network attacks, PBX fraud seldom makes the news despite being one of the biggest financial threats facing businesses operating in the VoIP space, or any business operating an IP-enabled PBX<sup>93</sup>. Globally, PBX fraud costs industry in excess of €34 billion per year<sup>94</sup>.

Over one quarter of Member States reported investigations into this type of fraud, with those that did so almost unanimously agreeing that the threat is growing.

## OTHER THREATS – WEBSITE DEFAACEMENT

While probably representing the least sophisticated type of attack in this category, the defacement of public and private websites belonging to government and industry is nonetheless a common one. Over one third of Member States and many non-EU states investigated website defacements. Often, case numbers were low, however such incidents were especially widespread following terrorist attacks. Consequently, France and Belgium were particularly affected in 2015/2016. Hacktivism appears to be the primary motivation behind the majority of these attacks, although a significant number were purely malicious.

The following table outlines some of the data breaches from the first half of 2016 that impact on the EU. These breaches originate either from within the EU, or from outside the EU, but involve significant numbers of EU citizens. In this context, a breach is defined as an incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorised party<sup>95</sup>.

<sup>83</sup> Verizon, 2016 Data Breach Investigation Report, <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>, 2016

<sup>84</sup> Verizon, 2016 Data Breach Investigation Report, <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>, 2016

<sup>85</sup> Verizon, 2016 Data Breach Investigation Report, <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>, 2016

<sup>86</sup> Ponemon Institute, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, <http://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1>, 2016

<sup>87</sup> Forbes, Data Breaches in Healthcare Totaled Over 112 Million Records In 2015, <http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#ec3fb0e7fd5a>, 2015

<sup>88</sup> International Business Times, Fling.com Breach: Passwords and Sexual Preferences of 40 Million Users Up for Sale on Dark Web, <http://www.ibtimes.co.uk/fling-com-breach-passwords-sexual-preferences-40-million-users-sale-dark-web-1558711>, 2016

<sup>89</sup> Financial Times, Bitcoin Bitfinex Exchange Hacked: The Unanswered Questions, <http://www.ft.com/cms/s/0/1ea8baf8-5a11-11e6-8d05-4ea66292c32.html>, 2016

<sup>90</sup> ArsTechnica, Breach of Nulled.io Crime Forum Could Cause a World of Pain for Members, <http://arstechnica.com/security/2016/05/breach-of-nulled-io-crime-forum-could-cause-a-world-of-pain-for-members/>, 2016

<sup>91</sup> Office of Inadequate Security, ShOping.su Hacked, Thousands of Credit Cards and Accounts Leaked, <https://www.databreaches.net/shOping-su-hacked-thousands-of-credit-cards-and-accounts-leaked/>, 2016

<sup>92</sup> The Register, PBX Phone System Hacking Nets Crook \$50 million Over Four Years, [http://www.theregister.co.uk/2016/02/12/pbx\\_hacking\\_nets\\_crooks\\_50m/](http://www.theregister.co.uk/2016/02/12/pbx_hacking_nets_crooks_50m/), 2016
















<sup>93</sup> VoIP Fraud Analysis, Simwood 2016

<sup>94</sup> CFA, 2015 Global Fraud Loss Survey, <http://cfca.org/fraudlosssurvey/2015.pdf>, 2015

<sup>95</sup> Verizon, 2016 Data Breach Investigation Report, <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>, 2016



# DATA BREACHES IMPACTING ON THE EU<sup>96</sup>

ORGANISATION	INDUSTRY	COUNTRY	SOURCE OF BREACH	RECORDS COMPROMISED	DATA COMPROMISED
Fling	Adult		Malicious outsider	40 000 000	Email address, passwords, IP address, date of birth, sexual preferences
T Mobile	Telecoms		Malicious insider	1 500 000	Undisclosed
Kiddicare	Retail		Malicious outsider	794 000	Name, address, email address, telephone number
Nullified.io	Criminal		Unknown	474 000	Username, email address, IP address, hashed password, personal messages
Kinoptic	Technology		Accidental loss	198 000	Username, email address, hashed password
Rosebutt Board	Adult		Malicious outsider	107 000	Username, email address, IP address, hashed passwords
Postbank, Commerzbank, and Landesbank Berlin	Finance		Malicious outsider	85 000	Credit card data
Swiss People's Party (SVP)	Government		Malicious outsider	50 000	Name, email address
Islamic State Human Resources & Recruiting	Military		Malicious insider	22 000	Name, address, telephone number, place of birth and sponsor
University of Greenwich	Education		Malicious outsider	21 000	Name, address, date of birth, telephone number, signature
Engitel	Technology		Hacktivist	20 000+	Username, email address
Faithless	Entertainment		Malicious outsider	18 000	Email address
National Childbirth Trust (NCT)	Other		Malicious outsider	15 000	Email address, username, password
ShOping.su	Criminal		Malicious outsider	16 500	Username, email address, compromised card details
University of Liverpool	Education		Malicious outsider	6 500	Name, address, email address

<sup>96</sup> Breach Level Index, Data Breach Statistics, <http://www.breachlevelindex.com/#!breach-database>, 2016



# FUTURE THREATS AND DEVELOPMENTS

If current trends continue, it is obvious that DDoS attacks will continue to grow in scale, with the current top-end attacks becoming the norm as attacks reach new heights in terms of bandwidth and volume. While security providers must continue to match the scale of these attacks with mitigation solutions, the primary response for law enforcement remains unchanged – the arrest of perpetrators. Such a response does however require the timely involvement and competent action of the appropriate authorities.

The growing Internet of Things will expand the range of (often insecure) internet connected devices potentially capable of participating in DDoS attacks<sup>97</sup>. Coupled with IPv6, providing unlimited unique IP addresses and likely a host of undiscovered vulnerabilities, it is fertile ground for botnets<sup>98</sup>.

Data will always be a key commodity for cybercriminals but the ways that cybercriminals use or interact with it will continue to evolve as different data types are targeted for new purposes. Data is no longer just stolen for immediate financial gain, but can be used for the furtherance of more complex fraud, encrypted for ransom, or used to disrupt rivals or directly for extortion. Alternatively, when considering the illegal acquisition of intellectual property it can represent the loss of years of research and huge investment by the victim. It can be expected that while the compromise of financial data will continue, other sensitive data sources will increasingly be targeted such as the healthcare sector.

In areas where data plays a key role, such as the pharmaceutical sector which has sometimes decade-long research, testing and approval cycles to develop drugs that support precision personalised medicine, targeted attacks to exfiltrate such data sets are likely to increase.



# RECOMMENDATIONS

- Following any attack it is essential that law enforcement become involved as early as possible.
  - Law enforcement must therefore continue to build relationships with industry in order to encourage rapid engagement and reporting of the incident to law enforcement.
- It is encouraging to note that law enforcement are discovering an increasing number of external breaches<sup>99</sup>, often as a result of botnet takedowns and subsequent notifications to owners of infected systems.
  - Law enforcement must therefore continue to cooperate with private industry and other law enforcement partners to conduct large-scale operations both to disrupt cybercrime and to reassure the public and business that law enforcement are actively seeking to protect them.
- Law enforcement must continue to develop and invest in the appropriate specialised training required to effectively investigate highly technical cyber-attacks.
- When investigating attacks, law enforcement must take into account the increasing use of diversionary attacks to obfuscate more damaging underlying attacks, and keep this under consideration when investigating what they initially believe to be the primary crime.
- Booter/stresser tools are responsible for a growing proportion of DDoS attacks. A concerted and coordinated effort is required by law enforcement to tackle this threat.
- Security-by-design and privacy-by-design should be the guiding principles for industry. This includes the need to only collect the minimum amount of data necessary, automatically protect personal data by using proactive security measures such as end-to-end encryption and means to make individuals less identifiable, to mention some.
- In the context of the NIS directive, law enforcement should be fully engaged to avoid potential white spots in its view of the threat landscape and to help promote the engagement of victims of data breaches with law enforcement.

<sup>97</sup> Arbor Networks, The Lizard Brain of Lizardstresser, <https://www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser/>, 2016

<sup>98</sup> Dark Reading, IPv6 and the Growing DDoS Danger, <http://www.darkreading.com/attacks-breaches/ipv6-and-the-growing-ddos-danger/a/d-id/1322942>, 2016

<sup>99</sup> Verizon, 2016 Data Breach Investigation Report, <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>, 2016

# ATTACKS ON CRITICAL INFRASTRUCTURE



Critical infrastructure sectors are considered vital to the functioning of modern societies and economies to the point that their incapacitation or destruction would have a debilitating and cascading effect; yet these systems are vulnerable to damage as a result of natural disaster, physical incidents or cyber-attacks. Vulnerabilities continued to plague industrial control systems (ICS) and supervisory control and data acquisition systems (SCADA) in 2015, impacting on critical infrastructure organisations managing complex IT and physical networks<sup>100</sup>.

Malicious code can potentially be used to manipulate the controls of power grids, financial services, energy providers, defence, healthcare databases and other critical infrastructure, resulting in real-world catastrophic physical damage, such as blackouts or disruptions to an entire city's water supply<sup>101,102</sup>.

In most of the reported or analysed attacks targeting ICS, the initial infection began with targeted spear phishing and a malware drop to attack the network. In such a scenario, ICS-focused protection alone proved unable to prevent cyber-attacks. Relying only on detection is not enough - the key to success in securing ICS is prevention. However, there is a need to strike a balance between adding sensors to the network and the risk to be overwhelmed with alarms, alerts and indicators<sup>103</sup>.

With securing critical infrastructure becoming a priority, a ho-

listic approach is required where vulnerabilities and threats to the physical security and the security of ICT must be managed and controlled in the context of a comprehensive risk management framework, considering all interconnections and dependencies, and taking into account a total stakeholder view.

## KEY THREAT - ATTACKS ON THE INFRASTRUCTURE GRID

Cyber threats to critical infrastructure are a serious threat, due to their network device and service exposure to the internet and their reliance on networked services with limited preoccupation towards the security and monitoring of the exposed devices and services. Attackers can gain knowledge of how a specific control system works, and can respond by releasing ICS-specific attack vectors that could spread from the IT network to the ICS or SCADA, exploiting vulnerabilities or stressing control gauges until systemic failure ensues with a cascading effect and serious consequences<sup>104</sup>.

In 2015, law enforcement across Europe reported a number of attacks on critical infrastructures which often included unsophisticated methods such as SQL injections and cross site scripting but also APT-type attacks.

<sup>100</sup> EC3 Cyber Bit, Series: Trend 19/2016

<sup>101</sup> Kaspersky, BlackEnergy APT Attacks in Ukraine, <http://www.kaspersky.com/internet-security-center/threats/blackenergy>, 2016

<sup>102</sup> McAfee Labs Blog, A Case of Mistaken Identity? The Role of BlackEnergy in Ukrainian Power Grid Disruption, [https://blogs.mcafee.com/mcafee-labs/blackenergy\\_ukrainian\\_power\\_grid/](https://blogs.mcafee.com/mcafee-labs/blackenergy_ukrainian_power_grid/), 2016

<sup>103</sup> BlackHat, PLC-Blaster: A Worm Living Solely in the PLC,

<https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf>, 2016

<sup>104</sup> Verizon, Data Breach Digest, [http://www.verizonenterprise.com/resources/reports/rp\\_data-breach-digest\\_xg\\_en.pdf](http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf), 2016

*Black Energy, a Trojan used in the past to conduct DDoS attacks, cyber espionage and information destruction, was used to carry out an attack on the Ukrainian power grid in December 2015. The malware had been modified specifically to carry SCADA-related plugins, in this case a module named Killdisk, in order to attack ICS<sup>105</sup>. Spear phishing was used to target individuals within the organisation with messages containing Microsoft Office documents; these documents contained malicious macros that once clicked, installed the malware onto the system<sup>106</sup>.*

Due to the destructive payload, campaigns such as Black Energy pose an additional threat to companies beyond the critical infrastructure sector. These companies may have a false sense of security due to the fact that they are not critical or public-facing or too important enough to be targeted, but due to the spreading of this kind of malware they might well fall victim, with greater impact due to their relative unpreparedness<sup>107</sup>.

## KEY THREAT - EVERYDAY MALWARE AND ZERO-DAYS

After incidents such as Stuxnet it is not surprising that critical infrastructure facilities can be infected with viruses, which are generally harmless unless the infrastructure is the specific target. In 2015, law enforcement across Europe reported a number of malware infections within air-gapped<sup>108</sup> control system networks, combined with the exploitation of zero-day or unpatched vulnerabilities in control system devices and software.

However, it is often clear that there is no need to develop or purchase customised hacking tools, as there is a wealth of existing malware and vulnerabilities that can be exploited with minor tweaking to take advantage of the lack of security-by-design that is often found in ICS and SCADA systems<sup>109,110</sup>.

*In April 2015, a German nuclear plant was infected with malware, including Conficker and Ramnit, which can allow remote access to an infected system and are capable of spreading through USB drives. In this case no harm was done; the malware required internet access to contact a command-and-control network - which it did not have - and the infection appeared to be incidental, i.e. the plant was not specifically targeted<sup>111</sup>.*

Despite the fact that new vulnerabilities are discovered every day, when it comes to critical infrastructure relatively few dis-

closures can be seen<sup>112</sup>. At the same time, this underreporting of incidents and vulnerabilities increases the risk for such systems, given the wide-spread use of the same software/hardware in the industry. Another important threat is posed by insiders, as they have intimate knowledge of how such systems work<sup>113</sup>. If researchers report the discovery of vulnerabilities back to manufacturers and asset owners, then the whole industry benefits from an increase in security<sup>114</sup>. With these types of attack, it may be that an adequate response needs to be modelled on the joint approach by executive branches of government, with a focus on the interests at stake. This means that the inclusion of law enforcement and judiciary authorities in crisis-management plans and exercises is becoming more relevant.

## KEY THREAT - SPEAR PHISHING, WATERING HOLE ATTACKS AND SOCIAL ENGINEERING

As with other network attacks, spear phishing is a common ICS attack vector, providing targeted entry into an organisation's system. The use of the supply-chain as an attack vector is increasing, where the attackers target third-party vendors or partners, targeting the weakest link, and moving laterally to the actual target<sup>115,116</sup>.

*In late 2014, hackers attacked a German steel mill in one of the first confirmed cases in which a wholly digital attack caused physical destruction of equipment. The attackers gained access via spear phishing and social engineering to obtain the credentials required to access the mill's network<sup>117</sup>.*

## ■ KEY THREAT - INSIDERS

Insiders pose a huge potential risk to critical infrastructure, as insiders have intimate knowledge of the details of ICS and SCADA. While malicious actions of insiders are one potential threat, involuntary disclosure of sensitive information during phishing attempts, due to lack of training, can have devastating consequences. People, technology, processes and training should be combined to tackle this threat<sup>118,119</sup>. Monitoring access rights is essential when managing the risk associated with

<sup>105</sup> Kaspersky, BlackEnergy APT Attacks in Ukraine, <http://www.kaspersky.com/internet-security-center/threats/blackenergy>, 2016

<sup>106</sup> EC3 Cyber Bit, Series: Trend 1/2016

<sup>107</sup> Trend Micro, KillDisk and BlackEnergy are not just Energy Sector Threats, <http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/>, 2016

<sup>108</sup> An air-gap refers to computers and networks not connected directly to the internet, or to any other computers or networks that are connected to the internet.

<sup>109</sup> Kaspersky, Low-tech Attackers Harness Open Source Security Tools for Targeted Cyberespionage, <http://www.kaspersky.com/about/news/virus/2016/Low-tech-attackers-harness-open-source-security-tools-for-targeted-cyberespionage>, 2016

<sup>110</sup> The Hague Security Delta, Securing Critical Infrastructures in the Netherlands, [https://www.thehaguesecuritydelta.com/media/com\\_hsd/report/53/document/Securing-Critical-Infrastructures-in-the-Netherlands.pdf](https://www.thehaguesecuritydelta.com/media/com_hsd/report/53/document/Securing-Critical-Infrastructures-in-the-Netherlands.pdf), 2015

<sup>111</sup> Trend Micro, Malware Discovered in German Nuclear Power Plant, <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant>, 2016

<sup>112</sup> Fortinet, (Known) SCADA Attacks Over The Years, <https://blog.fortinet.com/2015/02/12/known-scada-attacks-over-the-years>, 2015

<sup>113</sup> NIST Computer Security Resource Center, Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia, [http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study\\_report.pdf](http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf), 2008

<sup>114</sup> ENCS, Do We Need More Vulnerability Disclosures in Critical Infrastructure? <https://www.encls.eu/2016/06/16/do-we-need-more-vulnerability-disclosures-in-critical-infrastructure/>, 2016

<sup>115</sup> Check Point, Everyday Malware Poses a Risk to Critical Infrastructure, <http://blog.checkpoint.com/2016/05/19/everyday-malware-poses-a-risk-to-critical-infrastructure/>, 2016

<sup>116</sup> Radiflow, Ukraine Cyber Attack Analysis, [http://radiflow.com/wp-content/uploads/2015/12/Ukraine\\_cyber\\_attack\\_report.pdf](http://radiflow.com/wp-content/uploads/2015/12/Ukraine_cyber_attack_report.pdf), 2016

<sup>117</sup> SANS Industrial Control Systems, German Steel Mill Cyber Attack, [https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks\\_Facility.pdf](https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf), 2014

<sup>118</sup> SANS Institute, Mitigating Insider Sabotage, <https://www.sans.org/reading-room/whitepapers/casestudies/mitigating-insider-sabotage-33189>, 2009

<sup>119</sup> SANS Institute, Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey, <https://www.sans.org/reading-room/whitepapers/analyst/incident-response-capabilities-2016-2016-incident-response-survey-37047>, 2016

<sup>118</sup> SANS Institute, Mitigating Insider Sabotage, <https://www.sans.org/reading-room/whitepapers/casestudies/mitigating-insider-sabotage-33189>, 2009

<sup>119</sup> SANS Institute, Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey, <https://www.sans.org/reading-room/whitepapers/analyst/incident-response-capabilities-2016-2016-incident-response-survey-37047>, 2016



potential insider threats<sup>120,121</sup>.

## FUTURE THREATS AND DEVELOPMENTS

As most critical infrastructure (CI) was not designed with cyber security in mind, there is a need to rethink security, incorporating security-by-design into hardware and software components. As the software and hardware components of CI tend to be in use for often many years, there is also a need for improved vulnerability and patch management based on a holistic assessment and evaluation of assets, threats and risks<sup>122</sup>.

Because of the increased availability of tools and the wide attack surface presented by CI, we can expect attacks to increase in quantity. Serious damage could potentially be caused by those attackers deploying blended attacks incorporating phishing techniques and malware – including the growing threat of ransomware<sup>123</sup>.

Cyber insurance plans, targeting the critical infrastructure sector, will be on the rise and will steadily increase to cover a variety of costs related to cyber-attacks such as revenue lost due to downtime, notifying customers impacted by a data breach, and providing identity theft protection<sup>124</sup>. The likely impact of insurance measures is unclear; whether it will result in a positive scenario where such insurances require due diligence and minimum security standards, or where this new landscape will lead to risk transferring strategies. Making use of a cyber-insurance should not result in ignoring IT security<sup>125</sup>, however, the insurance industry could be an important player in setting the baseline for adequate levels of security.

The transposition into national legislations of the NIS Directive will positively impact the whole cyber security ecosystem, mandating reporting and improving the sharing of vulnerabilities in this sector. However, the lack of law enforcement involvement in the mechanism, which is only foreseen in a voluntary or ad hoc form, might make it difficult for attacks on critical infrastructure to result in the investigation and prosecution of the responsible actors<sup>126</sup>. This may be further complicated by the fact that the focus of operators of critical infrastructure will be on business continuity, which may be at odds with law enforcement's investigative requirements.

There is a balance to be struck between the requirements of such operators and law enforcement in terms of improved exchange of information and the development of better joint work practices with a view to increasing the understanding on both sides.

It is not only critical infrastructures that are increasingly vulnerable; there is also a risk of attackers gaining entry to the systems where they can illegally acquire sensitive information. Illegal access to intellectual property (IP) is an added risk to consider when designing cyber defences for critical infrastructures. Specific threat groups, such as the Sofacy group (APT28), actively target European institutions and, in addition to acquiring sensitive data, engage in cyber-operations to manipulate the media and public opinion<sup>127</sup>. Widespread attacks have been observed from a multitude of sources targeting the EU institutions throughout 2016<sup>128</sup>. However, in this area there is little or no crime reporting, generating a negative spiral where there is no reporting, so law enforcement cannot respond and because law enforcement are not seen to respond, such activities go unreported to law enforcement.

## RECOMMENDATIONS

- Law enforcement and judicial authorities must be engaged early following serious cyber security incidents. Working collectively is our best route to getting ahead of attackers. Moreover, information security needs to be one of the first lines of defence against insider threats.
  - Building trusted relationships is a major consideration in encouraging organisations to report incidents and share information. More interactions between law enforcement, the critical infrastructure sector and CSIRT community are needed to build that trust<sup>129</sup>.
- While securing critical infrastructures remains a private sector responsibility, attention should be given, by regulators, to the compliance of IT systems and mandatory security-by-design.
  - There needs to be a baseline of security standards for those operating systems that manage critical industrial systems, transportation, power grids or air traffic<sup>130</sup>.
  - There is need for provisions aimed at protecting critical infrastructures<sup>131</sup> and securing network and information systems<sup>132</sup> in order to align cyber security capabilities in all the EU Member States and ensure efficient exchange of information and cooperation.
- Reputational and financial damage is an obvious barrier to sharing and reporting. Nevertheless, in those cases where authorities have to report incidents to the national CSIRT, agreements should be undertaken to make sure that law enforcement is able to follow up with criminal investigations when needed<sup>133</sup>.
- Operators of critical infrastructure and law enforcement should work together towards an improved exchange of information and the development of better joint work practices.

<sup>118</sup> SANS Institute, Mitigating Insider Sabotage, <https://www.sans.org/reading-room/whitepapers/casestudies/mitigating-insider-sabotage-33189>, 2009

<sup>119</sup> SANS Institute, Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey, <https://www.sans.org/reading-room/whitepapers/analyst/incident-response-capabilities-2016-2016-incident-response-survey-37047>, 2016

<sup>120</sup> IBM 2015 Cyber Security Intelligence Index, <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEW03073USEN>, 2015

<sup>121</sup> ICS-CERT, Cyber-Attack Against Ukrainian Critical Infrastructure, <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>, 2016

<sup>122</sup> European Commission, Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, <https://ec.europa.eu/digital-single-market/en/news/communication-strengthening-europes-cyber-resilience-system-and-fostering-competitive-and>, 2016

<sup>123</sup> Fortinet, SCADA Security Report 2016, <https://blog.fortinet.com/2016/04/05/scada-security-report-2016>, 2016

<sup>124</sup> SANS Institute, Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey, <https://www.sans.org/reading-room/whitepapers/analyst/bridging-insurance-infosec-gap-2016-cyber-insurance-survey-37062>, 2016

<sup>125</sup> Allianz, A Guide to Cyber Risk, [https://www.allianz.com/v\\_1441789023000/media/press/document/other/Allianz\\_Global\\_Corporate\\_Specialty\\_Cyber\\_Guide\\_final.pdf](https://www.allianz.com/v_1441789023000/media/press/document/other/Allianz_Global_Corporate_Specialty_Cyber_Guide_final.pdf), 2015

<sup>126</sup> European Commission, The Directive on Security of Network and Information Systems (NIS Directive), <https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive>, 2015

<sup>127</sup> CERT-EU, <https://cert.europa.eu>, 2016

<sup>128</sup> CERT-EU, <https://cert.europa.eu>, 2016

<sup>129</sup> EU Member State, Law enforcement recommendation, 2016

<sup>130</sup> Enterprise Forward, IT Spend Slowdown Puts the Squeeze on Innovation, <http://hpe-enterpriseforward.com/spend-slowdown-puts-squeeze-innovation/>, 2016

<sup>131</sup> European Commission, Communication from the Commission on a European Programme for Critical Infrastructure Protection, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN>, 2006

<sup>132</sup> European Commission, The Directive on Security of Network and Information Systems (NIS Directive), <https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive>, 2015

<sup>133</sup> EU Member State, Law enforcement recommendation, 2016

# ■ CRIMINAL FINANCES ONLINE



Like any economy, the digital underground relies on the possibility to transfer funds in exchange for goods or services. These can involve paying for those tools needed to commit the crime, or those that enable the distribution and storage of the proceeds of crime. Which of the diverse selection of available payment mechanisms is used for any particular transaction depends on a range of factors. Are they operating in an environment where a particular payment mechanism is preferred or enforced? Is the payee or payer likely to have a corresponding account? How anonymous do they require it to be? There are many such questions, the answers to which will be partly decided by the nature of the transaction.

## CRIMINAL TO CRIMINAL (C2C) PAYMENTS

When making payments to other cybercriminals, for example to pay for a criminal service or commodity, payments need to be secure and as anonymous as possible. In some online environments that payment mechanism is largely dictated to them. Darknet markets for example almost exclusively use Bitcoin, with the payment mechanism incorporated into the market structure. Where cybercriminals have greater freedom to choose, despite the huge array of options available to them, the selection used is actually somewhat constrained and in many cases fairly unsophisticated.

Many payments still occur within the realm of the regulated financial sector. The use of simple wire transfers is common. It is likely that this reflects the use of either compromised accounts or money mules. Credit cards and pre-paid cards are also commonly used, although again it is likely that this refers to compromised or stolen cards. The abuse of money transfer

services such as Western Union or MoneyGram also account for a substantial proportion of 'real world' C2C payments.

Much transactional activity between cybercriminals remains entirely within the digital realm however. Here the most commonly used single currency for C2C transactions is Bitcoin. Perhaps evolving from its popularity on the Darknet, Bitcoin has become the currency of choice for much of cybercrime. A primary concern for criminal users of Bitcoin has been the transparency of the blockchain, however the increasing availability of Bitcoin mixing services – which pool and redistribute multiple transactions to confuse transaction trails - has given them increased confidence by understanding the additional layers of anonymity. While the cryptocurrency landscape is constantly evolving, and there are a growing number of alternate currencies which offer more anonymity, none have yet attained the level of popularity or attention of Bitcoin.

The abuse of centralised digital currencies such as WebMoney is still reported, although in a much smaller number of cases. While such payment systems were historically believed to be a preferred mechanism, this is certainly no longer the case as more and more cybercriminals migrate to Bitcoin. Like any currency, criminals can be expected to migrate to whatever others are using.

## VICTIM TO CRIMINAL (V2C) PAYMENTS

Where victims are voluntarily (even if reluctantly) making payments to criminals, either as a result of extortion or fraud, the payment system requirements differ only slightly. Here anonymity only needs to be uni-directional, and simplicity and

accessibility are key, in order to maximise the victims' likelihood of paying. Still, it is commonplace for criminals to have to provide detailed instructions on how to obtain the necessary currencies.

Fraud relies on a semblance of normality and legitimacy, therefore the use of conventional payment mechanisms is more likely. The more unusual a payment system is, the more likely a scam would be to arouse suspicion. Consequently, wire transfers are common, as is the use of money transfer services.

Conversely, in cases of extortion there is no need for pretence, and criminals again resort to payment mechanisms which maximise their own security. Pre-paid voucher-based systems such as paysafecard are still popular. However Bitcoin is again the preferred option, and the primary payment mechanism for most current ransomware as well as other extortion schemes. The prominent DDoS groups of the past years likewise demanded payment in Bitcoins.

## MONEY LAUNDERING – MONEY MULES

Even when using centralised and ostensibly traceable payment systems, such as paysafecard, the service-based digital underground provides a range of opportunities to safely cash out, convert or otherwise clean (launder) criminal proceeds. There is no shortage of individuals offering these services for a suitable commission. While criminals can, in relative safety, transfer and circulate funds within the digital economy, there comes a time when it is necessary to monetise these funds so that the criminal can make use of them in the real world. In some cases, particularly when the funds sit with a compromised card or account tied to an entity within the regulated financial sector, specialised services are required – money mules.

Money mules are individuals recruited, often by criminal organisations, to receive and transfer illegally obtained money between bank accounts and/or countries. The recruited individuals may be willing participants, however some may, initially at least, be unaware that they are engaging in criminal activity and believe they are performing a legitimate service.

The investigation of money mule networks is a top priority for both law enforcement and the financial sector.

*In February 2016, law enforcement agencies and judicial bodies primarily from Belgium, Denmark, Greece, the Netherlands, the United Kingdom, Romania, Spain and Portugal joined forces in the first European Money Mule Action (EMMA). The operation was also supported by Europol, Eurojust and the European Banking Federation (EBF). Over one week nearly 700 money mules were identified across Europe and 81 individuals were arrested after 198 suspects were interviewed by law enforcement agencies. With the support of over 70 banks, significant financial losses were discovered and prevented, and over 900 victims of this crime were identified. More than 90% of the reported money mule transactions were linked to cybercrime. The following week was devoted to raising awareness of this threat and to attempt*

*to dissuade people from getting involved in this type of crime.*

## ■ PACKET MULES

Rather than receiving and retransmitting stolen funds some mule services instead receive goods fraudulently ordered online using compromised credit cards, and then forward these onto their customers. This service is also referred to as providing “drops” or as “reshipping”. The mule effectively takes on the risk of being in receipt of the goods instead of those committing the fraud. A new trend in this area is the use of automated packet stations. Only available in some countries, these are stations consisting of a number of mailboxes. The stations are un-manned and require a registered user to login and open their box via a terminal. While they have a number of security features to minimise such abuse, these stations can be used in place of, or by, packet mules to reduce the risk of directly receiving fraudulently obtained goods.

## FUTURE THREATS AND DEVELOPMENTS

Virtual currencies continue to gain wider acceptance as the community grows and matures. With it comes the development of new currencies, building on the foundations of Bitcoin. Many of these new currencies focus on innovation and utility, making them more accessible or useful for business, but even these show potential for criminal use.

Officially launched in July 2015, Ethereum has taken the #2 spot in the virtual currency market<sup>134</sup>. Amongst its other innovations, Ethereum focuses on the use of smart contracts – contracts able to self-verify their own conditions using both blockchain as well as external data, and self-execute by releasing payment, while remaining tamper resistant<sup>135</sup>. While smart contracts naturally have a wide range of legitimate and positive uses, they also reinforce the crime-as-a-service model of the digital underground. Assuming the contract creator had the skill to create a contract able to detect the fulfilment conditions, any criminal service from website defacement to illicit data exfiltration could be dealt with via smart contracts. Such uses have already been demonstrated to be quite possible<sup>136</sup>. This is of course an issue of smart contracts themselves, rather than any particular currency. If smart contracts do indeed become a tool for the cyber underground, we can no doubt expect to see the appearance of criminal cyber-notaries, drawing up smart contracts for criminal customers as a service.

While many new cryptocurrencies are clearly focussing on benefits to enterprise and business, some continue to focus on issues of privacy and anonymity. Bitcoin is only pseudonymous, meaning that there is some potentially traceable data (namely a Bitcoin address) that could be used to link a transaction to an individual. Additionally, the blockchain itself is relatively transparent. There are currencies in development that seek to redress this issue. The philosophy behind many of these projects is the protection of the privacy of those who perhaps need it most, such as activists or those outspoken against oppressive regimes. However, it is not hard to imagine who would be the

<sup>134</sup> Coinmarketcap, <http://coinmarketcap.com/>, 2016

<sup>135</sup> SmartContract, <http://about.smartcontract.com/>, 2016

<sup>136</sup> Juels, Kosba, Shi, The Ring of Gyges: Investigating the Future of Criminal Smart Contracts, <http://www.in3.org/files/Gyges.pdf>, 2016.



primary benefactors of a currency which was entirely anonymous and resistant to law enforcement surveillance<sup>137</sup>.

In 2014 we reported that some small online criminal communities had developed their own in-house currencies<sup>138</sup>. We have not seen an expansion of this phenomenon, perhaps due to the availability of alternate currencies. The majority of law enforcement currently has its attention focused on Bitcoin, a fact which is not lost on the criminal community. It is therefore logical to assume that some smaller criminal communities may be abusing lesser-known cryptocurrencies in order to stay under the radar.

Blockchain technology also attracts considerable interest from industry and academia. It has potential applications for many transactional activities such as voting, identity management, digital assets and stocks, smart contracts, file storage and record keeping, to name just a few<sup>139,140</sup>. While there have been previous indications that the blockchain itself could be abused for criminal purpose, such as for storing child abuse images, or malware code<sup>141</sup>, there is little evidence of this currently happening. However, a new variant of the CTB-Locker malware does use the blockchain to deliver decryption keys<sup>142</sup>. As entrepreneurial cybercriminals become more familiar with blockchain technology and its potential, it can be expected that we will see more creative use of its capabilities.

Many in the Bitcoin community consider exchanges as a single point of failure, and the need for a decentralised solution has been a topic within the Bitcoin community for years<sup>143</sup>. Such platforms would be unlikely to implement any KYC<sup>144</sup> measures and would therefore provide users with an additional level of security and anonymity.

In 2016, a functional beta version of Bitsquare<sup>145</sup> was released. This is the first decentralised exchange that brings together buyers and sellers of dozens of virtual currencies. It uses a P2P network built on top of Tor, where every user is given a dedicated .onion address. Payment methods used on the platform include Single Euro Payments Area (SEPA)<sup>146</sup> transfers but the data is only shared with the trading counterparty. The current implementation suffers from liquidity issues, and the amount of daily trade is limited to several thousands of euros, nevertheless its popularity is on the increase.

Internet crowdfunding campaigns are an increasingly popular method of raising funds for the development of new products or technologies. Criminals have also taken advantage of this trend, using them not only as a means of laundering criminal funds by investing them in the project, but additionally subsequently defrauding investors who believe they are funding a

legitimate project<sup>147</sup>.

## RECOMMENDATIONS

- As the criminal use of virtual currencies continues to gain momentum, it is increasingly important for law enforcement to:
  - Build and maintain relationships with the virtual currency community, in particular virtual currency exchangers;
  - Ensure that cybercrime and financial investigators have adequate training in the tracing, seizure and investigation of virtual currencies.
- While Bitcoin is clearly the current currency of choice, regular horizon scanning exercises should be carried out to assess which alternate currencies are either also being abused, or are likely to be abused in the future.
- Law enforcement should continue to invest into and develop new investigative tools and tactics, together with key partners from other sectors, to facilitate investigations involving cryptocurrencies and the blockchain.
- Following the success of the EMMA initiatives in 2015 and 2016, more European countries should endeavour to contribute and engage in the operational and prevention activity. This will result in a greater and more widespread impact on this key area of criminality.
- Law enforcement should make themselves aware of any packet station services operating in their jurisdictions in order to build working relationships with them to mitigate the abuse of these services.

<sup>137</sup> Wired, Zcash, an Untraceable Bitcoin Alternative, Launches in Alpha, <https://www.wired.com/2016/01/zcash-an-untraceable-bitcoin-alternative-launches-in-alpha/>, 2016

<sup>138</sup> RSA, Mo Money Mo Problems, <https://blogs.rsa.com/mo-money-mo-problems/>, 2014

<sup>139</sup> WeUseCoins, Potential Uses of Blockchain Technology, <https://www.weusecoins.com/blockchain-uses/>, 2016

<sup>140</sup> Quora, What Other Uses are there for the Bitcoin Blockchain?, <https://www.quora.com/What-are-the-most-interesting-uses-of-blockchains-other-than-cryptocurrencies>, 2016

<sup>141</sup> Interpol, Interpol Cyber Research Identifies Malware Threat to Virtual Currencies, <http://www.interpol.int/News-and-media/News/2015/N2015-033>, 2015

<sup>142</sup> Sucuri Blog, Website Ransomware – CTB-Locker Goes Blockchain, <https://blog.sucuri.net/2016/04/website-ransomware-ctb-locker-goes-blockchain.html>, 2016

<sup>143</sup> Reddit, Bitcoin Needs a Decentralized P2P “Exchange”, [https://www.reddit.com/r/Bitcoin/comments/1obhra/bitcoin\\_needs\\_a\\_decentralized\\_p2p\\_exchange/](https://www.reddit.com/r/Bitcoin/comments/1obhra/bitcoin_needs_a_decentralized_p2p_exchange/), 2013

<sup>144</sup> Know Your Customer

<sup>145</sup> Bitsquare, The Decentralized Bitcoin Exchange, <https://bitsquare.io>, 2016

<sup>146</sup> European Commission, Single Euro Payment Area (SEPA), [http://ec.europa.eu/finance/payments/sepa/index\\_en.htm](http://ec.europa.eu/finance/payments/sepa/index_en.htm), 2016

<sup>147</sup> Flashpoint, Highlights & Trends in the Deep & Dark Web, [https://www.flashpoint-intel.com/home/assets/Media/Flashpoint\\_2015\\_Highlights\\_and\\_Trends.pdf](https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_2015_Highlights_and_Trends.pdf), 2016

# ■ CRIMINAL COMMUNICATIONS ONLINE

When it comes to online communication, cybercriminals are no different to any other internet users. They use the internet to contact each other, to carry out business and to socialise, often using everyday applications; they protect their data and their identities with the same means available to any private citizen. In this chapter we discuss the trends, tools and methods currently favoured by cybercriminals.

## CRIMINAL TO CRIMINAL (C2C) COMMUNICATIONS

Criminal forums within the deep web or Darknet remain a crucial environment for cybercriminals to communicate. They are a key component of the crime-as-a-service business model which underpins much of cybercrime, providing cybercriminals, entry-level and upwards, with access to the tools and services they need, and providing an environment where they can teach, learn, buy and sell, advertise and do business. Following the law enforcement take-down of the Darkode forum in July 2015<sup>148</sup> - the most prolific English speaking criminal forum at the time - there do not appear to be any notable replacements.

Other web-based communication platforms such as chatrooms or open forums are still commonly used for C2C communications, as is 'simple' email. Secure, encrypted email is readily available. Some states still report the use of draft emails to communicate from accounts with shared access.

While forums may be suitable for initial contact, most subsequent communications continue using alternate, less public means. Here Jabber is a commonly used tool, and believed to be the preferred means of communication for the more technically competent cybercriminals. To a slightly lesser extent, IRC and ICQ are also used, whereas commercial 'branded' products are largely absent. More exotic means of communication such as the use of gaming consoles or even RATs are rare.

Essentially, cybercriminals will use whatever communication method they deem to be the most convenient and/or that which they perceive to be sufficiently secure.

## CRIMINAL TO VICTIM (C2V) COMMUNICATIONS

Whereas a key requirement for C2C communication channels is security, the primary requirement for C2V communications is accessibility. This means the ability to contact potential victims en masse or to select a communication means readily available to a targeted victim.

Email remains the simplest and most convenient method for both approaches. Many phishing and malware (e.g. Dridex) campaigns are distributed via email spam in order to maximise their impact based on limited success rates. Similarly, emails can be handcrafted in order to maximise their effectiveness on specific victims targeted for social engineering.



<sup>148</sup> Europol Press Release, Cybercriminal Darkode Forum Taken Down Through Global Action, <https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action>, 2015

Beyond email, a wide range of popular, publically available tools are used for C2V communications; tools such as Skype, (Facebook) Messenger, WhatsApp and Viber. All are easy to obtain and access by victims yet offer attackers a degree of security and anonymity. An already used means of communication may of course be the means of attack, if an attacker has carried out the appropriate research.

## ANONYMISATION TOOLS

The majority of reporting countries indicated that cybercriminals under investigation are using some form of IP anonymisation. The use of simple proxies was the most common tool, closely followed by the use of Tor and Virtual Private Networks (VPNs). The use of I2P has increased on previous years but is still only encountered in a low number of cases. Tor usage was reportedly more common in cyber-enabled crime rather than cyber-dependent crime which more often made use of either commercial or criminal (as-a-service) VPNs. It is likely that access to those VPNs, run by the more sophisticated criminal groups, is strictly controlled.

## THE USE OF ENCRYPTION

While the use of encryption is highly useful to private citizens and industry in protecting their data, thereby denying it to criminals who desire it for criminal purposes, the use of encryption by criminals to similarly protect their data presents significant challenges for law enforcement across all areas of cybercrime and cyber-facilitated crime.

Twenty European countries, including 13 EU Member States, report the use of encrypting software (such as Truecrypt, Bitlocker, etc) by cybercriminals to protect their stored data. Moreover, the phenomenon is no longer restricted to desktop computers as increasingly third party or native encryption is available on mobile devices. The use of encryption deprives law enforcement of crucial evidential opportunities. Eight Member States specifically state that dealing with encryption is a major challenge to investigating cybercrime.

Additionally, almost half of Member States indicate that their investigations involve the use of some form of encrypted communications, typically Jabber, but also commercial applications such as WhatsApp and Viber. Many commercially available communication platforms now have encryption activated by default. This is increasingly done by way of end-to-end encryption (service level encryption, instead of a network layer encryption such as https), leading to situations where services are not interceptible.

## FUTURE THREATS AND DEVELOPMENTS

In terms of the tools and applications used by criminals to share, send, and store their data and communications, little has changed in the past year. Criminals continue to use whichever tools or applications they are familiar and comfortable with or which fit their intended purpose. What has changed is the growing movement and involvement of public and private

bodies in debating the issue of encryption, and the desire for privacy and security versus the need for law enforcement to effectively investigate crime. While 2015/2016 has seen much discussion on the matter, no definitive answers have been proposed by either side, as indeed there is no simple solution at present.

There is a growing market for communication apps offering additional security features such as end-to-end encryption, and the possibility to permanently delete messages and traces. It is likely that these will be increasingly adopted by criminals (cyber- or otherwise) or that existing, commonly used applications will evolve to encompass these features. Some cybercriminals are counter-surveillance aware, using apps and other software to erase or detect the interception of their communications.

There are currently ongoing discussions on whether or not the courts can/should compel suspected offenders to disclose their encryption keys. This discussion varies from jurisdiction to jurisdiction but some countries have already integrated this policy in their legal systems (e.g. UK). Many topics have emerged<sup>149</sup> from the discussion including the right of non-self-incrimination.

## RECOMMENDATIONS

- To counter the criminal use of encryption, law enforcement must ensure it has the training, tools and tactics it requires to obtain and handle digital evidence in situ using techniques such as live data forensics.
- Law enforcement should continue to monitor trends in the use of applications and software by cybercriminals and maintain awareness of the different investigative opportunities and challenges that each provides.
- It is essential for law enforcement to build and maintain relationships with academia and private industry as they may be able to assist or advise law enforcement where it lacks the technical capability to progress an investigation.

<sup>149</sup> CNET, DoJ: We Can Force You to Decrypt That Laptop, <http://www.cnet.com/news/doj-we-can-force-you-to-decrypt-that-laptop/>, 2011



# DARKNETS AND HIDDEN SERVICES



This section looks at the criminal use of anonymising peer-to-peer networks such as Tor, I2P and Freenet. These networks are often referred to as ‘Darknets’. While these tools are designed and intended to protect users from traffic analysis, which “threatens personal freedom and privacy, confidential business activities and relationships, and state security”<sup>150</sup>, they are also used by criminals operating online to protect their own freedom - by frustrating law enforcement attempts to identify and arrest them. In addition to concealing the identity of criminals themselves, such tools can be used to hide the hosting location of criminal websites, forums and online markets, commonly referred to as “hidden services”.

2015 has been a tumultuous year for Darknet markets, with the underground economy plagued by major exit scams and market closures. We previously reported that in March 2015, the Evolution marketplace shut down, with its administrators allegedly stealing EUR 11 million of their customers’ Bitcoins<sup>151</sup>. At that time, Evolution’s departure left only a few large popular markets (along with many smaller ones), including the Agora and Nucleus markets. However, in August 2015, the administrators of Agora voluntarily took the marketplace down to allegedly address vulnerabilities in Tor which may have allowed their servers to be de-anonymised<sup>152</sup>. The Nucleus market closed its forums in September 2015 and sometime in early 2016 the market also appears to have shut down. Whether this is also an exit scam is not clear as customers’ funds still sit in the market’s wallet.

Three major Darknet markets all went offline within a 12 month period without any apparent law enforcement action, highlighting the inherent volatility of the Darknet market economy. While users of these sites can take any number of operational security measures to protect themselves from law enforcement investigation, there is nothing they can do to prevent these markets folding from within, which is an inherent risk in using these sites.

Disruption is a core tactic for law enforcement, therefore the self-disrupting effect of the market volatility is something of a boon to law enforcement. The impact of Operation Onymous<sup>153</sup> in 2014 was significant at the time but the remaining markets rallied back and new ones formed. Today, message board chat relating to these services is often seeded with paranoia, not that law enforcement has taken further action, but that a market has performed an exit scam with their funds or simply closed down. This is particularly so when these services are unavailable, often as a result of DDoS attacks (presumably from rivals), which is not uncommon.

Some research indicates that almost 30% of hidden services on Tor relate to some form of illicit activity<sup>154</sup>. The majority of law enforcement investigations on the Darknet focus on markets selling illicit drugs – or at least the vendors and buyers thereon. Those selling weapons, compromised data or other illicit products such as pharmaceuticals and chemicals are also key targets for law enforcement. One of the main

<sup>150</sup> Tor, <https://torproject.org/>

<sup>151</sup> 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

<sup>152</sup> DeepDotWeb, Agora Admin Explains: Why Is Agora Down?, <https://www.deepdotweb.com/2014/09/01/agora-admin-explains-why-is-agora-always-down/>, 2014

<sup>153</sup> DeepDotWeb, Global Action Against Dark Markets on Tor Network, <https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network>, 2014

<sup>154</sup> Daniel Moore, Thomas Rid, Cryptopolitik and the Darknet, 2016

challenges for law enforcement in this area - aside from the additional attribution issues - is the ability to operate lawfully in these environments, with one quarter of respondents clearly restricted by their national legislation.

It is true that there is some measure of cybercrime activity on hidden services on the Darknet, the majority of illicit activity on hidden services relates primarily to drugs and to a lesser extent other illicit commodities and is firmly cyber-facilitated. This highlights the increasing dependence of other crime areas on online services, and the subsequent need for all law enforcement to have the capability to investigate online.

However, law enforcement presence in an area that has no effective national boundaries causes issues with deconfliction. To effectively progress such investigations requires at least EU-level cooperation.

## FUTURE THREATS AND DEVELOPMENTS

In other areas of cybercrime, there is a continuous arms race between cybercriminals looking for vulnerabilities to exploit and security professionals looking to defend against them. Conversely, the opposite is largely true with regards to the use of Darknets and hidden services. Criminals shelter themselves behind imperfect anonymisation solutions while law enforcement and researchers seek to find ways to penetrate their shields of anonymity, while keeping protection intact for legitimate users. Of course, other developers are also looking for ways to plug the security holes to make the system safer for legitimate users.

We previously reported the possibility of a wholesale movement from Tor to other networks such as I2P, however this has not happened. There is still a clear preference for Tor, perhaps due to the simplicity of its use, or conversely the technical challenges of moving to I2P. We can however still expect to see the improvement of existing and the development of new networks as researchers and developers seek to overcome the flaws and limitations of existing networks whilst building on their strengths; networks such as *Riffle* which is under development by MIT<sup>155</sup>. *Riffle* incorporates Tor's onion encryption and 'shuffles' traffic to minimise the possibilities of traffic analysis. The project was created with anonymous file sharing in mind<sup>156</sup>, and to prevent snooping by "authoritarian" governments<sup>157</sup>. While initiatives such as this no doubt represent a fascinating area of academic study, one must question who the principal benefactors of this new technology will likely be, with so many obvious advantages to those operating against the good of society such as violent extremists and child sex offenders.

Hidden services may remain protected behind different anonymisation solutions but Operation Onymous highlighted that these networks are not impervious. While their locations may be hidden, they are still hosted somewhere which

often represents a single point of potential failure – not taking into account criminal business continuity plans. New projects such as OpenBazaar may overcome this weakness though. OpenBazaar is a decentralised marketplace accessed through a client. Customers can search for goods and purchase directly from a merchant using bitcoins. The system is entirely peer-to-peer with no centralised servers and uses multisignature (multisig) bitcoin addresses for security<sup>158</sup>. What the repercussions of the migration of existing Darknet drug and illicit commodities markets to this type of system would be for law enforcement investigations is not yet clear, however the first drugs listings appeared only hours after OpenBazaar's official launch<sup>159</sup>.

## RECOMMENDATIONS

- Given the significant challenges investigations on the Darknet present to law enforcement, this represents an area where effective deconfliction, collaboration and the sharing of intelligence sharing is essential. This will serve to prevent duplication of effort, facilitate the sharing of tactics and tools and improve our understanding of the scope of the threat.
- Darknets are an environment where cyber-facilitated crime is becoming firmly established. It is not feasible or practical that all such crime is dealt with by cybercrime units when the predicate crime is related to drugs, firearms or some other illicit commodity. It is essential therefore that appropriate training and tool support is extended to those working in these areas to provide them with the required knowledge and expertise.
- The difficulties faced by law enforcement operating lawfully in these environments are clear with many jurisdictions restricted by their national legislation. A harmonised approach to undercover investigations with clear directions and boundaries and is required across the EU. Part of this effort must focus on locating hidden services, to give ownership of an investigation to a specific Member States.
- Law enforcement would benefit from a strategic/tactical assessment of the scope of the criminal abuse of alternative Darknets (such as I2P and Freenet).

<sup>155</sup> Massachusetts Institute of Technology

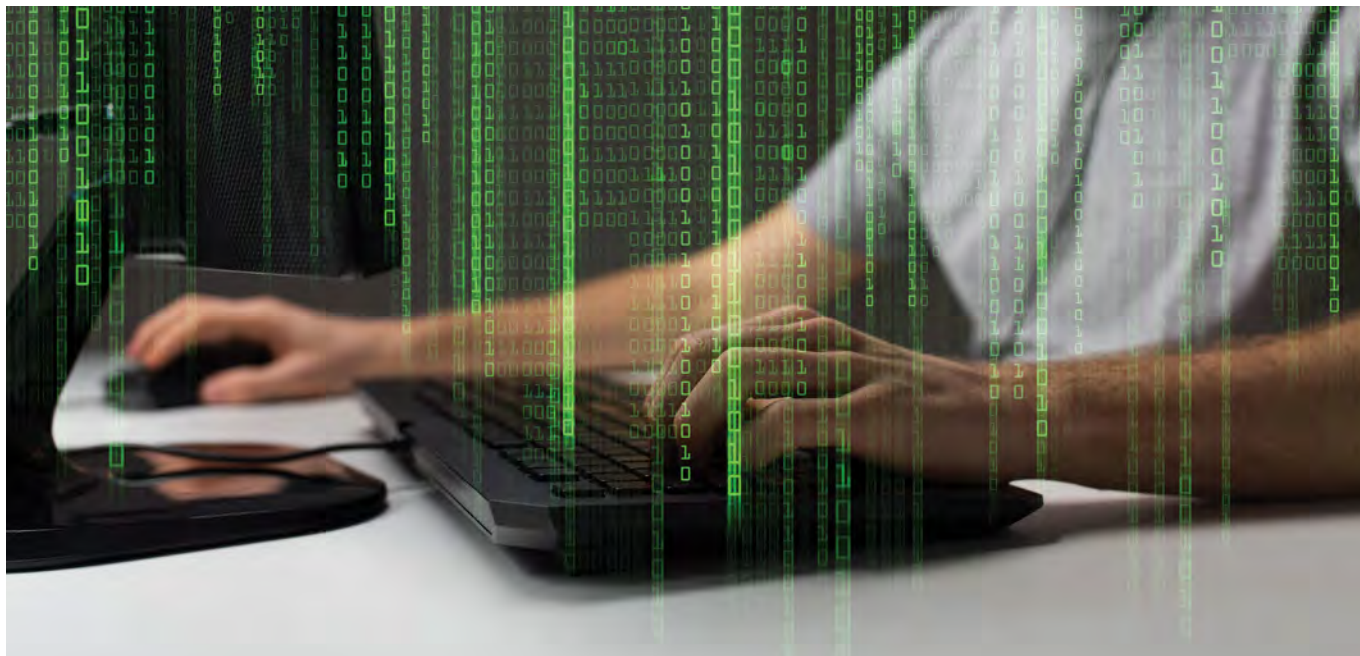
<sup>156</sup> MIT News, How to Stay Anonymous Online, <http://news.mit.edu/2016/stay-anonymous-online-0711>, 2016

<sup>157</sup> Kwon et al., Riffle: An Efficient Communication System With Strong Anonymity, <https://people.csail.mit.edu/devadas/pubs/riffle.pdf>, 2016

<sup>158</sup> OpenBazaar Blog, What is OpenBazaar?, <https://blog.openbazaar.org/what-is-openbazaar/>, 2016

<sup>159</sup> CoinDesk, Hours After Launch, OpenBazaar Sees First Drug Listings, <http://www.coindesk.com/drugs-contraband-openbazaar/>, 2016

# THE CONVERGENCE OF CYBER AND TERRORISM



The abuse of technology and legitimate online tools and services is not an exception in the terrorism landscape. Terrorists are becoming increasingly proficient in hiding their traces and activities by using anonymising and encryption tools and services. Furthermore, the anonymity provided by cryptocurrencies, and their preferential use in the trades taking place on darkmarkets, seems to be leading terrorists to invest in this currency. Goods and services offered on Darknet such as Tor are available to different actor groups, including terrorist groups. This ranges from malware, to illegal goods like stolen weapons, to crowdfunding sites claiming to support terrorist groups.

The thriving of the as-a-service industry in the digital underground provides easy access to criminal products and services that can be used by anyone, from technically savvy individuals to non-technically skilled terrorists. This allows cyber-attacks to be launched that are of a scale and scope disproportionate to the technical capability of the actors involved.

Nevertheless, currently most internet usage by terrorists, reported by law enforcement, relates to the use of unsophisticated tools and a widespread use of social media for propaganda, communication, recruitment and knowledge dissemination. Europol's EU Internet Referral Unit (EU IRU) has also reported a limited set of techniques currently used by terrorist groups online, focusing primarily on information disclosure and disruption of service.

## KEY THREAT – THE USE OF SOCIAL MEDIA

The most reported activity by law enforcement concerning terrorist activity on the internet is the use of social media. Terrorist groups use social media platforms extensively to engage in recruitment campaigns, propaganda, incitement of terror acts and for claiming responsibility for attacks.

Social media has been key to some terrorist groups' propaganda; it is used to disseminate their objectives and their achievements and has been shown to be crucial in the process of radicalisation and self-radicalisation. It is a process difficult to control, even when the platforms are fast in removing the content, due to the speed and simplicity of information dissemination online. Some law enforcement agencies note a growing trend in the process of self-radicalisation perhaps facilitated by fast and easy access to online propaganda. This seems to simplify the radicalisation process of "lone actors", who can be drawn to extremist ideals in front of their computer screens and led to commit attacks in their own countries without having to travel to war theatres in order to fight for the terrorist cause. This trend is enabled by the fact that the target group are usually millennials, with significant online presence for most of their lives. Some incidents suggest that terrorist groups target or appeal to individuals who are emotionally unstable and prone to violence, or have a history of criminal offences. These individuals are not necessarily affiliated with the religious ideology disseminated by some terrorist groups.



Social media is also the favoured method for dissemination of kill-lists (doxing)<sup>160</sup>. This provides lone actors with opportunities to demonstrate their support and affiliation of terrorist groups without having to leave their home countries<sup>161</sup>. The internet plays a fundamental role in the radicalisation of foreign fighters. Terrorist groups often rely either on platforms that are slow to remove content or instead demonstrate flexibility by changing platforms as required when their content is removed on a regular basis. Their strong strategy has been proved by the swiftness with which their acts are publicised online<sup>162</sup>. Furthermore, messaging applications often offering end-to-end encryption are increasingly being used by terrorist groups, not only to exchange information, but also as an advertising channel in the sex slavery trade<sup>163</sup> and other illegal trades.

Social media has had a great impact in cases of rapid radicalisation which, due to its swiftness, might fall under the radar of law enforcement agencies. Many recent attacks seem to have been an individual response to terrorist propaganda campaigns without direct intervention of terrorist groups 'leadership'<sup>164</sup>, adding challenges to the work of law enforcement agencies.

The role of the internet (and social media) has become one of the major themes in the radicalisation debate. It is worth noting that, thus far, there is no empirical evidence to suggest that the internet is amongst the root causes driving people into extremism. Equally, there are no conclusive findings supporting the view that an individual can become radicalised only from the internet without any offline influence.

Nevertheless, one can say that the internet can fulfil certain functions enabling an individual to become further entrenched into the radicalisation process. Firstly, it makes a large volume of extremist and terrorist material readily available to the user. This can reinforce the user's ideological predisposition and feed into his arguments.

In addition, the user can selectively choose among the information available online, editing out (disregarding) what is not in line with his thinking and absorbing only what corroborates his pre-existing beliefs - using the internet as an "echo chamber".

Finally, the user may find it easier to befriend like-minded individuals online rather than offline. If, for instance, he finds it hard to share his radical views with people in his physical milieu, he may be able to find other people eager to communicate with him online.

In general, the internet and social media can be considered a place in which an individual already on his path to radicalisation can validate his views and get recognition and confirmation from others about them. In that case the internet

is an *enabler* for the (self)radicalisation of an individual.

## KEY THREAT – DARKNET

Criminal forums and marketplaces usually operated in the open or Deep Web<sup>165</sup>. However, nowadays the Darknet is increasingly becoming host to such sites, commonly known as hidden services. Characterised by anonymity and availability of criminal tools, the Darknet is also a resource increasingly used by terrorists. Even though law enforcement is not reporting a significant trend on this matter, certain investigations on the aftermath of some attacks indicate that terrorists are aware of the potential of this environment, namely to communicate undetected by law enforcement or to purchase illegal materials. There is an increased demand for weapons that is fuelled by online markets where it is not difficult to purchase either gun parts or modified guns, demonstrating once again how online criminality is fuelling serious real world crime, such as terrorist attacks<sup>166</sup>.

Even though there is little evidence of sophisticated cyber-attacks by terrorists, the cybercrime as-a-service business model which drives criminal forums on the Darknet provides the access to tools and services to people with little knowledge of cyber matters, circumventing the need for expert technological skills. Furthermore, the environment also promotes exchange of information as well as "learning kits".

There appears to be an increasing trend in the number of Darknet forums dedicated to terrorist ideals. This growth has also been reflected in the increase of technically savvy terrorist affiliated individuals who share and disseminate their ideas in these forums. This has resulted in amplified cyber-attacks to Western targets even if they have been of little impact. However, this trend is indicative of growing cyber capability amongst these groups as their knowledge expands and they exchange expertise<sup>167</sup>.

## KEY THREAT – ENCRYPTION

Law enforcement agencies have reported an increasing trend in the use of encryption methods by terrorists including the use of encrypted communication apps. Terrorist groups are resorting to encryption and anonymising tools<sup>168</sup> in order to keep their identities hidden while they communicate, plan attacks, purchase illegal materials and perform financial transactions. There are strong parallels with security measures taken by CSE offenders and cybercriminals. There is also evidence of terrorist groups sharing expertise amongst themselves on how to remain untraceable online in order to better avoid the authorities. A good example of this practice is the OPSEC manual developed by a terrorist group, detailing practices on how to be secure on the web, and sharing best practices. In addition,

<sup>160</sup> Europol's ECTC, EU Internet Referral Unit, Affiliation & Capabilities of Cyber-Hacking Collectives with Jihadist Groups, 2016

<sup>161</sup> BBC, French Police Hit by Security Breach as Data Put Online, <http://www.bbc.com/news/world-europe-36645519>, 2016

<sup>162</sup> Perspective on Terrorism, Volume 9, edition 3, 2015

<sup>163</sup> International Business Times, ISIS Selling Yazidi Sex Slaves on Telegram and WhatsApp, <http://www.ibtimes.co.uk/isis-selling-yazidi-sex-slaves-telegram-whatsapp-1569132>, 2016

<sup>164</sup> Europol's ECTC, EU Internet Referral Unit 1st year report, 2016

<sup>165</sup> The term Deep Web refers to the part of the internet that is not accessible via standard search engines (e.g. password-protected sites, dynamically created or encrypted content). It is estimated that the Deep Web is considerably larger than the Surface Web.

<sup>166</sup> Time, How Europe's Terrorists Get Their Guns, <http://time.com/how-europes-terrorists-get-their-guns/>, 2015

<sup>167</sup> Flashpoint, Highlights & Trends in the Deep & Dark Web, [https://www.flashpoint-intel.com/home/assets/Media/Flashpoint\\_2015\\_Highlights\\_and\\_Trends.pdf](https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_2015_Highlights_and_Trends.pdf), 2016

<sup>168</sup> Flashpoint, Tech for Jihad: Dissecting Jihadists' Digital Toolbox, <https://www.flashpoint-intel.com/home/assets/Media/TechForJihad.pdf>, 2016

some terrorist groups have even developed their own customised terrorist tools, such as encryption applications<sup>169</sup>. Without proper training or guidance however, there is no guarantee that these will be used systematically or correctly.

Many legitimate services abused by criminals are also abused by terrorist groups; services such as DDoS mitigation tools which are being utilised to hide the real IP address of the websites that host propaganda. Terrorist groups also make use of bullet-proof hosting services located in the Middle-East in order to maintain anonymity and avoid surveillance while sharing and hosting information.

The use of multi-layered encryption, VPNs, Tor, and similar services, has been increasing amongst terrorists who are investing more and more in their online security, bringing added challenges to investigations<sup>170</sup>.

## KEY THREAT – CYBER-ATTACKS

Next to the use of social media, defacement of websites by terrorist groups is the most reported cyber activity by law enforcement. By defacing websites, the terrorists aim to spread their ideals, since the content of the website is usually replaced by propaganda. This technique also aims to create the idea amongst the general public that terrorist groups are skilled at hacking. However, defacements usually exploit common vulnerabilities and are relatively easy to perform. The fact that defacement of websites is the most common technique used by terrorists demonstrates that their cyber capabilities are currently low, even though the recent fusion of terrorist affiliated cyber groups might indicate an attempt to build-up resources and develop expertise. As some terrorist groups are reaching out to recruit in the western world, they might be capable of reaching out and attracting appropriately skilled people for their hacking groups<sup>171</sup>.

## FUTURE THREATS AND DEVELOPMENTS

Cyber-warfare and attacks on critical infrastructure are not usually conducted by a single individual, as it requires a high level of cyber capacity. Nevertheless some industry systems are poorly protected, which could be taken advantage of by these actors. Furthermore, the possibility of a cyber-attack with consequences in the real world should not be ignored. Terrorists have demonstrated willingness to develop their skills and can complement their existing capabilities with ready-made hacking products purchased in underground markets. The possibility of terrorist affiliated cyber groups engaging in cyber-warfare sponsored by nation states – those with the capabilities to engage in this type of attacks - should not be discounted. The availability of cybercrime facilitators, including zero-days exploits and data acquisition systems,

together with the increasing possibility of locating critical infrastructure systems, which increasingly have internet facing components, might attract different types of actors. Another potential threat to consider is a coordinated terrorist attack, where a complementary cyber-attack, even if small scale, could further amplify or exacerbate the damage of a real world attack.

Even though there is already evidence of terrorist groups using cryptocurrencies, it is expected that this phenomena will increase in the near future and that this type of currency might be increasingly used to launder money and fund terrorism. In addition, the current trend of money-making malware such as ransomware currently seen amongst ‘pure’ cybercriminals, together with the easy access to other cyber-crime tools, may lead terrorists to start employing this modus operandi to fund real world attacks. Access to tools, expertise and data, together with a growing number of internet facing devices and the constant development of the IoT, 3D printing, drones and smart contracts, seem to converge to an infinite number of possible scenarios to be exploited in the near future by terrorist affiliated cyber groups, even those without a high cyber capability.

## RECOMMENDATIONS

- Member States should consider establishment of proactive referral units following Europol’s EU IRU model, in order to pass on referrals quickly, efficiently and effectively, in close cooperation with the industry;
- The legal framework for the removal of terrorist and extremist online content needs to be improved. The referral of such activity does not currently constitute an enforceable act, and the decision and removal of referred/identified terrorist and extremist online content is presently taken by the concerned service provider;
- Member States competent authorities should increase their OSINT capacity in order to monitor the development of new technologies that have potential for abuse by terrorists and which have already been adopted, and to proactively monitor social media to detect early patterns of radicalisation;
- Enhanced cooperation is needed with national security services inside the EU frameworks in order to exchange timely and effective intelligence. The swiftness of terrorist groups’ communication online and the fast patterns of radicalization should be countered by an efficient fusion of intelligence at EU level. The EU constitutes an area where threats are shared, and where security must be provided collectively.

<sup>169</sup> Wired, Security Manual Reveals the OPSEC Advice ISIS Gives Recruits, <https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/>, 2015

<sup>170</sup> Trend Micro, Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/overlapping-technologies-cybercriminals-and-terrorist-organizations>, 2016

<sup>171</sup> International Business Times, ISIS Cyber Army Grows in Strength as Caliphate Hacking Groups Merge on Telegram, <http://www.ibtimes.co.uk/isis-cyber-army-grows-strength-caliphate-hacking-groups-merge-telegram-1553326>, 2016

# BIG DATA, IOT AND THE CLOUD



This section provides an updated law enforcement view on the interlinked topics of the Internet of Things, Big Data and Cloud computing and services<sup>172</sup>.

The growing adoption of the IoT further contributes to the convergence of people, processes, data, and objects to deliver new or enhanced services such as precision personalised medicine<sup>173</sup>, and provide improved contextual awareness and decision support. This not only introduces cybersecurity risks and ethical questions but also creates a number of challenges in terms of identity, privacy and trust.

Cloud computing and services provide the environment needed to support the storage and distributed processing of the data collected via the IoT. This links it to the concept of Big Data, which in essence is about new ways of analysing, visualising and leveraging large amounts of data in real-time or near real-time.

These concepts are a driving factor behind new types of 'critical infrastructure' such as smart cars, smart ships<sup>174</sup> or smart cities. However, they also play a crucial role in more conventional types of critical infrastructure, as more and more smart and connected sensors are being used in such settings too.

For law enforcement, Big Data, the IoT and the Cloud are no longer emerging threats but feature regularly in investigations. While there has been some improvement in terms of law enforcement's ability in dealing with these threats, the

dominating view is that police are still playing catch up in these areas.

As more and more relevant data will be located in the Cloud, cross-border cooperation to access electronic evidence and legal assistance will become even more critical. Consequently, some of the key concerns raised by law enforcement were around the perceived inadequacies of the MLAT process, difficulties in international cooperation and technical and procedural difficulties in seizing evidence stored abroad.

## CRIMINAL ABUSE OF THE CLOUD

More than 30% of European countries have investigations involving criminal infrastructure abusing the Cloud. For most of the reporting countries, the threat is medium to high and increasing. Nearly 50% of law enforcement in the EU reported the need to gather evidence from the Cloud during investigations and a small number of countries additionally reported investigations into attacks against Cloud providers, involving, in one instance, a ransomware attack.

For law enforcement, this is an increasing issue, which comes with legal, operational and technical challenges. While about half of law enforcement cooperates with academia and industry, only 41% of the reporting law enforcement agencies provide training on this topic to staff.

<sup>172</sup> IOCTA 2015, <https://www.europol.europa.eu/iocta/2015/big-data.html>, 2015

<sup>173</sup> Keith G. Kozminski, Biosecurity in the Age of Big Data: A Conversation with the FBI, <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4710219/>, 2015

<sup>174</sup> BIMCO, Cyber Security Guidelines for Ships Launched Today, [https://bimco.org/News/2016/01/04\\_Cyber\\_security\\_guidelines.aspx](https://bimco.org/News/2016/01/04_Cyber_security_guidelines.aspx), 2016



MORE THAN  
**30%**  
OF EUROPEAN  
STATES  
HAVE  
INVESTIGATIONS  
INVOLVING  
CRIMINAL  
INFRASTRUCTURE  
ABUSING  
THE CLOUD.



FOR MOST  
OF THE REPORTING  
COUNTRIES,  
**THE THREAT  
IS MEDIUM  
TO HIGH AND  
INCREASING.**

NEARLY  
**50%**  
OF LAW  
ENFORCEMENT  
IN THE EU  
REPORTED THE NEED TO GATHER  
EVIDENCE FROM THE CLOUD  
DURING INVESTIGATIONS.



## CRIMINAL ABUSE OF THE IOT

Over half of European law enforcement agencies surveyed indicated that many investigations involve smart devices, mostly in the form of smartphones. Nine countries also reported investigations into attacks against smart devices.

The IoT presents a growing number of legal and technical challenges including closed/proprietary systems and communication protocols (and the variety of operating systems), making standardised analysis difficult (e.g. requiring live data forensics). Moreover, encryption, fast development cycles and the rapid introduction of new products and a lack of training and education are additional issues.

While 68% of law enforcement cooperates with academia

and industry in relation to the IoT, only about 32% of the reporting agencies provide training in this area.

## BIG DATA

The increasing digitisation of evidence creates substantial volume challenges for law enforcement. The reported average volume of data per investigation is now close to 3TB and it is expected that this figure will continue to rise.

48% of the responding European countries cooperate with academia and industry on Big Data and/or provide training. However, only 24% of these countries use Big Data analytics as part of their work in, for instance, the identification of crime hotspots.

Law enforcement has highlighted a number of challenges in relation to Big Data such as the difficulty in seizing large amounts



of data in a forensically sound manner. The subsequent analysis of the data also takes proportionately longer. Other issues include lack of tool support, hardware and software costs (particularly data storage costs including backup solutions), legal and privacy issues (such as how to protect personal data) as well as the need for specialist skills and training.

## FUTURE THREATS AND DEVELOPMENTS

The increasing amount of data that is being collected and processed via the IoT creates new privacy, cybersecurity and trust issues and risks. Because of the scale of the IoT, trust between different devices and across different platforms can be hard to engineer and expensive to guarantee.

The decision support and contextual awareness offered by smart devices will make them and any supporting infrastructure a target for criminal data manipulation too.

It is inevitable that the new types of ‘critical infrastructure’ created by the IoT, as well as existing infrastructures, will be the targets of novel hybrid threats such as new forms of extortion involving hacked smart devices (ranging from very small medical devices, to smart cars, smart container ships and smart cities), data theft, attacks resulting in physical and mental harm, and new types of botnets<sup>175</sup>. Such attack scenarios would not be limited to a particular category of attackers or a particular set of motives.

New approaches to increasing cybersecurity for the IoT and to establishing trust and ensuring privacy in the decentralised network it creates may include the use of the blockchain or Distributed Ledger Technology (DLT)<sup>176</sup>. DLT can potentially provide a framework to facilitate transaction processing and

coordination among interacting IoT devices. It may also be applied to ensure that the operating system and firmware used in a smart component of critical infrastructure has not been tampered with.

An area of particular concern is the field of biosecurity and the link to the increasing market of private companies offering DNA sequencing. Unlike stolen credit card information, someone’s DNA fingerprint cannot be ‘invalidated’ once it has been leaked.

<sup>175</sup> Security Intelligence, The Threat From Weaponized IoT Devices: It’s Bigger Than You Think!, <https://securityintelligence.com/the-threat-from-weaponized-iot-devices-its-bigger-than-you-think/>, 2016

<sup>176</sup> CoinDesk, IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things, <http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/>, 2015

## RECOMMENDATIONS

- Supported by a pro-active, agile and adaptive model, law enforcement requires the relevant training and skills to be able to effectively investigate crimes involving smart devices, including seizing evidence stored in the Cloud. This should also cover the use of new technologies and possibilities such as Big Data analytics to support the work of law enforcement.
- Law enforcement should further strengthen collaboration with industry, the financial sector and academia with a view to achieving improved technology readiness and developing the required preventive and investigative capabilities.
- Research should be stimulated into Big Data analytics, machine learning and Artificial Intelligence (AI) approaches with a view to improving cybersecurity and law enforcement work through better threat detection and prediction, intelligence collection and analysis, and faster responses.
- Law enforcement needs to dedicate resources to further building and enhancing the necessary skills and expertise and to acquiring the tools needed to process, index, analyse and visualise large amounts of data.
- As already highlighted in previous reports, security-by-design, security-by-default and privacy-by-design should be the guiding principles when developing smart devices, making use of standards, industry best practices and recommendations<sup>177</sup>.



<sup>177</sup> ENISA, Securing Europe's IoT Devices and Services, [https://www.enisa.europa.eu/events/copy\\_of\\_enisa-workshop-on-cyber-security-for-iot-in-smart-home-environments/1-enisa-securing-europes-iot-devices-and-services](https://www.enisa.europa.eu/events/copy_of_enisa-workshop-on-cyber-security-for-iot-in-smart-home-environments/1-enisa-securing-europes-iot-devices-and-services), 2015



# INTERNET GOVERNANCE

The internet is governed according to a 'multi-stakeholder model'<sup>178</sup> whereby a multitude of parties – mostly private actors – interact to discuss and develop principles and norms that regulate how the Internet will develop and function. Compared to the traditional intergovernmental approach where sovereign states discuss on an equal footing, in the multi-stakeholder model, governments which represent the public interest only have a limited influence in the process.

This brings an important challenge for the law enforcement community whose actions to attribute crime online are directly dependent on the standards and rules governing the Internet. In addition, those rules and norms can leave vulnerabilities that can be exploited by criminals. For example, the Domain Name System (DNS) which translates domain names into IP addresses can be abused by criminals to carry out illegal activities: by manipulating DNS records<sup>179</sup>, criminals can hijack a domain to redirect traffic to another domain which will distribute malware. The TCP/IP protocol can also be exploited to launch a DDoS attack via SYN flooding<sup>180</sup>.

There are many challenges from a law enforcement perspective pertaining to the current developments in the Internet Governance field. However, in 2016 the main ones are related to: the discussion on the accreditation of Privacy and Proxy services, the reform of the DNS WHOIS and to the generalisation of the use of Carrier-Grade Network Address Translation (CGN) technologies by internet service providers (ISPs).

## ACCREDITATION OF PRIVACY AND PROXY SERVICES

One of the most relevant issues for law enforcement discussed within ICANN<sup>181</sup>, relates to the accreditation of Privacy and Proxy services. Registrars often offer Privacy and Proxy (P/P) services to customers who wish to keep certain information from being made public via the WHOIS (publicly available database of the registration information of each domain name holder). However, P/P services are often misused to hide criminal activities. For instance bullet proof hosters (BPHs) will use untraceable WHOIS details to register servers aided by privacy-protection legal services<sup>182</sup>.

ICANN has committed to establish an accreditation program for P/P service providers to establish a contractual framework. The bottom line is that ICANN should only accredit Registrars that cooperate with public authorities to avoid - as much as possible - rogue actors providing key elements of bullet proof hosting infrastructure and obscure pertinent information.

Unfortunately, the concerns of the law enforcement community have not been included in the current recommendations adopted by the ICANN Board<sup>183</sup>. The consequences are detrimental to the prevention of crime online:

- Firstly, according to the ICANN Board recommendations, P/P service providers should only comply with express requests from LEA not to notify a customer where this is required by applicable law. In other words, P/P service providers will not have to keep law enforcement request for information confidential unless served with a court order.
- Second, P/P service providers may only be compelled to respond to law enforcement requests coming from within their own jurisdiction while many investigations are cross-border.
- Thirdly, entities running domains/websites actively engaged in commercial transactions – i.e. the collection of money for a good or service – will be allowed to conceal their identity using privacy and proxy services.

Some of these concerns could possibly be addressed during the implementation of the recommendations but the law enforcement community needs to engage with its government representatives at ICANN to ensure a positive outcome.

## REPLACING THE DNS WHOIS

The WHOIS is a free, publicly available directory containing the contact details of registered domain name holders (registrants). Anyone, including law enforcement, who needs to know who is behind a domain name can make a request for that information via the WHOIS protocol. The data is collected and made available by registrars and registries under the terms of their agreements with ICANN. Accurate WHOIS information is therefore essential for consumer protection and law enforcement to investigate and attribute abuse and unlawful activity online.

However, despite a number of ICANN contractual obligations to ensure accurate WHOIS information, bad actors have found many ways to register domain names anonymously. In parallel data protection authorities have been criticising the WHOIS for failing to adhere to European data protection standards.

A new ICANN Policy Development Process (PDP) has been established in 2016 to determine whether a new system could replace the WHOIS. The PDP has started working on the basis of the recommendations of a report adopted in 2014 by an Expert Working Group (EWG)<sup>184</sup>.

<sup>178</sup> EastWest, Exploring Multi-Stakeholder Internet Governance, <https://www.eastwest.ngo/idea/exploring-multi-stakeholder-internet-governance>, 2015

<sup>179</sup> For instance using a DNS changer malware or by announcing false DNS records to peer ASNs.

<sup>180</sup> SYN flooding is a TCP sequence number prediction to generate counterfeit packets in a TCP connection and access the target host using a normal TCP/IP connection.

<sup>181</sup> ICANN – the Internet Corporation for Assigned Name and Numbers - manages domain names and IP addresses at global level.

<sup>182</sup> Trend Micro, Criminal Hideouts for Lease: Bulletproof Hosting Services, <http://www.trendmicro.nl/media/wp/wp-criminal-hideouts-for-lease-en.pdf>, 2015

<sup>183</sup> ICANN, Approved Board Resolutions, Special Meeting of the ICANN Board, <https://www.icann.org/resources/board-material/resolutions-2016-08-09-en#2.e>, 2016

<sup>184</sup> ICANN, A Next-Generation Registration Directory Service (RDS), <https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf>, 2014



In order to reconcile privacy and data protection laws with the requirement to have contact details for each domain names, the EWG recommended of a “gated access” to WHOIS information. In other words, the current model of anonymous public access to all gTLD<sup>185</sup> registration data might be discontinued. Instead, registration data would be disclosed for permissible purposes only, with some data elements being accessible only to authenticate requestors. This means that law enforcement agencies will need to be validated and accredited in order to query the database of registration of domain names.

This raises a number of issues as to which organisation will serve as the accrediting body and how this will impact the speed at which LEA will be able to obtain relevant information.

## CARRIER-GRADE NETWORK ADDRESS TRANSLATION (CGN)

Recently, many new technologies have made the headlines because they hinder law enforcement’s ability to follow criminal leads and attribute crime. But the Going Dark problem is not limited to the TOR network, proxy servers, bullet proof hosting and encrypted communication apps. A far more diffused technology is posing massive attribution problems to the law enforcement community.

The global demand for internet accessibility has led to an explosion in use of internet enabled devices. This growth has resulted in the exhaustion of the Internet Protocol version

4 (IPv4) addresses. The new version of the Internet Protocol known as IPv6, offers a virtually unlimited number of IP addresses. However, the transition from IPv4 to IPv6 has been slower than expected because of the lack of commercial incentive to do so and the numerous necessary upgrades to the IPv4 legacy infrastructure. The transition from IPv4 to IPv6 has forced many network operators and Internet Service Providers (ISPs) to support and maintain both address infrastructure schemes so that devices are able to run IPv4 and IPv6 in parallel (dual stack).

Against this background and in order to address the gradual exhaustion of IPv4 addresses, ISPs and mobile Internet service providers have adopted a temporary solution called Carrier-Grade Network Address Translation (CGN).

### ■ WHAT IS CARRIER GRADE NAT (CGN)?

CGN is an evolution of the traditional Network Address Translation (NAT) protocol, which has been used for the last 25 years in private networks (home, small businesses). NAT dynamically translates a collection of private IP addresses connected to each of the home or business user’s devices to one public IPv4 address used within one network (i.e. routable on the internet). That one public IP address is announced at the customer endpoint user’s modem which interfaces with the customer endpoint user’s content service provider network. CGN is much more pervasive than NAT; instead of an endpoint user having a single public IP address, CGN allows a single IP address to be shared by potentially thousands of subscribers at the same time.

<sup>185</sup> Generic Top Level Domain.

## ■ CGN IMPACT ON LAW ENFORCEMENT INVESTIGATIONS

With CGN, law enforcement has lost its ability to associate and link a particular cyber criminal's activity back to a particular IP address. Cyber investigators now need to determine which one of the hundreds of consumers associated with a particular public IP address is behind the actions which they are investigating.

One Member State reported that in a recent investigation into Child Sexual Exploitation Material (CSEM) distributed and hosted via a cloud-based service, the investigators had to investigate each one of the 50 clients using that public IP at this time in order to identify who was ultimately uploading the CSEM, because the cloud-based service provider did not log the relevant information to discriminate which customer was using the public IP.

## ■ SCALE OF THE PROBLEM

A survey conducted in August 2016 among European cyber-investigators, shows that problem of crime attribution related to CGN technologies is regularly encountered by 90% of the respondents during their investigations<sup>186</sup>.

In a number of cases, the investigation is discontinued. Alternatively the investigations were delayed because the investigators needed to resort to additional, lengthy and possibly more invasive investigative techniques in order to identify the end-user. 98% of the respondents support a European-wide mandatory legal requirement for electronic service providers to identify end users of IP addresses.

## FUTURE THREATS AND DEVELOPMENTS

For many years, most actors involved shared the view that the simplest solution to this problem was to wait for the full transition to IPv6, because the trillions of IP addresses available would do away with the need to use CGN. Current trends indicate that the transition to IPv6 will not be completed before at least the next two decades.

Currently, almost all European mobile ISPs use CGN technologies and a large majority of conventional ISPs (cable, fiber and ADSL) have converted their network infrastructure to use CGN.

In addition, responding to customers' demand, telecom equipment companies such as CISCO and JUNIPER have started selling software solutions to translate IPv6 addresses into IPv6 addresses<sup>187</sup>. This means that CGN is here to stay and that the law enforcement community needs to resort to other means to continue to be able to perform a trace back to an individual end user of an IP address.



## RECOMMENDATIONS

- In order to be able to trace back an individual end user to an IP address on a network using CGN, law enforcement must request additional information<sup>188</sup> from the service providers via legal process:
  - Source and Destination IP addresses.
  - Source port number.
  - Exact time of the connection (within a second).
- However, the lack of harmonised data retention standard requirements in Europe<sup>189</sup> means that content service, Internet service and data hosting providers are under no legal obligation to retain this type of information, meaning that even a more elaborate request from a law enforcement agency would not yield useable information from the provider.
- Regulatory/legislative changes are required to ensure that content service providers systematically retain the necessary additional data (source port) law enforcement requires to identify end users.
- Alternatively, practical solutions can be developed through collaboration between the electronic service providers and law enforcement. Some electronic providers in Europe do store the relevant information (source port). A European-wide portal could maintain an updated list of those providers and a list of contact points to address in case an investigation is stalled by CGN.

<sup>186</sup> Internal survey conducted by the European Cybercrime Centre among all EU Member States cyber divisions

<sup>187</sup> NetFlask, NAT66 and IPv6 ULA on Juniper SRX, <https://www.netflask.net/nat66-and-ipv6-ula/>, 2014

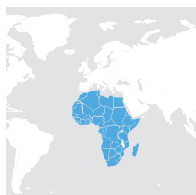
<sup>188</sup> Internet Engineering Task Force (IETF), Recommendation for Comment (RFC) 6302, Logging Recommendations for Internet-Facing Servers, <https://tools.ietf.org/html/rfc6302>, 2011

<sup>189</sup> On 8 April 2014 the European Court of Justice annulled the Data Retention Directive <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>, 2014



# THE GEOGRAPHIC DISTRIBUTION OF CYBERCRIME

The following is a brief summary of geographic threats and cybercrime activity throughout 2015-2016 based on law enforcement and industry data. The overview makes use of the United Nations geoscheme<sup>190</sup> and uses the reported data to highlight in which countries European law enforcement has identified criminal suspects and/or infrastructure (CSI) throughout the course of the reporting period. It does not however reflect the number of individual investigations.



## AFRICA

While Africa boasts a rapidly growing internet infrastructure it still has the lowest global internet penetration (28.6%). What it lacks in saturation it makes up for in numbers with almost 10% of global internet users (compared to Europe, which has 17% despite 74% penetration)<sup>191</sup>. Benefiting from a series of high bandwidth undersea conduits along the eastern and western seaboard, African almost suffers more now from power distribution issues than internet access<sup>192</sup>.

Arriving somewhat later to the scene, some African nations have profited from being able to skip a number of technology milestones such as landlines and branch banking, instead leaping straight to mobile telephones and online banking. By 2020, smartphone internet connections are expected to exceed those of North America<sup>193</sup>. This is not without consequence however, as Africa now has one of the highest global mobile malware infection rates<sup>194</sup>.

While many African states are rapidly adopting cybercrime legislation<sup>195</sup>, they are still relatively lagging behind when it comes to implementing and practising cyber security.

11 European countries identified CSI in 13 different African states throughout 2015/2016, with Nigeria featuring as a cybercrime hotspot for all 11 European countries. Indeed, Nigeria was the third most frequently identified country as the location for CSI alongside the UK and Germany.



<sup>190</sup> UN Statistics Division, Geographical Region and Composition <http://unstats.un.org/unsd/methods/m49/m49regin.htm>, 2013

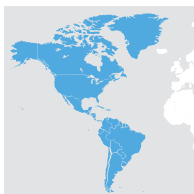
<sup>191</sup> Internet World Stats, <http://www.internetworldstats.com/stats.htm>, 2016

<sup>192</sup> The Guardian, Can the Internet Reboot Africa?, <https://www.theguardian.com/world/2016/jul/25/can-the-internet-reboot-africa>, 2016

<sup>193</sup> The Guardian, Can the Internet Reboot Africa?, <https://www.theguardian.com/world/2016/jul/25/can-the-internet-reboot-africa>, 2016

<sup>194</sup> McAfee Labs, Threats Report, <http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-may-2016.pdf>, June 2016

<sup>195</sup> PCWorld, Africa's Effort to Tackle Cybercrime Gains Momentum, <http://www.pcworld.com/article/2981739/africas-effort-to-tackle-cybercrime-gains-momentum.html>, 2015



## THE AMERICAS

The United States continues to maintain its global lead (~ 30% of global figures<sup>196,197</sup>) in the hosting of botnet command and control servers. The US was also a top spam sending country in 2015, accounting for up to 16% of global spam and was the largest global host of malicious URLs<sup>198</sup> including phishing websites<sup>199,200,201</sup>. Unsurprisingly the US was the top location identified by European law enforcement for harbouring CSI.

The digital underground in the US largely operates from the Surface Web. As a highly competitive, English-speaking community, this environment attracts many fledgling cybercriminals. The Canadian underground is still in its relative infancy, and largely centres on the sale of forged or stolen ID documents and compromised financial credentials<sup>202</sup>. Canada would appear to be a growing concern for European law enforcement as it held joint 7th place in terms of destinations where law enforcement identified CSI.

Latin America is a region that registers some of the highest

malware infection rates<sup>203</sup>. Although it varies from month to month, some South American countries such as Chile and Belize host significant proportions of global phishing sites, on occasion surpassing that of the USA<sup>204</sup>.

Brazil has nurtured a thriving digital underground, although it largely operates openly and brazenly on the Surface Web internet rather than hiding in the Deep Web. While the Brazilian market is dominated by home-grown banking Trojans, almost any recognisable cybercrime tool can be found on these markets<sup>205</sup>.

Eight European countries identified CSI in South America, with Brazil and Mexico being top destinations, followed by Chile and Colombia.



## ASIA

China has an extensive and increasingly innovative digital underground. While it makes less use of traditional cybercrime forums, instead choosing to use instant messaging or spam on existing (unrelated) fora to drum up business, the range of products and services available mirrors that of Western underground markets. These markets are a key source for tools and equipment relating to card crime, such as ATM and POS skimmers<sup>206</sup>.

China and Taiwan have some of the highest global malware infection rates and consequently highest volumes of global bots<sup>207,208</sup>. As a region, Asia also has the highest rate of mobile malware infection after Africa<sup>209</sup>.

China, Vietnam, India, Japan and Taiwan are reported as top sources of global spam<sup>210,211</sup>. Additionally, Asia is allegedly the source of over 50% of global DDoS attacks, with China alone responsible for over one quarter of these attacks. South Korea, India, Thailand and Japan make up the remainder<sup>212</sup>.

16 European countries identified CSI in Asia, with 12 of those locating CSI in China. Other common countries for the location of CSI were typically in East or South-East Asia, however India was the second most common Asian country alongside Hong Kong.

<sup>196</sup> McAfee Labs, Threats Report, <http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-may-2016.pdf>, June 2016

<sup>197</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>198</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>199</sup> APWG, Phishing Activity Trends Report, 1st-3rd Quarters 2015, [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1-q3\\_2015.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf), 2015

<sup>200</sup> Symantec, Internet Security Threat Report 2016, <https://www.symantec.com/security-center/threat-report>, 2016

<sup>201</sup> SecureList, Spam and Phishing in Q1, 2016, <https://securelist.com/analysis/quarterly-spam-reports/74682/spam-and-phishing-in-q1-2016/>, 2016

<sup>202</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>203</sup> Panda, Pandalabs' Annual Report 2015, <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>, 2015

<sup>204</sup> APWG, Phishing Activity Trends Report, 1st-3rd Quarters 2015, [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1-q3\\_2015.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf), 2015

<sup>205</sup> Trend Micro, Ascending the Ranks, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-ascending-the-ranks.pdf>, 2015

<sup>206</sup> Trend Micro, Prototype Nation, The Chinese Cybercriminal Underground in 2015, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-prototype-nation.pdf>, 2015.

<sup>207</sup> Panda, Pandalabs' Annual Report 2015, <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>, 2015

<sup>208</sup> Symantec, Internet Security Threat Report 2016, <https://www.symantec.com/security-center/threat-report>, 2016

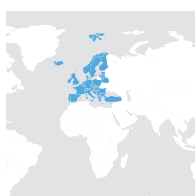
<sup>209</sup> McAfee Labs, Threats Report, <http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-may-2016.pdf>, June 2016

<sup>210</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>211</sup> Symantec, Internet Security Threat Report 2016, <https://www.symantec.com/security-center/threat-report>, 2016

<sup>212</sup> Akamai, State of the Internet, Akamai, Q1 2016,

<https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf>, 2016



## EUROPE

While many European countries no doubt have some form of domestic digital underground, Germany is considered by some researchers to have one of the fastest growing underground markets within the EU, although much of its crimeware products focus only on domestic targets<sup>213</sup>. Russia, or at least Russian speaking countries, are still generally considered to maintain some of the most established cybercrime marketplaces<sup>214</sup>.

Europe benefits from some of the lowest global malware infection rates<sup>215</sup> for both computer and mobile malware<sup>216</sup>. Out of this however, Germany and France have the highest proportions of connections to C2 infrastructure (effectively a measure of the number of bots) in the EU<sup>217</sup>. Germany, the Netherlands, France and the UK are top EU countries for the hosting of C&C infrastructure, with the Ukraine and Russia leading the non-EU states<sup>218,219</sup>. Russia is also the top European country for the hosting of malicious URLs, with the Netherlands not far behind<sup>220</sup>. While only representing a fraction of global figures, Italy, Belgium, France, Germany, Italy, the Netherlands and the UK also commonly feature in top 10 lists for hosting phishing websites<sup>221</sup>.

Within the EU, Spain and Italy are top spam sending countries,

with Russia leading within Europe as a whole<sup>222</sup>. Additionally Spain is consistently one of the top 10 global sources of DDoS, accounting for between 6-7% of global attacks<sup>223</sup>.

Of the top 20 countries where European states have identified CSI, more than half were other European states, although this may reflect higher levels of cooperation and communication, facilitated by Europol. Germany and the UK were top locations for the identification of CSI with 10 other European states pinpointing each of those jurisdictions.



## OCEANIA

It is reported that, globally, Australia is one of the top five countries clicking on malicious URLs, and as a likely consequence also one of the top five countries making connections to C2 infrastructure<sup>224</sup>. Australia does however benefit from one of the lowest mobile malware infection rates<sup>225</sup>.

While still only a tiny fraction of global figures (less than 1%), Australia hosts a growing number of phishing websites<sup>226</sup>.

Six European countries identified CSI in Oceania as part of their investigations, five of those in Australia.

<sup>213</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>214</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>215</sup> Panda, Pandalabs' Annual Report 2015, <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-annual-EN.pdf>, 2015

<sup>216</sup> McAfee Labs, Threats Report, <http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-may-2016.pdf>, June 2016

<sup>217</sup> McAfee Labs, Threats Report, <http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-may-2016.pdf>, June 2016

<sup>218</sup> McAfee Labs, Threats Report, <http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-may-2016.pdf>, June 2016

<sup>219</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>220</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>221</sup> APWG, Phishing Activity Trends Report, 1st-3rd Quarters 2015, [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1-q3\\_2015.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf), 2015

<sup>222</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>223</sup> Akamai, State of the Internet, Akamai, Q1 2016,

<https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf>, 2016

<sup>224</sup> Trend Micro, Annual Security Roundup, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf>, 2015

<sup>225</sup> McAfee Labs, Threats Report, <http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-may-2016.pdf>, June 2016

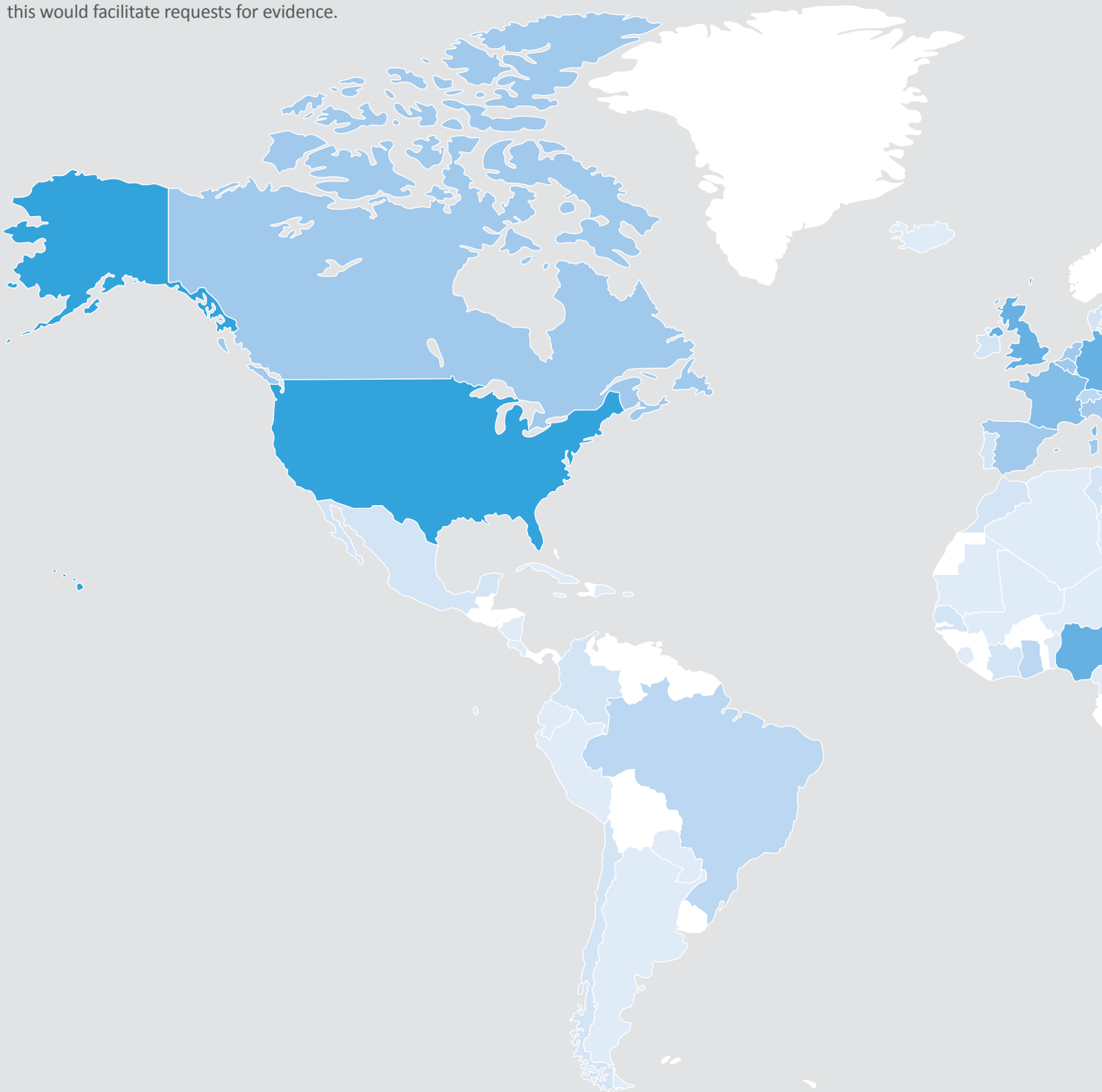
<sup>226</sup> APWG, Phishing Activity Trends Report, 1st-3rd Quarters 2015, [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1-q3\\_2015.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf), 2015



# CYBERCRIME HEATMAP

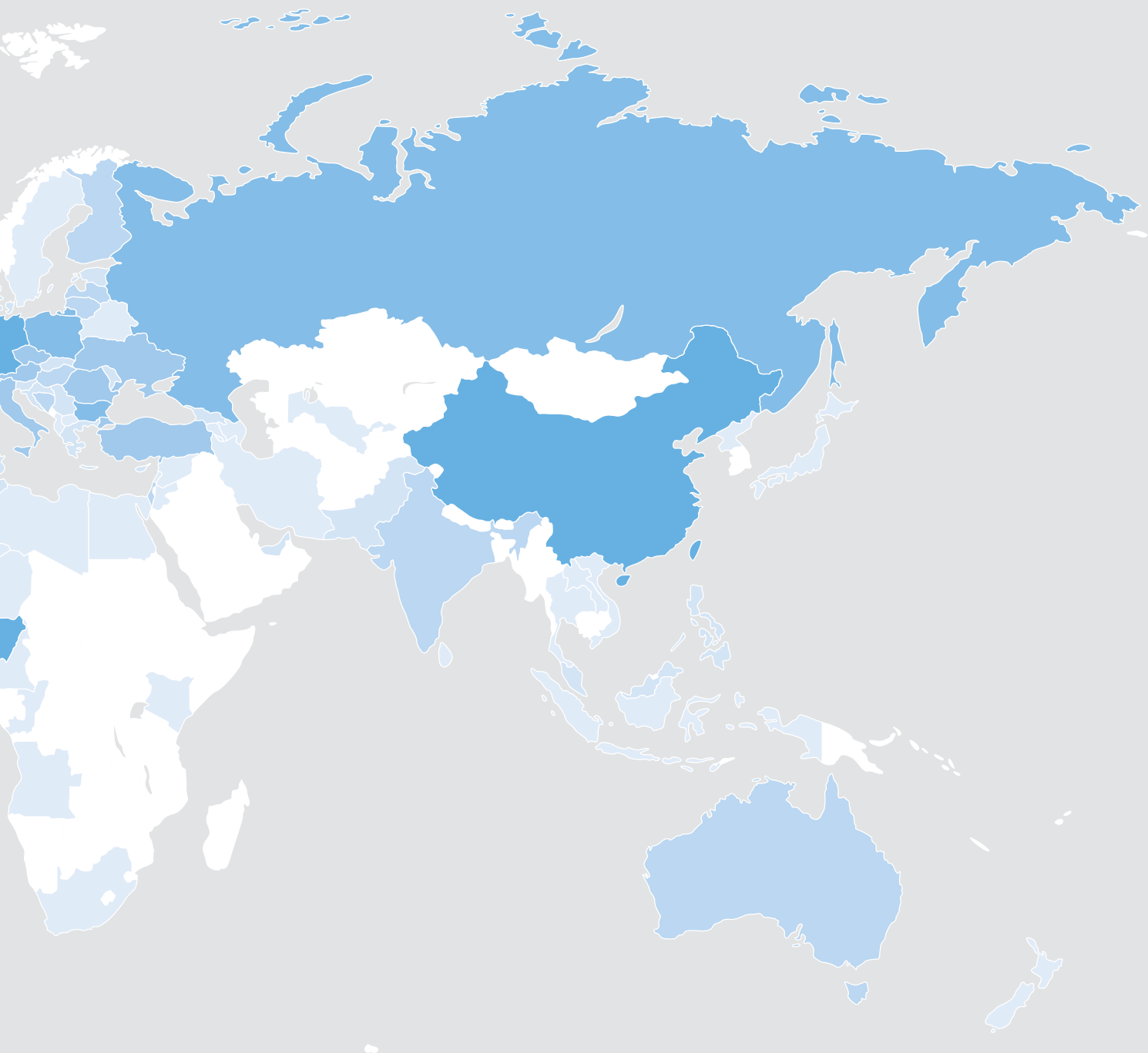
The heat map below highlights the number of European countries that have identified criminal suspects and/or infrastructure (CSI) in each shaded country. Note that this does not reflect the number of individual investigations, simply the number of states that have identified CSI there during the reporting period.

Less than one third of countries identified as the location of CSI were forwarded an MLAT as part of that investigation. There is no apparent pattern to whether a country receives MLAT requests; countries within and outside the EU are as likely or unlikely to be sent an MLAT request. The probability may reflect the nature of individual investigations, individual states' relationships with the other jurisdiction, or perhaps the use of other information or intelligence sharing pathways, not that this would facilitate requests for evidence.





The number of European states that have identified criminal suspects and/or infrastructure in each country.



# ■ APPENDICES

## A1. THE THREAT POSED BY QUANTUM COMPUTERS

### ■ INTRODUCTION

There has been considerable progress made in recent years into producing a viable quantum computer. Forms of quantum computer are already being sold to organisations such as Google, NASA and Lockheed Martin. This has led some to speculate that such computers pose an imminent threat to on-line security and, if made available to criminals, would leave many vulnerable.

### ■ QUANTUM COMPUTERS - THE THREAT

Whereas conventional computers use “bits” for computing algorithms, quantum computers use “qubits”. Both bits and qubits can have the values 0 and 1, but qubits can be both 0 and 1 simultaneously during the execution of certain algorithms. In essence, quantum computers can run certain algorithms on a range of possible values in parallel, reducing to a single answer only when measurements are taken.

One of the first quantum algorithms developed was by Peter Shor. It was a way of using a well-known conventional algorithm for deriving the two prime numbers that have been multiplied to produce a composite number, known as factoring. One of the most popular public key encryption schemes in use today, RSA, relies upon the fact that it is easy to multiply two large prime numbers together but very difficult to determine those prime numbers given the resulting large product. All of the main forms of public key encryption in use on the internet today (RSA, ECDSA and DSA) rely upon mathematics that should be easy to compute in one direction but are computationally very hard to reverse (one way functions).

Shor’s algorithm introduced a way in which one particular part (known as order finding) could take advantage of the parallelism afforded by quantum computers. The result was that a quantum computer could derive the prime numbers in a composite in a fraction of the time it would take a conventional computer running the same algorithm. Subsequently it was realised that Shor’s algorithm was one of a class of quantum algorithms known as the Hidden Subset Problem (HSP).

It was then realised that the mathematics behind RSA, ECDSA and DSA are all solvable by variants of the HSP, using a quantum computer, in timescales that render these encryption schemes insecure. What might take thousands of years to solve on a conventional computer will take minutes on a large quantum computer running, for example, Shor’s algorithm.

### ■ THE EXTENT OF THE THREAT

It is likely that the first substantial quantum computers will be

run by large, possibly government, organisations. Hence, one might argue that the threat is limited even once they enter operation. However, even before they evolve to domestically housed devices in the way conventional computers did, it is highly likely that the ability to use such systems will be widely available.

This model is already visible in the way companies such as IBM and DWave make their existing quantum computer facilities accessible to the wider public as a form of cloud computing. Hence, it is possible that criminals may be able to utilise the power of quantum computers to undermine internet security within the foreseeable future. The consensus is that this situation could exist as early as 2025-2030.

It is notable that although quantum information processing has been studied since the 1980s, there have not been a large number of quantum algorithms developed. There are essentially only three classes of quantum algorithm of which the HSP is the only class that appears to have implications for on-line security.

It should also be noted that not all quantum computers use the same principles. For example, the offering from DWave is not suitable for running algorithms for solving the HSP.

Some argue that the second class of quantum algorithm that contains Grover’s algorithm (a form of rapid searching in unstructured data) means that it is easier to, for example, conduct searches for encryption keys when those keys are of a known form. This typically applies to symmetric encryption rather than public key encryption. However, the speed advantage given by Grover’s algorithm is not the same exponential increase seen with Shor’s algorithm. The consensus is that by doubling the length of the shared secret key used by parties to a secure dialogue the advantages of using a quantum computer would be overridden.

Whilst law enforcement should be concerned about the threat that quantum computers pose, and they should be aware that it is a problem already looming on the horizon, it is a problem that has well understood boundaries. Hence, in working with academia and industry, law enforcement should encourage research into, and the adoption of, encryption schemes that are not susceptible to quantum algorithms within the HSP.

### ■ CANDIDATE SOLUTIONS

Candidates are being sought where a mathematical one way function that replaces those in use with RSA, ECDSA and DSA, and for which the HSP does not provide a solution. In searching for such a post quantum candidate, one also has to remember that it has to satisfy all of the security requirements of current schemes, i.e. it has to resist attacks that might be run on conventional computers.

Some candidates have existed since the earliest days of public key encryption, and despite 30 years of attempts they have resisted all attempts to break them. However, they failed to gain traction for a variety of reasons. For example, the public key that was generated was very large and would necessitate



megabytes of data being exchanged for each transaction. Since the threat from quantum computers was recognised, variants of these early schemes have been suggested which solve some of the practical problems. Unfortunately, the variants so far proposed of these early schemes have been found to lack the level of security of the early versions.

The most likely source of post quantum encryption currently appears to be what is called Lattice Based Encryption. In the last 10 years this has seen a relatively rapid evolution into deployable schemes. The most popular of these schemes (known as NTRU) has not been widely explored in commercial practice as patents exist requiring licencing. However, this changes in late 2017. There are also recent variants of the NTRU scheme which are not affected by patents.

The most recent work has extended the original lattice based schemes with a technique known as Learning With Errors (LWE). These schemes have seen some very rapid evolution in the last two years. The most recent variant, proposed only at the end of 2015, is called New Hope. An experimental implementation of New Hope has already been deployed by Google as part of the SSL/TLS implementation in its Chrome browser.



## ■ CONCLUSION

Quantum computers are very likely to pose a threat to online security within the next decade.

Whilst quantum computers will require significant infrastructures to run in their early forms, there can be no doubt that the gains to be made from undermining existing online security will drive criminals to access such technology. In a world of cloud computing this is likely to be possible from the earliest eras of quantum computing.

However, whilst quantum computers pose a very specific threat we already know how it can potentially be mitigated. The European Union has already provided significant funding for research into identifying viable post quantum encryption schemes, and NIST<sup>227</sup> has begun public consultation on the criteria that it should specify in a post quantum encryption scheme competition.

In the same way that security software has to be updated to mitigate new forms of malware, or encryption libraries have to be updated if a flaw is identified, commercial implementations of public key encryption software (particularly implementations of TLS) are likely to adopt post quantum encryption schemes which will be useless in preventing crime if they are not put into use.

Those involved in ensuring online security should be encouraged to remain abreast of these developments as it could see steep changes which alter the threat landscape.

<sup>227</sup> National Institute of Standards and Technology

## A2. CYBER LEGISLATION

The 2014 and 2015 IOCTAs emphasised that it is essential for law enforcement to closely observe developments in the field of law.

### ■ UPDATE 1: EU CYBERCRIME LEGISLATIVE FRAMEWORKS

Since the publication of the last IOCTA, the European Union has not yet introduced a new legislative framework to harmonise the cybercrime legislation of the Member States.

One topic closely related to cybercrime is cybersecurity. Focus was therefore on the drafting process of the EU Directive on Network and Information Security (NIS Directive). It was adopted in July 2016. While the Directive addresses various issues related to cybersecurity in general it does not contain any provisions specifically focussing on cybercrime. However, the Directive states that Member States should encourage operators of essential services to report incidents to law enforcement. In any case, the NIS Directive will impact the entire cyber security ecosystem and its implementation will likely require cooperation between the various stakeholders, including law enforcement and the judiciary.

A second initiative that is worth mentioning is the work of the Commission in the field of fraud related to non-cash payments. Currently the 2001 Framework Decision combating fraud and counterfeiting of non-cash means of payment is the main legal instrument. It contains a provision related to computer-related fraud – a typical cybercrime. The European Agenda on Security includes a review of this Framework Decision. The list of planned Commission initiatives consequently includes the proposal for a Directive combating Fraud and Counterfeiting of Non-Cash Means of Payment. The Roadmap published in May 2016 includes various references to Cybercrime and the challenges for investigations due to the transnational dimension of offences such as “phishing” and “pharming”.

Furthermore, the data protection reform work done by the Commission has a direct impact on the effectiveness of criminal investigations into cybercrime. The reform package includes the General Data Protection Regulation (GDPR, adopted in April 2016) and the Data Protection Directive for the police and criminal justice sector (DPD, adopted in December 2015). The package will enhance the exchange of data between law enforcement authorities and harmonize data protection requirements across the EU.

Lastly, although strictly speaking not a legislative development, two sets of Conclusions, which have been adopted by the Council of the European Union under the Dutch Presidency, should be noted here. The first set of Conclusions regard the establishment of a European Judicial Cybercrime Network supported by Eurojust, where judicial authorities (prosecutors, judges and in some cases police officials) can meet and discuss developments and challenges in the fight against cy-

bercrime, as well as exchange practical information and best practices. All with a view to facilitate and enhance cooperation between the competent judicial authorities. The second set of Council Conclusions is aimed at improving criminal justice in cyberspace and calls on the Commission to explore and where necessary develop a common EU approach for (1) cross-border access to electronic evidence for the purpose of criminal investigations, (2) cooperation between law enforcement authorities and cloud providers and (3) establishing jurisdiction in cyberspace.

### ■ UPDATE 2: COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

By July 2016, the number of ratifications/accessions to the 2001 Council of Europe Convention on Cybercrime increased to 49 countries, including nine non-members of the Council of Europe. Outside of Europe, Australia, Canada, the Dominican Republic, Japan, Mauritius, Panama, Sri Lanka, the United States, and most recently Israel, are listed as non-Member States that ratified the Convention. In the last few years, the Council of Europe invited several more non-members such as Mauritius, Morocco, Paraguay and Peru to accede to the Convention. But the fastest growing and most relevant economies outside of Europe, such as the BRIC countries (China, Russia, Brazil and India), with whom European law enforcement authorities frequently deal, have still not been invited to accede to the Convention. Involvement of those countries would be a significant advantage for international law enforcement cooperation.





## A3. POSITIVE CHANGES: A FINANCE INDUSTRY PERSPECTIVE

Significant progress in the fight against cybercrime has been made in recent years and this needs to be recognised and highlighted. To put the positive change into better perspective, it's helpful to look back five or ten years and reflect on what the finance sector faced at the time. The Russian Business Network (RBN) was the famous bulletproof hoster, and early banking Trojans such as WSNPoem/Zeus and Sinowal/Torpig stunned the European banking industry with their high success rates. For many European banks these were their first encounters with complex targeted online banking Trojans. This wave of cybercriminal activity came unexpectedly and thrust a number of changes into motion. The seeds of intelligence sharing communities were planted, and banks began to collaborate amongst themselves and with law enforcement. Nearly a decade later, many positive changes across various industries have impacted cybercriminal activity.

### ■ TECH INDUSTRY CHANGES

Significant positive change has happened amongst ISPs and hosters. Often a phone call or email to an abuse@ email address will result in fast takedown of phishing sites, drive-by malware, or fraudulent email accounts. This is in contrast to a decade ago, when such takedowns were more difficult, often requiring a formal legal process.

Tech companies are becoming proactive against crime, with more collaborative investigations and takedowns together with law enforcement. Europol's EC3 is a prime example,

with numerous botnet takedowns executed together with Microsoft and other tech companies in recent years. These voluntary acts of collaboration didn't happen as easily in the past.

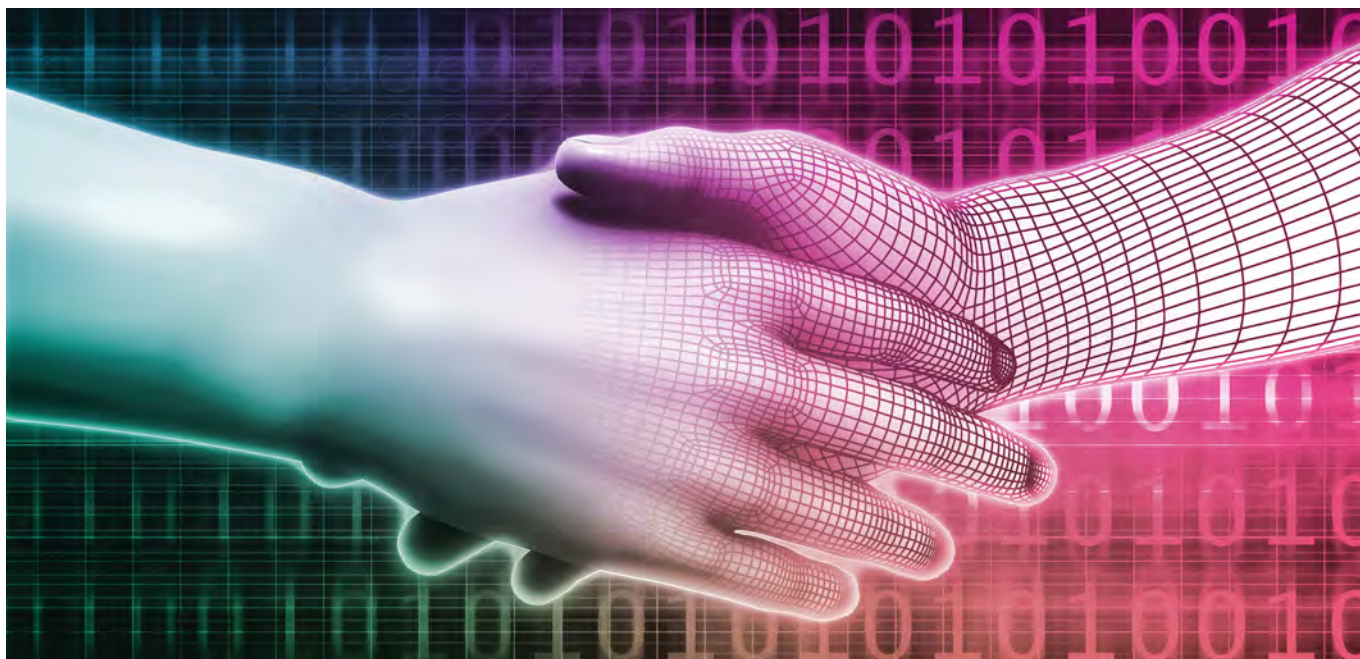
Tech companies are taking more responsibility for the security of their products. Platforms are becoming locked down by default with a trend towards controlled app stores for software distribution.

Providers are taking more responsibility for the security and health of their own networks and services. ISPs are actively detecting and filtering DDoS attacks, implementing standards such as BCP38 to reduce IP spoofing, detecting fraudulent logins, and other malicious activity.

### ■ FINANCE INDUSTRY CHANGES

Financial institutions have made many positive changes to combat criminal activity with payments and funds transfers. They are sharing more threat intelligence information between themselves, with law enforcement, and with tech industry partners. A number of inter-bank information sharing communities exist today. Some operate at a regional level within a country, others operate at an international level. Banks still need to be conscious of what they can legally share within their regulatory framework, and regulators and legislators are working to make changes that improve the ability to share information to protect clients and citizens.

Many of the current intelligence sharing groups started out of necessity, or grew out of early industry crisis meetings. The focus was to protect customers, help banks detect and stop fraudulent activity, and to help law enforcement obtain the evidence needed for the successful arrest and prosecution of criminals.



Other positive changes across the finance industry have been a trend towards two factor authentication (2FA) or additional authentication for unusual payments. Banks are detecting anomalies indicative of malware infection or fraud and reaching out to inform clients. A decade ago, banks did not consider this to be within their scope of responsibility.

Among banking staff, there is an increased awareness and understanding of criminal activity. Client relationship managers are more vigilant and suspicious of activity. They are challenging suspicious payments, and reconfirming payment orders received through less secure channels.

## ■ GOVERNMENT AND LAW ENFORCEMENT CHANGES

A number of positive changes have been happening within government and law enforcement. Locally and internationally, law enforcement agencies are finding new ways to efficiently collaborate on investigations involving the internet across borders and jurisdictions. Agencies are not relying solely on formal processes like MLATs to exchange intelligence information. An excellent example of international law enforcement collaboration is the EC3 J-CAT initiative which brings multiple agencies together in a single location with the purpose of investigating transnational cybercrimes.

There has also been significant change in the engagement with the private sector to share information and collaborate with private industry organisations. A good example is Europol's private sector Advisory Groups in Finance and Technology. Law enforcement have also gained a better understanding of private sector industries. They know what questions to ask, what data to request, and who to approach to best support ongoing investigations. They have a better understanding of technical capabilities available within the private sector, and how those

capabilities can be leveraged to fight crime.

More cybercrime related arrests are being made now than at any other point in the history of the internet. Publicity surrounding arrested cybercriminals has a strong deterrent effect. People participating in cybercriminal activities perceive a higher risk. Public awareness of successful arrests helps to reduce the number of criminals willing to take this risk. Compare this to a decade ago, when the risk of getting caught for internet based crime was perceived as low.

Public-private partnerships (PPPs) have also proliferated in the past decade. Governmental CERTs dedicated to assisting the private sector with cyber related problems have appeared. Some countries have even created dedicated "FinCerts" or financial CERTs which focus on finance sector issues. These public-private interfaces facilitate intelligence sharing and collaboration.

## ■ CHANGES WITH THE PUBLIC

The general public has also made positive progress in the past decade. People are more aware of the risks online and more suspicious of activity. Online fraud, social engineering, theft, and impersonation are better understood by the public today. There is improved recognition of phishing sites, spam mails, and scams.

There is more concern and interest in security and privacy. The public expects companies and suppliers to protect their personal data. The public is taking more steps to protect their own privacy online, managing the security of their electronic devices, and teaching children about online risks.

Media coverage of issues has also changed. Information about malicious attacks and new risks are actively and prominently

published by the media. Banks, governmental CERTs, law enforcement, and industry, can easily approach the media to issue warnings through the press. Social media channels facilitate rapid dissemination of threat information to the public.

## ■ CHANGES WITH CRIMINALS

The criminals themselves have also been changing. They have become more industrialised, forming an underground economy. They specialise in different services such as recruiting money mules, distributing malware, maintaining botnets, etc, and sell these services to other criminals. The technical expertise needed is decreasing as criminals move to a "Crime-as-a-Service" model, where cybercriminal activity is easier to execute, and support from the seller is provided.

The cost and complexity to develop and deploy malware has created more interest in social engineering attacks. Social engineering is simpler and often just as effective as technical exploitation. Consider the recent wave of business email compromise (BEC) and CEO fraud attacks targeting businesses, or the fake support phone calls and vishing attacks that target the public.

There is also an increased use of stolen data circulating in the Darknet or on data leak sites. This data contains credentials which can be used to gain unauthorised access to accounts such as email, online stores, social media sites, bank accounts, and other user accounts.

## ■ KEEPING AN EYE ON THE FUTURE

The positive changes outlined above have helped to slow (or even reduce) the growth of cybercriminal activity in many areas. For example, many banks have seen a decrease in banking Trojans and phishing attacks compared to half a decade ago. This decrease in activity is partly due to the combination of positive changes described in this appendix.

However, we cannot let these positive changes make us complacent in our fight against crime. Criminals are creative and always finding new ways to commit crimes. The global crime fighting community needs to evolve together with the criminals to keep society safe.

The amount of criminal activity can often seem overwhelming, and it sometimes feels like we are losing the battle. But remember how things were five or ten years ago, and how far we have come since then. A lot of amazing work has been done and has had a very positive effect. We need to keep making positive changes - it makes a difference.





- PO Box 90850  
2509 LW The Hague  
The Netherlands
- [www.europol.europa.eu](http://www.europol.europa.eu)  
[www.facebook.com/Europol](https://www.facebook.com/Europol)  
[www.youtube.com/EUROPOLtube](https://www.youtube.com/EUROPOLtube)  
Twitter: @Europol @EC3Europol

