IOCTA

INTERNET ORGANISED CRIME THREAT ASSESSMENT

[2019]

EUROPOL | EC3 European Cybercrime Centre

IOCTA
[2019]

EUROPOL

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019

www.europol.europa.eu

CONTENTS

FOREWORD

I am pleased to introduce the 2019 Internet Organised Crime Threat Assessment (IOCTA), Europol's annual presentation of the cybercrime threat landscape, highlighting the key developments, threats and trends, as seen by law enforcement authorities across Europe. As always, I extend my gratitude to the invaluable contributions from our colleagues within European law enforcement and to our partners in private industry and academia for their ongoing support and input.

This year's IOCTA demonstrates that while we must look ahead to anticipate what challenges new technologies, legislation, and criminal innovation may bring, we must not forget to look behind us. 'New' threats continue to emerge from vulnerabilities in established processes and technologies. Moreover, the longevity of cyber threats is clear, as many long-standing and established *modi operandi* persist, despite our best efforts. Some threats of yesterday remain relevant today and will continue to challenge us tomorrow.

Ransomware maintains its reign as the most widespread and financially damaging form of cyber-attack, while criminals continue to defraud e-commerce and attack the financial sector. Criminals target and exploit vulnerable minors across the globe. All of these crimes seriously impact the physical, financial and psychological safety, security and stability of our society and require a coherent and coordinated response by law enforcement.

Cybercrime continues to mature and become more audacious, shifting its focus to larger and more profitable targets. To tackle it, law enforcement must be equally audacious in order to meet the challenge head-on.

To do so, however, law enforcement needs the knowledge, tools and legislation required to do so quickly and effectively. As criminals adapt, law enforcement and legislators must also innovate in order to stay ahead, and seek to capitalise on new and developing technologies. This in turn requires training to produce the specialised capabilities required to investigate technically challenging or complex cybercrimes, such as those involving the abuse of cryptocurrencies or the dark web.

Europol is addressing these challenges with its Strategy 2020+. Our agency is at the forefront of law enforcement innovation and acts as a knowledge platform for the provision of EU policing solutions in relation to encryption, cryptocurrencies and other issues. In doing so, we expand the toolbox available to law enforcement officers across Europe and beyond, increasing their technical and forensic capabilities. The European Cybercrime Centre (EC3) at Europol is the first port of call for cybercrime investigators.

This only enforces the need for greater cooperation and collaboration with the private sector and academia, with whom law enforcement shares the responsibility for fighting cybercrime, and with the policy-makers who shape our society.

The IOCTA continues to celebrate the many successes of law enforcement in the fight against cybercrime, and the feats that can be achieved from the synergistic relationships with its partners in both the public and private sector. I have no doubt that such relationships will continue to go from strength to strength, but their full potential can only be realised under the right legislative and budgetary conditions. We can look forward to reporting further successes in the years to come.

Catherine De Bolle
Executive Director of Europol

ABBREVIATIONS

AMLD 5 5th EU Anti-Money Laundering Directive

APT Advanced Persistent Threat

ATM Automated Teller Machine

BEC Business Email Compromise

C2C Criminal to Criminal

CERT Computer Emergency Response Team

CNP Card Not Present

CPU Central Processing Unit

CSE Child Sexual Exploitation

CSEM Child Sexual Exploitation Material

DDoS Distributed Denial of Service

DMARC Domain-based message authentication, reporting and conformance

EBA European Banking Authority

EBF European Banking Federation

EC3 Europol's European Cybercrime Centre

EMAS Europol Malware Analysis Solution

EMMA European Money Mule Actions

EMPACT European Multidisciplinary Platform Against Criminal Threats

EMV Europay, MasterCard and Visa

EPC European Payment Council

FIOD Dutch Fiscal Information and Investigative Service

GDPR General Data Protection Regulation

GPU Graphics Processing Unit

I2P Invisible Internet Project

ICANN Internet Corporation for Assigned Names and Numbers

IOCTA Internet Organised Crime Threat Assessment

IP Internet Protocol

IS Islamic State

JIT Joint Investigation Team

LDCA Live Distant Child Abuse

NCPF Non-Cash Payment Fraud

OCG Organised Crime Group

OSP Online Service Provider

PNR Passenger Name Record

RDP Remote Desktop Protocols

RWE Right-wing extremism

SGEM Self-Generated Explicit Material

SWIFT Society for Worldwide Interbank Financial Telecommunications

THB Trafficking in Human Beings

Tor The Onion Router

URL Uniform Resource Locator

VIDTF Victim Identification Task Force

VPN Virtual Private Network

EXECUTIVE SUMMARY

This annual assessment of the cybercrime threat landscape highlights the persistence and tenacity of a number of key threats. In all areas, we see how most of the main threats have been reported previously, albeit with variations in terms of volumes, targets and level of sophistication. This is not for lack of action on the side of the public and the private sector. Rather, this persistence demonstrates the complexity of countering cybercrime and the perspective that criminals only innovate when existing *modi operandi* have become unsuccessful. Therefore, while much focus in contemporary parlance is on the potential impact of future technological developments on cybercrime, such as Artificial Intelligence, we must approach cybercrime in a holistic sense. Countering cybercrime is as much about its present forms as it is about future projections*. New threats do not only arise from new technologies but, as is often demonstrated, come from known vulnerabilities in existing technologies.

This year's IOCTA demonstrates that for all cybercrime, data remains the key element, both from a crime perspective and from an investigative perspective. Criminals target data for their crimes, making data security with respect to organisations and awareness of consumers all the more important. Data security has taken centre stage even more after the implementation of the General Data Protection Regulation (GDPR). While it is too early for a full assessment, the response to data breaches — through media headlines and high fines — will potentially have a positive impact and lead to enhanced data security.

Ransomware remains the top threat in this year's IOCTA. Even though we have witnessed a decline in the overall volume of ransomware attacks, those that do take place are more targeted, more profitable and cause greater economic damage. As long as ransomware provides a relatively easy income for cybercriminals, and continues to cause significant damage and financial losses, it is likely to remain the top cybercrime threat. In the area of payment fraud, we continue to identify card not present (CNP) fraud as the main priority — as reported by law enforcement and confirmed by private sector reporting in the payment fraud arena. Criminals primarily manage to carry out CNP fraud through data gathered from data security breaches and social engineering.

Data returns to the discussion of other threats as well. A crucial priority reported by both Member States and the private industry is Business Email Compromise (BEC). While BEC is not new, it is evolving. This scam exploits the way corporations do business, taking advantage of segregated corporate structures, and internal gaps in payment verification processes. Such attacks vary by the degree of technical tools used. Some attacks can successfully employ only social engineering, while others deploy technical measures such as malware and network intrusion. In both cases, data is again at the centre of the crime scene.

While using ransomware to deny an organisation access to its own data may be the primary threat in this year's report, denying others access to that organisation's data or services is another significant threat. Distributed Denial of Service (DDoS) Attacks are yet another data-focused threat to cope with. Of all the motivations behind such attacks, those with an extortion element were overwhelmingly the most prevalent.

Whereas criminals require data for most of their crimes, law enforcement needs access to relevant data for their investigations. Indeed, the ability of law enforcement agencies to access the data needed to conduct criminal investigations is an increasing challenge. This is a result of technological developments, such as the enhanced use of encryption which criminals abuse to obfuscate their tracks, as well as cryptocurrencies

* These were usefully explored in Europol's recent publication "Do Criminals Dream of Electric Sheep? How Technology Shapes the Future of Crime and Law Enforcement" (https://www.europol.europa.eu/publications-documents/do-criminals-dream-of-electric-sheep-how-technology-shapes-future-of-crime-and-law-enforcement)

to hide their illicit earnings. However, inaccessibility of relevant data also comes due to legislative barriers or shortcomings, which we must overcome to enhance cross-border access to electronic evidence and the effectiveness of public-private cooperation through facilitated information exchange.

These barriers are often related to the principle of territoriality, which sets limits to the scope of jurisdiction and to the investigative powers which law enforcement and judiciary have at their disposal under their national law. As a result, the tools in the hands of investigators and prosecutors do not correspond to what would be needed to deal with data flows, for which questions of territoriality are of no relevance.

At the same time, there is also the ever-increasing challenge of data overload, as we can see in the area of online Child Sexual Exploitation (CSE). The amount of Child Sexual Exploitation Material (CSEM) detected online by law enforcement and the private sector continues to increase. This increase puts a considerable strain on law enforcement resources and requires a response to ensure that the volume of data does not impede law enforcement authorities' responsibility to conduct criminal investigations into CSEM. This is one example where innovation and law enforcement agencies must innovate to find ways to digest the increasing volumes of data coming in.

Related challenges also demonstrate how the evolution of existing threats is often a result of scale. Self-generated explicit material (SGEM) is more and more common, driven by a growing number of minors with access to high-quality smartphones. On top of this growing access, a lack of awareness about the risks on the side of minors exacerbates the problem. At Europol, through the organisation of the first European Youth Day, we have specifically aimed to enhance minors' awareness about online risks. The online solicitation of children for sexual purposes remains a serious threat, with a largely unchanged *modus operandi* in terms of grooming and sexual coercion, demonstrating again the tenacity of existing forms of cybercrime.

Access to data allows criminals to carry out various forms of fraud. Such data is also available on the dark web, which is often a key enabler of many other forms of illegal activity. Within this report, it once again becomes evident how the dark web underpins many crime areas and how investigators highlight the phenomenon as a priority.

Moreover, as the dark web evolves, it has become a threat in its own right, and not only as a medium for the sale of illicit commodities such as drugs, firearms or compromised data. The impact of law enforcement action in this arena is palpable as the environment remains in a state of flux. As a result, more coordinated investigation and prevention actions targeting the phenomenon are required, demonstrating the ability of law enforcement to have a lasting impact and deterring users from illicit activity on the dark web.

As more and more companies outsource areas of their business, such as moving more infrastructure to third-party cloud services, we expect to see a growth in supply chain attacks, and the evolution of such attacks to become increasingly complex. This develops a clear interdependency between organisations and leads to the necessity of having a higher level of cybersecurity across the spectrum to ensure the minimisation of successful cybercrime attacks. When an attack does occur, being prepared to respond rapidly is essential. Therefore, building on important steps already taken, we need to continue to enhance synergies between the network and information security sector and the cyber law enforcement authorities, in order to improve the overall cyber resilience of the entire cybersecurity ecosystem.

The IOCTA is a resource for the intelligence-led deployment of law enforcement resources. It also contains recommendations for policy-makers and for the orientation of further research and prevention measures. The diversity and complexity of online threats is such the full range of public and private actors must work together to make progress in prevention, legislation, enforcement and prosecution. All of these elements are necessary in order to disrupt organised crime activity and reduce the online threat to businesses, governments and, above all, EU citizens.

KEY FINDINGS #1

CYBER-DEPENDENT CRIME

- While ransomware remains the top threat in this report, the overall volume of ransomware attacks has declined as attackers focus on fewer but more profitable targets and greater economic damage.
- Phishing and vulnerable remote desktop protocols (RDPs) are the key primary malware infection vectors.
- Data remains a key target, commodity and enabler for cybercrime.
- Following the increase of destructive ransomware, such as the Germanwiper attacks of 2019, there is a growing concern within organisations over attacks of sabotage.
- Continuous efforts are needed to further synergise the network and information security sector and the cyber law enforcement authorities to improve the overall cyber resilience and cybersecurity.

CHILD SEXUAL EXPLOITATION ONLINE

- The amount of CSEM detected online by law enforcement and the private sector continues to increase, putting considerable strain on law enforcement resources.
- The online solicitation of children for sexual purposes remains a serious threat with a largely unchanged *modus operandi*.
- SGEM is more and more common, driven by growing access of minors to high quality smartphones and a lack of awareness of the risks.
- Although commercial CSE remains limited, live distant child abuse (LDCA) is a notable exception to this.

PAYMENT FRAUD

- CNP fraud continues to be the main priority within payment fraud and continues to be a facilitator for other forms of illegal activity.
- Skimming continues to evolve with criminals continuously adapting to new security measures.
- Jackpotting attacks are becoming more accessible and successful.

THE CRIMINAL ABUSE OF THE DARK WEB

- The dark web remains the key online enabler for trade in an extensive range of criminal products and services and a priority threat for law enforcement.
- Recent coordinated law enforcement activities, combined with extensive Distributed Denial of Service (DDoS) attacks have generated distrust in The onion router (Tor) environment. While there is evidence administrators are now exploring alternatives, it seems the user-friendliness, existing market variety and customer-base on Tor makes a full migration to new platforms unlikely just yet.
- There are increases in single-vendor shops and smaller fragmented markets on Tor, including those catering for specific languages. Some organised crime groups (OCGs) are also fragmenting their business over a range of online monikers and marketplaces, therefore presenting further challenges for law enforcement.
- Encrypted communication applications enhance single-vendor trade on the dark web, helping direct users to services and enabling closed communications. Although there is no evidence of a full business migration, there is a risk the group functions could become increasingly used to support illicit trade.

THE CONVERGENCE OF CYBER AND TERRORISM

- The wide array of online service providers (OSPs) exploited by terrorist groups presents a significant challenge for disruption efforts.
- Terrorist groups are often early adopters of new technologies, exploiting emerging platforms for their online communication and distribution strategies.
- With sufficient planning and support from sympathetic online communities, terrorist attacks can rapidly turn viral, before OSPs and law enforcement can respond.

CROSS-CUTTING CRIME FACTORS

- Phishing remains an important tool in the arsenal of cybercriminals for both cyber-dependent crime and non-cash payment fraud (NCPF).
- While cryptocurrencies continue to facilitate cybercrime, hackers and fraudsters now routinely target crypto-assets and enterprises.

RECOMMENDATIONS

#2

The following recommendations respond to the Key Findings found above in chapter 1 and the threats described throughout this report. These recommendations are intended to support law enforcement, regulators and policy-makers in their decision-making processes. Crucially they are of fundamental importance in informing the respective European Multidisciplinary Platform Against Criminal Threats (EMPACT) priorities when setting the actions for the 2020 Operational Action Plans for the three sub-areas of the EMPACT priority in cybercrime: cybercrime attacks against information systems, NCPF, and CSE online. These recommendations should also help inform research and innovation efforts and programmes at national and EU level.

CYBER-DEPENDENT CRIME

Successfully tackling major crime-as-a-service providers can have a clear and lasting impact. Law enforcement should continue focusing its concerted efforts into tackling such service providers.

Enhanced cooperation and improved data sharing between law enforcement, computer security incident response teams and private partners will be the key to tackling complex cyberattacks, and allow the private sector to take the necessary preventative security measures to protect themselves and their customers.

In response to major cross-border cyber-attacks, all cooperation channels should be explored, including Europol's and Eurojust's support capabilities as well as legal instruments designed for closer cross-border cooperation (such as Joint investigation Teams (JITs) and spontaneous exchange of information) in order to share resources and coordinate.

Further enhance the collaboration between the network and information security sector and the cyber law enforcement authorities by involving the latter in cyber resilience-related activities such as cyber simulation exercises.

Low-level cybercrimes such as website defacement should be seen as an opportunity for law enforcement to intervene in the criminal career path of young, developing cybercriminals.

CHILD SEXUAL EXPLOITATION ONLINE

Coordinated action with the private sector and the deployment of new technology, including Artificial Intelligence, could help reduce the production and distribution of online CSEM, facilitate investigations, and assist with the processing of the massive data volumes associated with CSEM cases.

A structural educational campaign across Europe to deliver a consistent high-quality message aimed at children about online risks is of the utmost importance to reduce the risks derived from SGEM such as sexual coercion and extortion.

As much CSEM, particularly that arising from LDCA, originates from developing countries, it is essential that EU law enforcement continues to cooperate with, and support the investigations of, law enforcement in these jurisdictions.

Fighting CSE is a joint effort between law enforcement and the private sector and a common platform is needed to coordinate efforts and prevent a fragmented approach and duplicated efforts.

To prevent child sex offenders from travelling to third countries to sexually abuse children, EU law enforcement should make use of passenger name record (PNR) data accessible through the Travel Intelligence team within Europol.

PAYMENT FRAUD

Cooperation between the public and the private sector as well as within the sectors is crucial to come to fruitful results. To this point, speedy and more direct access to and exchange of information from the private sector is essential for Europol and its partners.

Organisations must ensure they train their employees and make their customers aware of how they can detect social engineering and other scams.

THE CRIMINAL ABUSE OF THE DARK WEB

More coordinated investigation and prevention actions targeting the phenomenon are required, demonstrating the ability of law enforcement and deterring users from illicit activity on the dark web.

The ability to maintain an accurate real-time information position is necessary to enable law enforcement efforts to tackle the dark web. The capability needs to enable the identification, categorisation, collection and advanced analytical processing, including machine learning and AI.

An EU-wide framework is required to enable judicial authorities to take the first steps to attribute a case to a country where no initial link is apparent due to anonymity issues, thereby preventing any country from assuming jurisdiction initiating an investigation.

Improved coordination and standardisation of undercover online investigations are required to de-conflict dark web investigations and address the disparity in capabilities across the EU.

THE CONVERGENCE OF CYBER AND TERRORISM

Limiting the ability of terrorists to carry out transnational attacks by disrupting their flow of propaganda and attributing online terrorism-related offences requires continued and heightened counterterrorism cooperation and information sharing across law enforcement authorities, as well as with the private sector.

Any effective measure to counter terrorist groups' online propaganda and recruitment operations entails addressing the whole range of abused OSPs, especially start-ups and smaller platforms with limited capacity for response.

Cross-platform collaboration and a multi-stakeholder crisis response protocol on terrorist content online would be essential to crisis management the aftermath of a terrorist attack.

A better understanding of new and emerging technologies is a priority for law enforcement practitioners. Upcoming policy debates and legislative developments should take into account the features of these technologies in order to devise an effective strategy to prevent further abuse.

CROSS-CUTTING CRIME FACTORS

Law enforcement and the judiciary must continue to develop, share and propagate knowledge on how to recognise, track, trace, seize and recover cryptocurrency assets.

Law enforcement must continue to build trust-based relationships with cryptocurrency-related businesses, academia, and other relevant private sector entities, to more effectively tackle issues posed by cryptocurrencies during investigations.

Despite the gradual implementation of the Directive (EU) 2018/843 of the European Parliament and of the Council[1] (known as AMLD 5, 5th Anti-Money Laundering Directive) across the EU, investigators should be vigilant concerning emerging cryptocurrency conversion and cash-out opportunities and share any new information with Europol.

INTRODUCTION

#3

The European Union Serious and Organised Crime Threat Assessment (SOCTA) 2017 identified cybercrime as one of the 10 priorities in the fight against organised and serious international crime[2]. This overarching category includes cybercrime attacks against information systems, NCPF, CSE online and other enabling criminal activities.

Aim

The IOCTA aims to inform decision-makers at strategic, policy and tactical levels in the fight against cybercrime, to direct the operational focus for EU law enforcement. The 2019 IOCTA will contribute to the setting of priorities for the 2020 EMPACT operational action plan in the three above-mentioned sub-areas of the EMPACT priority of cybercrime, as well as cross-cutting crime enablers.

Scope

The 2019 IOCTA focuses on the trends and developments pertinent to the above-mentioned priority crime areas. In addition to this, the report will discuss other cross-cutting factors that influence or impact the cybercrime ecosystem, such as criminal abuse of cryptocurrencies and social engineering.

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. Furthermore, it draws on contributions from strategic partners in private industry and academia to support or contrast this perspective. The report seeks to highlight future risks and emerging threats and provides recommendations to align and strengthen the joint efforts of EU law enforcement and its partners in preventing and fighting cybercrime.

Methodology

The 2019 IOCTA was drafted by a team of Europol analysts and specialists drawing predominantly on contributions from 26 Member States and European third-party members, the European Union Cybercrime Taskforce, Eurojust, Europol's Analysis Projects Cyborg, Dark Web, Terminal, Twins and the Cyber Intelligence Team of Europol's European Cybercrime Centre (EC3), via structured surveys and feedback sessions. This has been enhanced with open source research and input from the private sector, namely EC3's Advisory Groups on Financial Services, Internet Security and Communication Providers. These contributions have been essential to the production of the report.

Acknowledgements

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

#4

CRIME PRIORITY

cyber-dependent crime

Cyber-dependent crime can be defined as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). Such crimes are typically directed at computers, networks or other ICT resources. In essence, without the internet criminals could not commit these crimes[3]. It includes such activity as the creation and spread of malware, hacking to steal sensitive personal or industry data and denial of service attacks to cause financial and/or reputational damage.

4.1 » KEY FINDINGS

- While ransomware remains the top threat in this report, the overall volume of ransomware attacks has declined as attackers focus on fewer, but more profitable targets, and greater economic damage.
- Phishing and vulnerable RDPs are the key primary malware infection vectors.
- Data remains a key target, commodity and enabler for cybercrime.
- Following the increase of destructive ransomware, such as the Germanwiper attacks of 2019, there is a growing concern within organisations over attacks of sabotage.
- Continuous efforts are needed to further synergise the network and information security sector and the cyber law enforcement authorities to improve the overall cyber resilience and cybersecurity.

4.2 » RANSOMWARE

Ransomware evolves as it remains the most prominent threat

The majority of private sector reporting indicates that there was a notable decline in ransomware attacks throughout 2018[4]. This may be attributable to a number of factors: an increased awareness among potential victims — fuelled by industry and law enforcement initiatives to mitigate the threat (such as NoMoreRansom); the increasing use of mobile devices by consumers (with most ransomware targeting Windows-based devices); and a decline in the use of exploit kits (which were a key delivery method).

Despite this, the number of victims is still high, and ransomware clearly and overwhelmingly retains its position as the top cyber threat faced by European cybercrime investigators, the second most prominent threat for the private sector[5], and one of the most common samples submitted to the Europol Malware Analysis Solution (EMAS). Moreover, as long as ransomware provides a relatively easy income for cybercriminals, and continues to cause significant damage and financial losses, it is likely to remain the top cybercrime threat.

Investigators cited over 25 individual identifiable families of ransomware, targeting citizens, and private and public entities within Europe. Several of these featured more prominently in law enforcement reporting, including the various versions of *Dharma/CrySiS, ACCDFISA, GlobeImposter,* and *Rapid*. GandCrab, Locky, and Curve-Tor-Bitcoin-Locker also featured prominently in EMAS submissions. While the Rapid ransomware only surfaced in January 2018, the other families, and many of the less frequently reported families have been in circulation for several years, highlighting the persistence of these threats once released into the wild.

Attacks shift to more valuable targets

Last year law enforcement began to see the shift from untargeted, scattergun attacks affecting citizen and businesses alike, to more targeted attacks. Both European law enforcement and Europol's private sector partners confirm a diminishing number of ransomware attacks targeting individual

citizens, and more attacks specifically engineered towards individual private and public sectors entities. This is also a likely explanation for the apparent decline in the overall volume of attacks.

While targeting specific companies is potentially more labour-intensive and technically challenging, requiring the attackers to follow the cyber kill-chain[6], it also means that attackers are able to pitch the ransom for decrypting the victim's files based on the victim's perceived ability to pay. For example, there are cases where a company's encrypted files have been ransomed for over EUR 1 million.

Remote desktop protocols and emails remain the key infection methods

Such targeted cyber-attacks require specific tactics to infect the target network. The trend in the use of social engineering and targeted phishing emails as a primary infection method continues from last year. Some reports highlight that as many as 65 % of groups rely on spear-phishing as their primary infection vector[7]. The use of vulnerable RDPs also continues to grow. Attackers can either brute force access to a target's RDP or often can buy access to the target network on a criminal forum. In this area, the importance of patching once again becomes apparent. In May 2019, for example, Microsoft published the security vulnerability CVE-2019-0708, named sometime later as BlueKeep.

An attacker can exploit this vulnerability by connecting via RDP to the target machine and sending specifically crafted requests. This particular vulnerability does not require either victim interaction nor user authentication, allowing any attacker who succeeds in exploiting the vulnerability to execute arbitrary code on the compromised machine. The exploit works completely filelessly, providing full control of a remote system without having to deploy any malware. In addition, it also does not require an active session on the target.

Almost one million devices may be vulnerable to this exploit[8].

case study

Ransomware attacks against local and state government agencies in the United States:

Most visible ransomware attacks in 2019 were those against local governments, specifically in the United States. This trend commenced earlier. In 2018, a ransomware attack paralysed the city of Atlanta for several weeks and this only proved to be the tip of the iceberg. After that, already more than half a dozen cities and public services across the US had fallen victim to ransomware, on a near-monthly basis[11]. Other examples of 2019 include Baltimore and Florida. The Governor of Louisiana even declared a state of emergency after another local ransomware attack[12]. According to an extensive historical overview of ransomware attacks targeting local and state governments, based on public disclosures, every state in the US has been hit with an attack with the exception of Delaware and Kentucky[13]. Whether this trend will also become a threat to Member States is something to be seen, but the experiences in the US definitely function as a warning.

devices will likely remain unpatched, allowing cybercriminals to include the BlueKeep vulnerability exploitation attack in their arsenal to be used with other well-known malicious software, like ransomware inside private and business networks.

While their use continues and new ones continue to be developed, exploit kits did not feature in law enforcement reporting this year.

Sabotage: a growing fear for the private sector

Another key development in the wake of attacks such as *NotPetya*, is that many private sector companies now fear not only 'conventional' ransomware attacks, but also destructive cyber-attacks; acts of sabotage which would permanently erase or otherwise irreversibly damage company data. Such concerns are particularly valid given the conclusion that cyberattacks designed to cause damage doubled during the first six months of 2019, of those attacked 50 % are in the manufacturing sector[9]. Whereas historically speaking destructive malware was predominantly associated with nation-state actors, since late 2018 cybercriminals are also increasingly incorporating 'wiper elements' as part of their attacks, through new strains of malware. GermanWiper surfaced during the summer of 2019 as a new type of ransomware which rather than encrypting the victim's files, rewrites the content resulting in the permanent destruction of the victim's data[10]. Without back-ups, victims are most likely to have permanently lose their data.

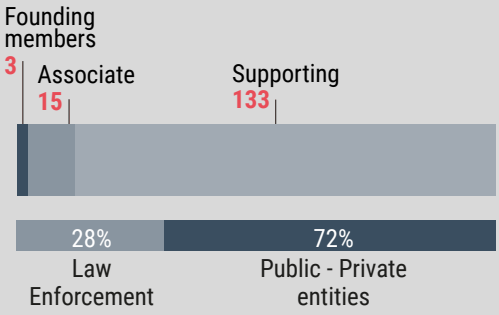
case study

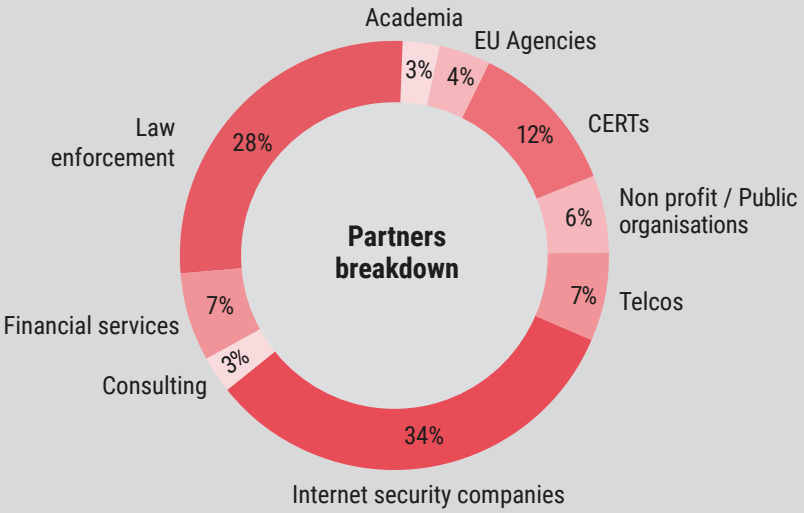
In January 2019, authorities from several US agencies, along with police and prosecutors from Belgium and Ukraine as part of a JIT assisted by Eurojust, seized the xDedic marketplace in an operation supported by the German Federal Criminal Police Office and Europol. Law enforcement seized the servers and domain names of the xDedic marketplace, and the website's criminal activities stopped.

The xDedic marketplace sold access to compromised computers worldwide as well as personal data and operated on both the clear and dark web. Users of xDedic could search for compromised computer credentials by criteria, such as price, geographic location, and operating system. The victims came from all around the globe and a variety of industries, including local, state, and federal government infrastructure, hospitals, emergency services, major metropolitan transit authorities, accounting and law firms, pension funds, and universities. Authorities believe the website facilitated more than EUR 60 million in fraud.

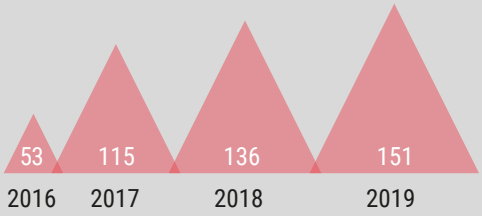
NO MORE RANSOM!

Partners 151

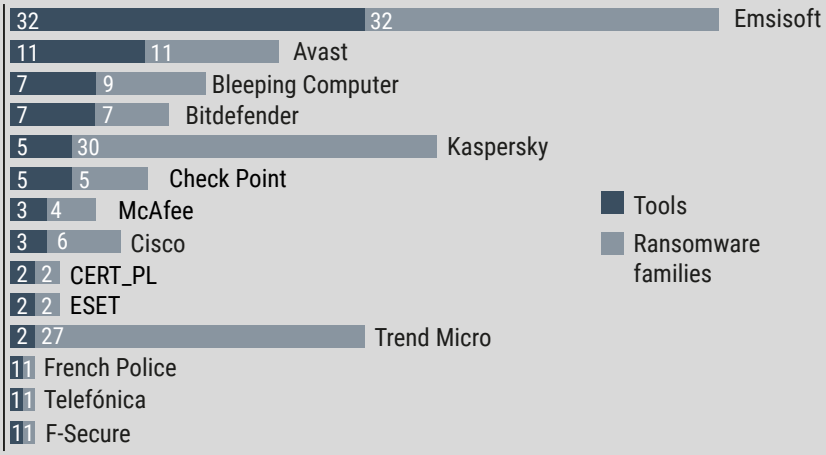




Partners annual growth



Tools 82



109
ransomware families covered

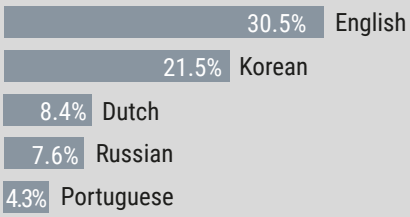
200K
victims helped

$108M
criminal profit prevented

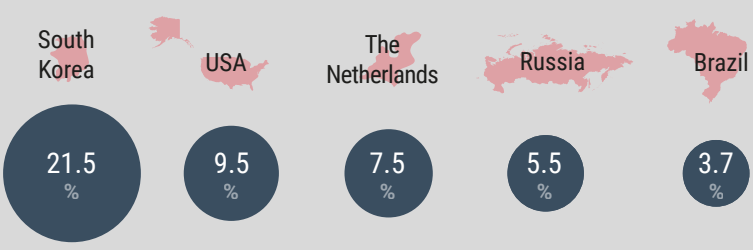
188
countries have accessed the NMR portal

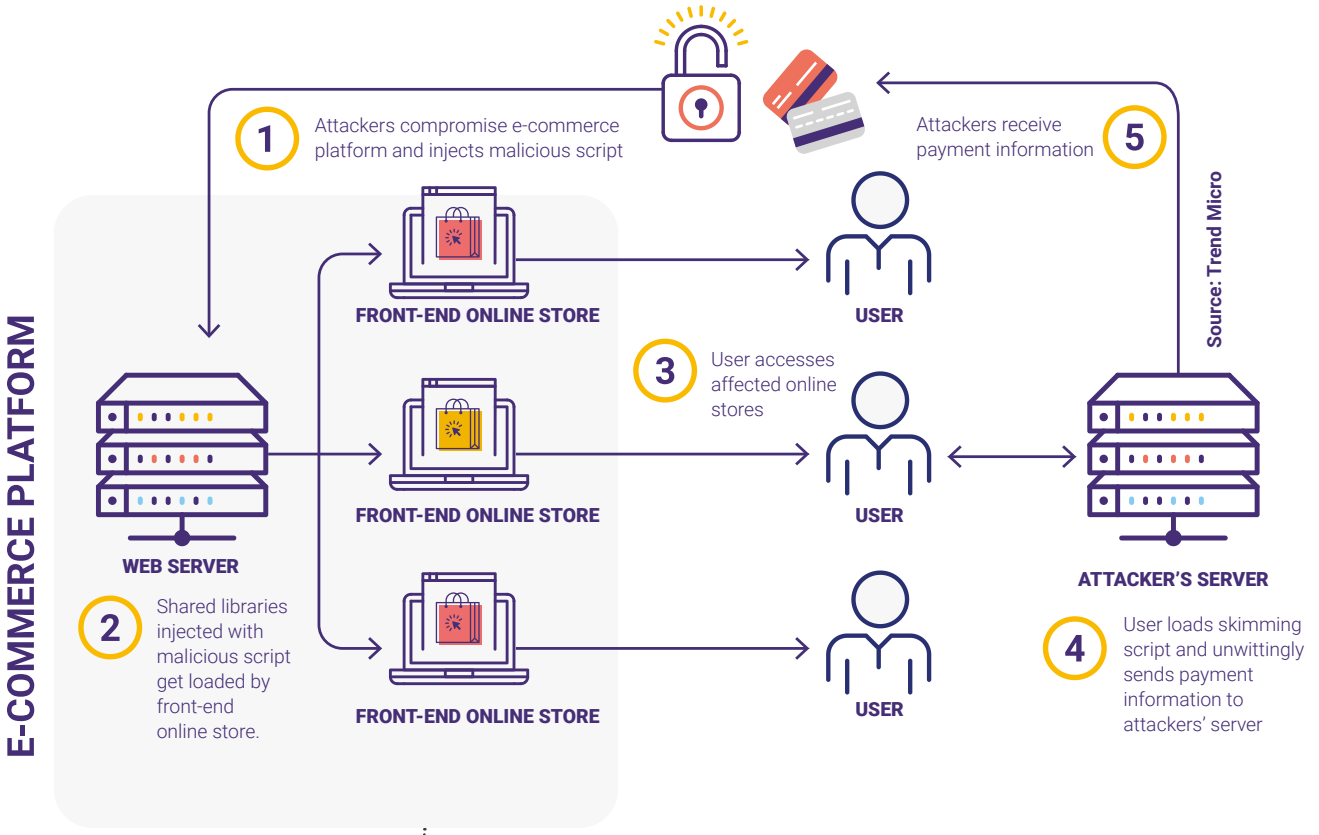
Language & countries

Top 5 languages among 36 available



Top 5 countries of traffic





criminal case study

The Magecart group

The Magecart group, which actually comprises at least six distinct groups operating independently, has been active since approximately 2015. It came to notoriety throughout 2018 when a number of prominent companies suffered massive data breaches. One breach alone resulted in the compromise of over 380 000 credit card details and a fine for the company of over GBP 183 million under GDPR[14].

The groups share a common *modus operandi* — attacking shopping cart platforms or third-party services used by e-commerce websites by injecting code that allows them to skim sensitive customer data; a technique known as formjacking.

The above illustration demonstrates the process of how the crime takes place step by step, from its inception until the attackers receive payment information.

4.3 » DATA COMPROMISE

Compromised data continues to fuel the cybercrime engine

After ransomware, the compromise of data represents the second-most prominent cyber-threat tackled by European cybercrime investigators. This most frequently relates to the illegal acquisition of financial data, such as credit card information, online banking credentials or cryptocurrency wallets, through means such as phishing, data breaches and information gathering malware. Such data is easily monetisable, either through its sale on the digital underground or direct use in fraud. This is also a major source to facilitate CNP fraud (see chapter 6).

Second to financial data, is personal data and other login credentials. While not directly monetisable (other than through its sale), such data is potentially much more valuable, particularly to the more sophisticated cybercrime gangs who may have the capability to best exploit it. Criminals can use the data to facilitate other targeted cyberattacks such as spear phishing, CEO/BEC fraud, account takeover, business process compromise and other frauds, any of which could yield much more significant criminal profits.

Most data breaches yield a variety of data types. One of the largest data breaches of 2018 was hotel giant Marriot International. Over 300 million records were disclosed. These records included data such as names, postal addresses, phone numbers, dates of birth, gender, email addresses, passport numbers and credit card data. Much of the data was encrypted however.

> As hardware and software manufacturing supply chains become ever more extended, the cybersecurity of some extremely important targets will become dependent upon the weakest link in this chain. Due diligence and sound engineering processes must be a part of any Secure Development Life Cycle.
>
> – PROFESSOR ALAN WOODWARD, UNIVERSITY OF SURREY, UK

The growing threat from within

The threat from malicious insider activity is an increasing concern for financial institutions, according to Europol's private sector partners, some of whom rank insider threats as the third-most significant threat actors. The potential impact of such attacks made apparent by a number of attacks publicised in 2019, such as the attacks on US telecoms company AT&T, where insiders allegedly took bribes to unlock more than 2 million devices and planted malware on the company network[15].

The threat from such attacks is amplified where the malicious insider works for a third-party service provider, who may have access to the data of multiple companies and their customers. Such was the case with the Capital One breach, where a former employee of Amazon Web Services is suspected of accessing data belonging to 106 million Capital One customers stored on Amazon's Simple Storage Servers (S3)[16].

GDPR implemented but more time needed to evaluate impact

Closely connected to the crucial threat of data compromise is the implementation of the GDPR. Perhaps one of the most anticipated pieces of legislation of the last few years, one year after entering into effect, many stakeholders demonstrated a welcomed eagerness to take stock of the developments and to gauge the impact of the legislation. In terms of available figures, the International Association of Privacy Professionals (IAPP) appears to have developed one of the most comprehensive overviews of the numbers pertaining to the GDPR one-year anniversary.

Others describe how, despite the passage of a year, we are too early in the process to evaluate the impact of the legislation[17]. Yet, momentum is essential and some write '[i]n the absence of large headlines about closed investigations that result in enormous fines, one of the questions

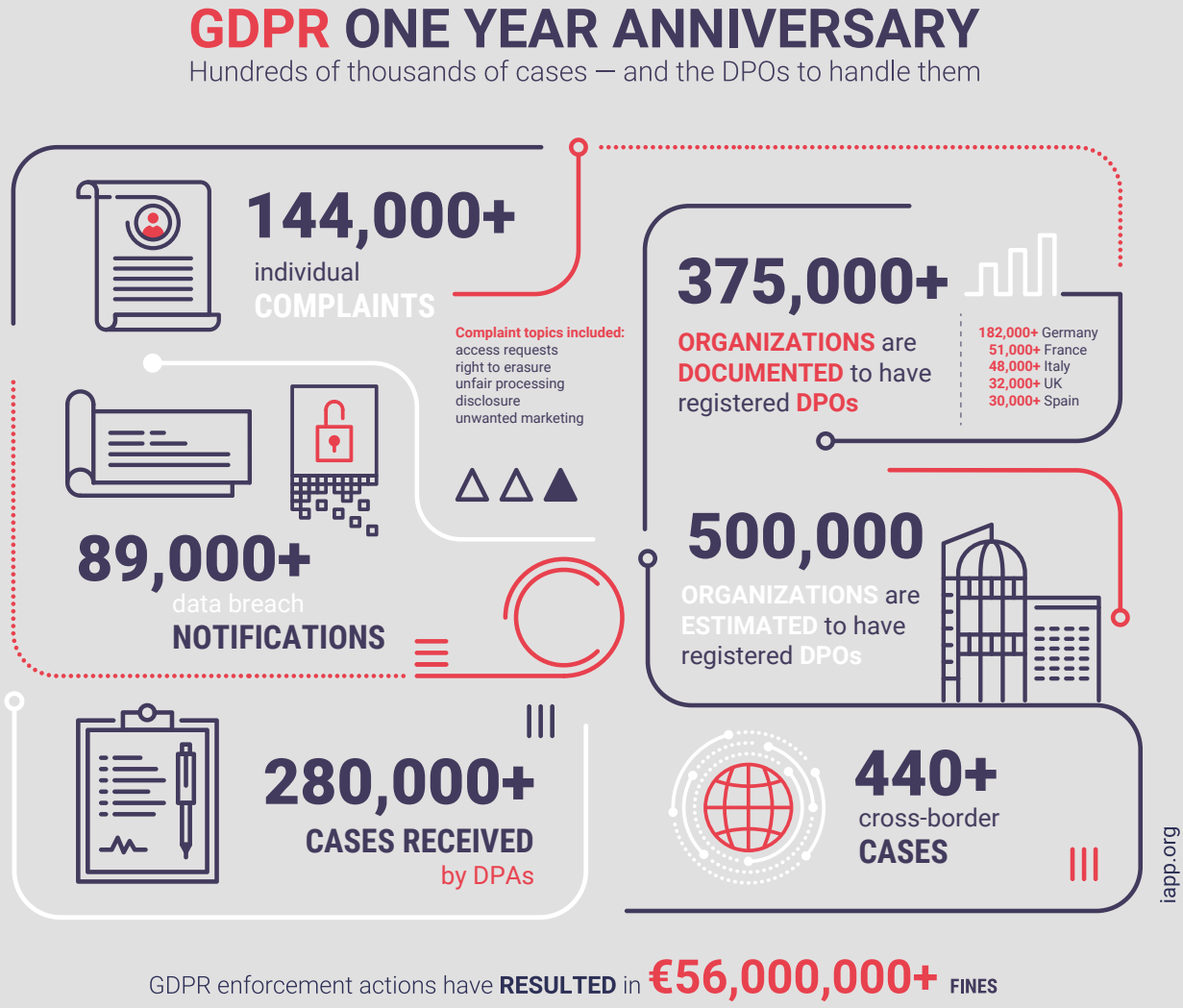
industry insight

Supply Chain Attacks

A clear and growing concern for Europol's private sector partners was attacks directed at them through the supply chain, i.e. the use of compromised third parties as a means to infiltrate their network. Often this will be suppliers of third-party software or hardware, but also other business services. Large companies may have a multitude of third-party suppliers, some with which they have a high degree of connectivity, each bringing its own risk. Such risks are similarly incurred when a larger company acquires a smaller company which may have lower cybersecurity maturity. Such was the case in the Marriot International breach.

Several partners have even indicated that supply chain attacks are considered to be the highest risk to their business. Some industry reporting indicate that supply chain attacks increased by 78 % in 2018[23].

Such attacks are becoming more complex, with compromised fourth or even fifth party suppliers exploited in multi-tier supply chain attacks[24]. Moreover, many companies are becoming increasingly reliant on third-party services such as the cloud.



criminal case study

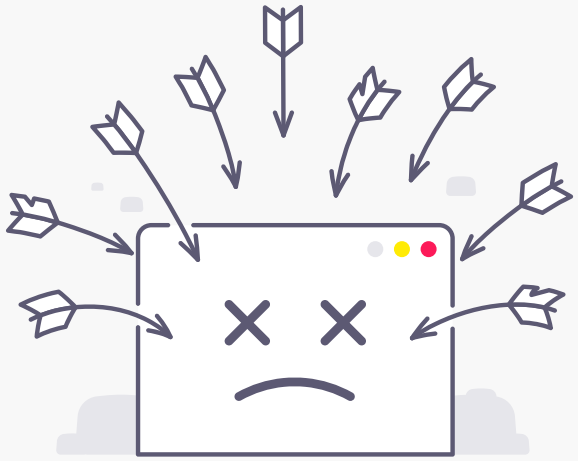
Operation ShadowHammer

In January 2019, Kaspersky Lab discovered that a server for a live software update tool for users of ASUS products had been compromised by attackers and that an estimated 500 000 Windows machines had received a compromised file that effectively acted as a backdoor to the devices for the attackers. The malicious file was signed with legitimate ASUS digital certificates to make it appear to be an authentic software update from the company.

However, the malware was designed to only activate on about 600 unique machines, based on their MAC addresses, indicating that despite the number of affected machines, the attack was extremely targeted[25].

about GDPR now is whether companies will become complacent and downscale their privacy programs[18]. At the time of its one-year anniversary, the largest fine issued — to Google — did not concern a data security breach, rather the French Data Protection Authority issued the fine because of the processing of data by the company.

After the passage of the one-year anniversary mark, however, at least two companies received a 'headline' fine. The United Kingdom's Information Commissioner's Office (ICO) issued its biggest penalties to date when it fined British Airways for GBP 183 million[19] and the Marriott for nearly GBP 100 million[20]. The fines are perceived as a wake-up call to improve means of data security on the side of companies that handle customer data. In this sense, the impact of such an action based on legislation such as GDPR could be significant; especially the public coverage of the development can lead to improved security practices. Previous research with regard to investment in cybersecurity demonstrates the value of incidents in terms of enhancing security practices of companies[21]. The magnitude of the fine combined with increasing public awareness of the impact of data compromise must act as a strong incentive for boards to closely examine their cybersecurity posture. At the same time, high fines could also backfire, as it could bring the potential for GDPR extortion back into the discussion[22].



criminal case study

Memcached amplification attacks[28]

2018 witnessed the two largest DDoS attacks seen to date, using a previously unknown amplification technique. Memcache is an open-source application that can be used to store small chunks of arbitrary data; its purpose to help websites and applications load content faster. Social networks and other content providers commonly use it.

By spoofing the targets IP address, exposed memcached-enabled servers can be used to mount a UDP-based reflection attack, with an amplification factor of over 50 000[29].

Such was the case in February of 2018, when two record breaking DDoS attacks of 1.35 terabytes per second and 1.7 terabytes per second were launched against attack against code depository GitHub, and an unnamed United States-based website respectively. Attacks in 2019, however, trumped these figures. At the start of 2019, Imperva's DDoS Protection Service mitigated a DDoS attack against one of its clients which crossed the 500 million packets per second (mpps) mark. That is more than four times the volume of packets sent at GitHub in 2018. In addition, the company believed at the time, it was the largest PPS attack publicly disclosed[30]. In April 2019, this belief became obsolete, as Imperva recorded an even larger attack against its clients of 580 mpps. These DDoS attacks have serious consequences as they paralyse organisations, including parts of critical infrastructure such as banks, as well as continuously forcing them to increase their mitigation capacity to ensure business continuity.

4.4 » DDoS ATTACKS

While denying a public or private sector entity access to its *own* data may be the primary threat in this year's report, denying others access to that entity's data or services was the third most significant threat highlighted by European cybercrime investigators. Of all the motivations behind such attacks those with an extortion element were overwhelmingly the most prevalent.

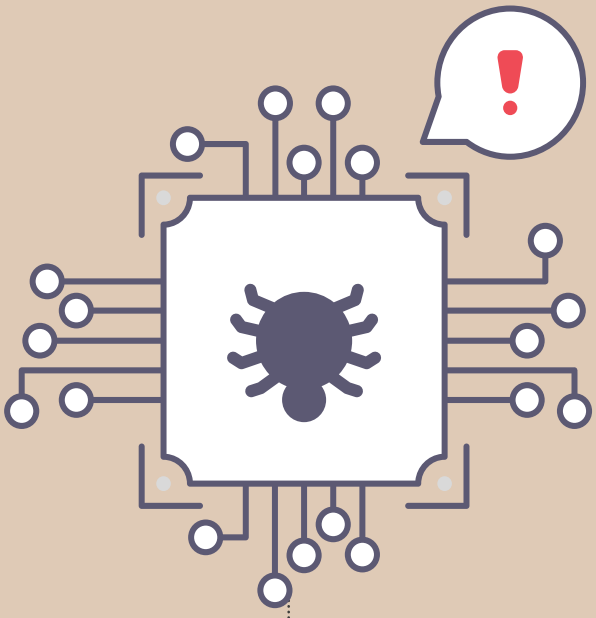
It's all about the money...

As in last year's report, while extortion was the primary motivation behind DDoS attacks reported to European law enforcement, attacks of an ideological/political nature were also common, as were attacks without an apparent motive and which appeared purely malicious.

Where stated, the most commonly identified targets were financial institutions, and public sector entities such as police or local governments. Other targets included the likes of travel agents, internet infrastructure, and services related to online gaming.

No honour among thieves

Interestingly, not only 'legitimate' enterprises are targets for DDoS attacks. Anyone familiar with any Darknet market listing service, such as the now defunct DeepDotWeb, will know that markets are typically listed with an 'uptime', with the primary reasons for downtimes being DDoS attacks. Hidden services are more vulnerable to DDoS attacks due to traits associated with the Tor browser itself. In early 2019



industry insight

DDoS attacks were one of the most prominent threats reported to Europol by its private sector partners, superseded only by phishing and other social engineering attacks, and ransomware.

Despite a noted decline in attacks by several banks following Operation Power Off, many banks report that DDoS attacks remain a significant problem, resulting in the interruption of online bank services, creating more of a public impact rather than direct financial damage.

Such attacks typically originate from low-capability actors, who can still leverage easily accessible DDoS-for-hire services that exploit booters/stressers. While most attacks can be successfully mitigated, emerging DDoS techniques which may be significantly harder to defend against, such as memcached attacks, are a concern for the financial sector.

the three largest Darknet markets were all under intense and prolonged DDoS attacks, with the moderators of Dream Market allegedly being extorted for USD 400 000 (≈ EUR 356 000), showing that anyone vulnerable to such attacks and with the means to pay is fair game to a DDoS extortionist[26].

Operation Power Off has significant and lasting impact on DDoS-as-a-service

Operation Power Off was executed in April 2018, led by the Dutch Police and the UK's National Crime Agency, and supported by Europol and a dozen law enforcement authorities from around the world. The operation resulted in the takedown of webstresser.org — considered at the time to be one of the world's largest marketplaces for hiring DDoS services — with over 150 000 registered users, and the source of 4 million attacks. A year later and the success of the operation still resonates. Moreover, the activity continues as several law enforcement authorities pursue the users of these services, and target other DDoS-for-hire services[27].

4.5 » ATTACKS ON CRITICAL INFRASTRUCTURE

The fourth cyber threat highlighted by European cybercrime investigators was attacks that disrupt or subvert the internal functions of one or more critical infrastructures. Predictably, there is some overlap between these attacks and some of the attack tools earlier in this chapter, i.e. these attacks may have involved DDoS or cryptoware, but these cases focus on attacks where the primary motive was to attack the infrastructure itself.

Law enforcement is increasingly responding to attacks on critical infrastructure

This year law enforcement appears to have become involved in a much wider variety of investigations into attacks on critical infrastructures, including attacks on the energy, transport, water supply, and health sectors. It is not possible to say whether this is due to an increasing number of attacks, or simply the growing involvement of law enforcement in such investigations. Attacks on these infrastructures by financially motivated criminals remain unlikely, as such attacks draw the attention of multiple authorities and as such pose a disproportionate risk. The most likely potential perpetrators include nation states as well as script kiddies. The accessibility of crime as a service allows such attackers to carry out potentially destructive attacks.

criminal case study

In March 2019, Norwegian company Norsk Hydro AS — renewable energy supplier and one of the world's largest aluminium producers — was compromised by the LockerGoga ransomware in a targeted cyber-attack. The attack affected large parts of the business, resulting in production stoppages in Europe and the USA. Projected costs for the company are up to NOK 350 million (≈EUR 35 million).

LockerGoga currently targets multiple industries with targeted attacks[36].

Emergency Response Protocol developed to improve cyber preparedness

The coordinated response to large-scale cyber-attacks remain a key challenge to effective international cooperation in the cybersecurity ecosystem. The development of the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises (Blueprint) and especially the EU Law Enforcement Emergency Response Protocol have significantly improved the cyber preparedness by shifting away from incongruent incident-driven and reactive response measures and acting as critical enablers for rapid response capabilities that support cyber resilience. Furthermore, such standardised procedures facilitate the multi-stakeholder coordination and ensure effective de-confliction between the different national competent authorities, international bodies and relevant private partners. Since law enforcement play a crucial role in investigating such cyber-attacks (e.g. electronic evidence collection, technical attribution, prosecution of suspects, etc.), their early involvement in the emergency response to cybersecurity incidents or crises of a suspected malicious nature is essential. Their proactive participation in cyber resilience-related activities such as cyber simulation exercises is also indispensable as such collaboration raises awareness of the roles, responsibilities and capabilities of each actor and increase the level of trust. In terms of next steps, it is crucial for the Blueprint to be operationalised, while ensuring alignment and de-confliction among the different procedures within the EU's crisis response architecture, especially the EU's Hybrid Threats framework[31].

Financial sector increasingly hit by APT-style cybercrime gangs

Another area of concern, highlighted by both European law enforcement and Europol's private sector partners, is attacks directed at internal networks within the financial sector. There are a growing number of cases of complex attacks on banks by sophisticated cyber-crime gangs employing Advanced Persistent Threat (APT)-style tactics to take control over certain aspects of a bank's internal network. Such attacks can manipulate internal fund transfer systems, such as those interfacing with the SWIFT network, in order to make illicit payments, or take control of card processing systems to allow mass cash-outs at ATMs.

Financially motivated criminal APT-style groups such as Cobalt, MoneyTaker, and Silence largely carry out such attacks[32]. In some instances however, nation states are involved, such as in the case of the Lazarus group. This APT group, which has ties to North Korea, was allegedly responsible for over half a billion USD in cryptocurrency thefts since 2017[33], and ongoing attacks against banks in South East Asia[34].

Cryptocurrency exchanges continue to be a magnet for financially motivated hacking groups. In 2018, over USD 1 billion in cryptocurrencies were stolen from exchanges and other platforms worldwide[35].

Such attacks not only result in huge criminal profits, but cause severe reputational damage to the victims and undermine confidence in the financial sector as a whole.

4.6 » WEBSITE DEFACEMENT

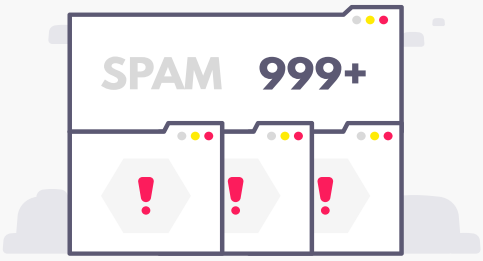
Defacing websites — a gateway to more serious cybercrime

While not a top priority for any individual country, collectively a significant number of European states have highlighted simple website defacement as one of the priorities for their jurisdiction. This implies that such activity, while low impact, is sufficiently common to result in a significant number of cases and commands a corresponding proportion of limited law enforcement resources.

The motive behind such attacks varies, but is typically for political/ideological reasons, or without purpose and purely malicious. The latter likely represents budding cybercriminals testing their capabilities.

The reason this crime area has been highlighted as a key threat is that by investigating these attacks, it provides law enforcement the opportunity to intervene with the perpetrators at an early stage in their cybercrime career. This could be a pivotal moment in preventing them from pursuing a career in cybercrime, which is the foundation of many national cybercrime prevention campaigns.

4.7 » WHAT HAPPENED TO...?



DATA STEALING/MANIPULATING MALWARE

For the second year running, data stealing malware did not feature prominently in law enforcement reporting, with only two Member States stating it as a priority. What industry reporting highlighted, is that criminals use some banking Trojans, particularly those with a modular and therefore variable functionality, such as Emotet and Trickbot, more for their network intrusion and malware delivery capabilities than simply their data-stealing capacity[37]. In some cases, criminals use such malware to install other malware, including ransomware.

Some of Europol's private sector partners report that banking Trojans remain a moderate threat and indeed they were submitted as samples to Europol's EMAS in significant numbers. While losses from banking Trojan activity against customers are at an all-time low, the ability of this malware to affect network hygiene remains a key concern. Banking Trojan veterans Dridex, Trickbot and Gozi still present the most significant banking threats, with some new Trojans such as BackSwap also now coming to the fore. Moreover, some malware families, such as Retefe, had a revival throughout 2018 and 2019, highlighting that while the popularity and prevalence of data gathering malware and banking Trojans may have declined, their development and refinement continues within certain cyber OCGs.

CRYPTOMINING

Last year we highlighted a massive surge in cryptomining; both passive cryptomining through scripts running in a victim's internet browser and more intrusive cryptojacking malware. Both techniques exploit a victim's processing power without their permission to mine cryptocurrencies — typically Monero. The size of this surge varies wildly across industry reporting but the veracity of the trend is almost unanimous. Some reports also attribute the decline in ransomware to attackers shifting to stealthier cryptojacking attacks[38].

Despite this, and despite some submissions of crypto-related malware to Europol's EMAS, we found no representation of this phenomenon in law enforcement reporting from 2018. This is likely due to its comparatively low impact (in most cases) compared to other cyber threats. Apart from the occasional exceptional case, cryptomining is likely to remain a low-priority threat for EU law enforcement.

The closure of Coinhive in March 2019 has led to a decline in the instances of browser-based cryptomining. However, attacks against public and private sectors entities not only continue, but continue to evolve (see also 9.4). There are reports of cryptojacking malware both going 'file-less[39]', and incorporating the Eternal Blue exploit in order to adopt worm-like spreading properties[40].

MOBILE MALWARE

Despite a large number of mobile malware submissions to Europol's EMAS, once again mobile malware featured only marginally in law enforcement reporting for 2018, although there was still an increase in reporting from the previous year. What law enforcement reported, related to data stealing malware, ransomware, and cryptomining malware, and, as in previous years, this largely related to Android phones. Private sector comments — from both Europol's private sector partners, and industry reporting — mirrored this. The latter highlighted parallel trends in mobile malware, such as the expansion of cryptomining malware and a general decline in ransomware[43]. Other mobile threats, such as banking Trojans continue to grow though, capitalising on the increase in m-banking.

4.8 » FUTURE THREATS AND DEVELOPMENTS

The majority of attacks rely on existing *modi operandi* and benefit from known vulnerabilities. Often, existing attacks will spread to previously untapped victims, such as ransomware targeting data centres or backup servers, and existing attack tools will continue to evolve, such as banking Trojans routinely incorporating self-propagating worm functionality.

New threats do not only arise from new technologies but, as is often demonstrated, come from pre-existing vulnerabilities in pre-existing technologies. For example, Memcached was first released in 2003[41] and yet the first DDoS attack exploiting it only occurred 15 years later.

As more and more companies outsource areas of their business, we expect to see a growth in supply chain attacks, and the evolution of such attacks to become increasingly complex. Cloud services pose a particular risk in this regard, as one company is likely to store the data for multiple clients, marking itself as a valuable target for financially motivated criminals and having a major impact if compromised.

While attacks on internal bank systems, which may interface with the SWIFT network, may have been mitigated by banks that have implemented the SWIFT recommended security program, it is not unlikely that sophisticated attackers could identify other upstream applications that generate transfers and similarly exploit those in a comparable fashion.

Various entities within the cryptocurrency ecosystem have presented themselves as profitable targets for competent cybercriminals. As the trend of crimes that traditionally target fiat currencies evolving to targeting cryptocurrencies continues, we will see more financially motivated APT-style cybercrime gangs shift their focus to any entity with large cryptocurrency assets[42] — hacking exchanges and manipulating the Blockchain with 51 % attacks*.

In early, 2019, Internet Corporation for Assigned Names and Numbers (ICANN) issued a warning over an 'ongoing and significant risk to key parts of the Domain Name System (DNS) infrastructure'. The warning relates to attacks with the potential to see data in transit, redirect traffic or allow attackers to 'spoof' specific websites. It is likely that either further existing, ongoing attacks on the DNS infrastructure will come to light, or that a new incident will occur.

* 51 % attacks can hypothetically occur when attackers control 51 % of the blockchain hashing power and can effectively double spend cryptocurrencies by reversing transactions.

> The biggest cybercrime threat of the future may be familiar to us already. The major threats we face today, such as ransomware or business email compromise, have been around for years. While we may see something quite novel, it's more likely that cybercriminals will continue refining attacks that have been shown to work, even relatively unsophisticated frauds that leverage social engineering for great monetary gain.
>
> — DR JONATHAN LUSTHAUS, UNIVERSITY OF OXFORD, UK

4.9 » RECOMMENDATIONS

Successfully tackling major crime-as-a-service providers can have clear and lasting impact. Law enforcement should continue focusing its concerted efforts into tackling such service providers.

Enhanced cooperation and improved data sharing between law enforcement, computer security incident response teams and private partners will be key to tackling complex cyberattacks and will allow the private sector to take the necessary preventative security measures to protect themselves and their customers.

In response to major cross-border cyber-attacks, all cooperation channels should be explored, including the support capabilities of Europol and Eurojust and legal instruments designed for closer cross-border cooperation (such as JITs and spontaneous exchange of information) in order to share resources and coordinate.

Further enhance the collaboration between the network and information security sector and cyber law enforcement authorities by involving the latter in cyber resilience-related activities such as cyber simulation exercises.

Low-level cybercrimes such as website defacement should be seen as an opportunity for law enforcement to intervene in the criminal career path of young, developing cybercriminals.

#5

CRIME PRIORITY

child sexual exploitation online

Online CSE refers to the sexual abuse and exploitation of children via the internet. Whereas the sexual abuse or exploitation very much takes place in the physical world, the subsequent sharing of images and videos depicting this abuse significantly aggravates the impact of this crime. The amount of online CSEM is staggering and continues to increase. As the number of young children accessing the internet grows, and offenders become more aware of anonymisation techniques, law enforcement authorities and industry partners fighting these disturbing crimes continue to face considerable challenges.

5.1 » KEY FINDINGS

- The amount of CSEM detected online by law enforcement and the private sector, continues to increase, putting a considerable strain on law enforcement authorities' resources.
- The online solicitation of children for sexual purposes remains a serious threat, with a largely unchanged *modus operandi*.
- SGEM is more and more common, driven by growing access of minors to high quality smartphones and a lack of awareness about the risks.
- Although commercial CSE remains limited, LDCA is a notable exception to this.

5.2 » ONLINE DISTRIBUTION OF CSEM

The amount of detected online CSEM continues to increase, as is reported by both law enforcement authorities and industry partners[44]. This has a serious impact on victims, who are repeatedly victimised every time such pictures or videos are shared. Out of 19 Member States who responded to this question, 10 have seen an increase in this criminal activity, with the other 9 believing the online distribution of CSEM has remained relatively stable. 5 out of 7 third partners also see an increase in this activity.

Referrals from industry and third country partners have reached record highs, putting a serious strain on the capacity of law enforcement authorities in the EU to investigate these crimes. At least 18 Member States received referrals from the USA through Europol and all Member States received referrals from Canada through Europol. Many of the referrals from the USA come via law enforcement partners from the National Center for Missing and Exploited Children, an NGO that collects reports of online CSEM. Electronic service providers in the USA are obliged to report content or links that involve CSEM.

In 2017, Europol handled 44 000 referrals from the USA for 18 Member States, increasing to 190 000 in 2018. In June 2019, the number of referrals had already reached 170 000. Referrals from Canada have seen a similar trend, increasing from 6 000 for all 28 Member States in 2018 to a current conservative prediction of 24 000 in all of 2019 for the same number of countries. Moreover, there are currently over 46 million unique images or videos relating to CSEM in Europol's repository[45].

The vast majority of online CSEM is detected on image host websites on the open web, with the Netherlands continuing to be the main hosting country[46]. Offenders keep using a number of ways to disguise online CSEM, making it more complicated for law enforcement authorities to detect such images and videos. Although online distribution of CSEM continues to take place via a variety of platforms, peer-to-peer sharing remains among the most popular way among perpetrators to share CSEM. This includes both one-on-one communication and larger groups.

case study

Over the course of two weeks in May 2019, Europol hosted the sixth Victim Identification Taskforce (VIDTF 6), an exercise where experts from Member States gather to analyse CSEM in order to identify victims and perpetrators. The taskforce continues to expand annually, with 34 experts from 24 countries, supported by INTERPOL specialists, and intelligence analysts from Europol staff.

During VIDTF 6, 466 new datasets were uploaded to the International Child Sexual Exploitation database hosted at INTERPOL, and new data was added to more than 280 existing datasets, increasing the chance victims could be identified.

The efforts led to three victims being tentatively identified: one in Europe, one in the USA and one in Russia, with another investigation ongoing to identify another European victim and offender.

However, dedicated bulletin boards on the Darknet are increasingly popular among offenders as a channel for the distribution of CSEM. This is especially the case for offenders with niche interests, including CSEM with infants and non-verbal children and demeaning material depicting torture and severe cruelty against children[47]. More generally, in many cases offenders use encryption and install software to cover their IP address and prevent identification, such as Virtual Private Networks (VPNs) and TOR.

There is an ongoing increase in the distribution of CSEM via social media applications. The self-destruct function of some of these applications make investigations particularly complicated. In some cases, this is the result of self-generated material being shared with peers, after which it is further distributed via social media and eventually ends up on CSEM platforms. There are also instances where fake social media accounts are created in order to spread private pictures and videos of underage victims together with their personal information. Although such accounts are often quickly deleted, it is easy for perpetrators to simply create a new account.

In many cases, offenders distributing CSEM online are also involved in hands-on CSE. The demand for such material perpetuates the ongoing abuse of children. However, there are also many perpetrators who possess and share such material, but are not involved in the actual sexual exploitation of children.

5.3 » ONLINE SOLICITATION OF CHILDREN FOR SEXUAL PURPOSES

The online solicitation of children for sexual purposes remains a serious threat in the EU, with many Member States reporting this crime is on the rise. As more and more minors are active on social media at a younger age, the number of potential victims continues to be high. At the same time, some countries have reported a decrease in cases related to online solicitation since the last IOCTA, possibly as a result of growing public awareness or offenders operating more carefully.

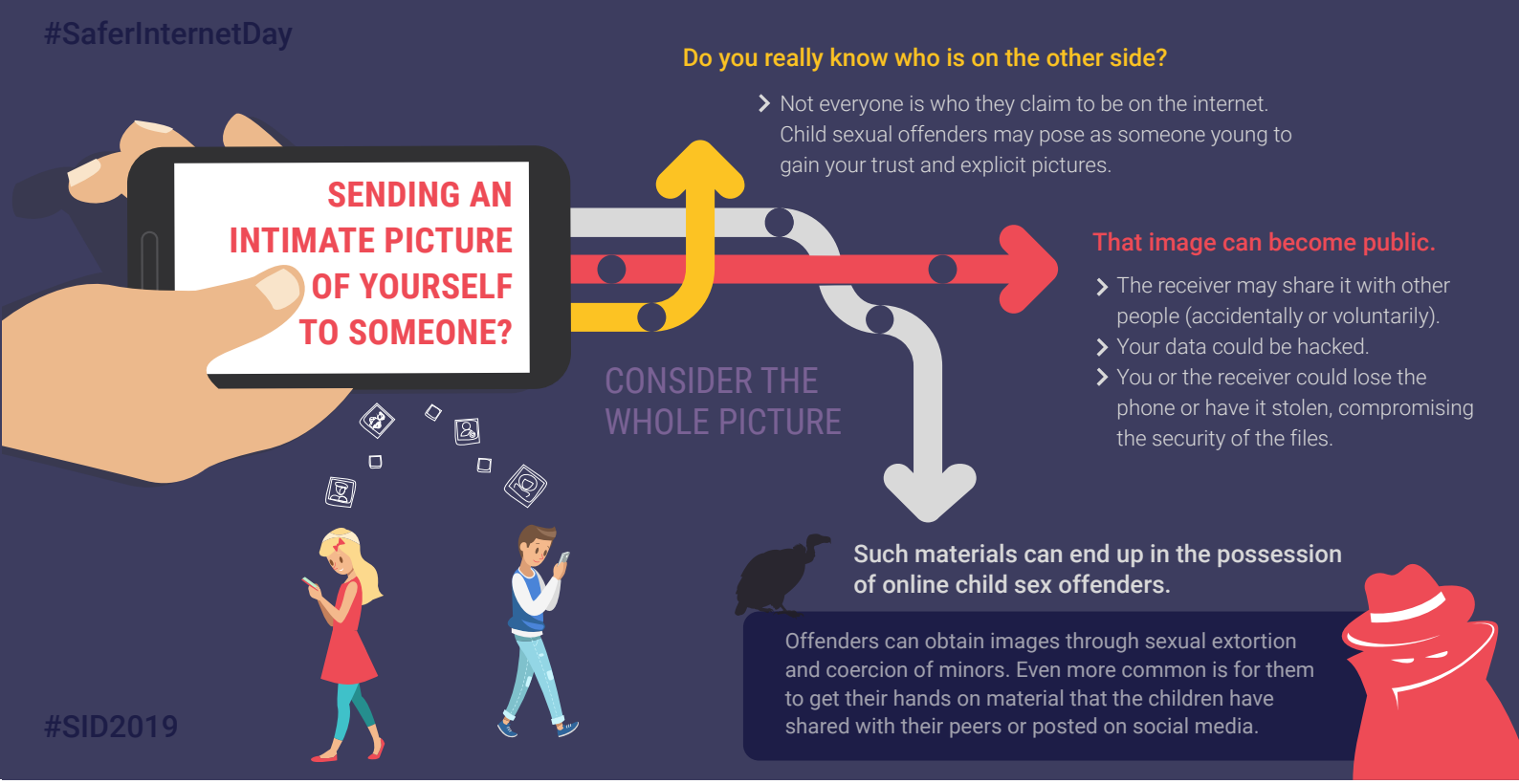
The *modus operandi* for this criminal activity remains largely unchanged. Offenders generally use the open web, as it simply much easier to get in contact with children than on the dark web. They get in touch with potential victims through a variety of social media services, creating fake profiles and frequently pretending to be of the same age. This can happen on many different platforms, ranging from Facebook and Instagram to online gaming environments. Minors are also sometimes approached on live video platforms. Once trust has been established, communication is quickly moved to encrypted online messaging applications, such as WhatsApp or Viber. Whereas explicit material is initially shared voluntarily, offenders subsequently use this material for further coercion and extortion for new CSEM. In some cases, suspects will harass their victims so that they do not file a complaint against them.

Victims are mostly young teenagers, both girls and boys. Some offenders specifically target profiles with many friends, as they believe this means a higher chance of successfully establishing contact.

case study

In March 2019, a German court convicted four men to sentences between 4 and 10 years in prison for running the online CSE platform 'Elysium' on the Darknet. They had set up, administered and moderated what was one of the largest forums of its kind, with more than 11 000 registered users from all over the world. One of the men was also convicted for the sexual abuse of two young children. None of the men involved had known each other in person. The forum had a wide range of different categories of CSEM, including serious violence and very young children.

A man in Sweden was sentenced to 10 years imprisonment for forcing children, all under the age of 15, from primarily North America and the United Kingdom to commit sexual acts in front of a camera or webcam. Despite the fact that he was not physically present at the crime scenes, the court nonetheless convicted him as a hands-on offender on the basis of the concept of 'virtual rape'. It was the first time an online CSE perpetrator had been convicted as a hands-on abuser.



5.4 » PRODUCTION OF SELF-GENERATED EXPLICIT MATERIAL

SGEM has been a growing problem for several years, as more and more young children share explicit material online. Growing access to high quality smartphones and other devices, in combination with relatively low awareness of the risks of producing and sharing SGEM, means this trend is likely to continue.

A distinction can be made between SGEM produced voluntarily and SGEM produced under coercion or extortion by a child sex offender. Regarding the first category, there is a growing number of minors sharing sexual pictures or videos with peers. Children are making themselves vulnerable on a number of levels through this behaviour, including in the context of online solicitation by child sexual offenders. Moreover, in many cases the pictures or videos may be spread further, first between other peers, but eventually ending up in the collections of online child sex offenders. Such cases can subsequently lead to the minors being subjected to sexual coercion and extortion by online child sex offenders for new SGEM or material involving their siblings or other friends.

case study

European Youth Day to raise awareness

On 20 November 2018, Europol introduced a new initiative: The European Youth Day. This was a first event of its kind, which brought together Europol experts and around 100 young students aged between 12 and 15 years old under the topic 'Digital Rights of Youth against Violence'. Following on from the #SayNo initiative, the 2018 European Youth Day at Europol took the discussion one step further, allowing young people themselves to bring their opinions to the table on current cyber threats affecting them, as well as how best to tackle these.

5.5 » SEXUAL COERCION AND EXTORTION OF MINORS FOR NEW CSEM

Although sexual coercion and extortion of minors also happens for financial gain, in the majority of cases the aim is to obtain new CSEM. Offenders mostly use existing explicit pictures or videos of a victim and threaten to share this with the victim's network or on social media, unless they receive more material. These existing pictures or videos can come from two sources: either through online solicitation of minors for CSEM, or because they have found SGEM and have been able to identify and contact the victim. Some offenders will send explicit images and messages to a minor. Even if they do not receive any explicit pictures, they use screenshots of the conversations for coercion purposes. As stated above, such coercion can involve producing material of or with other children within or outside their own family. The impact is significant as sextortion can lead to significant trauma for the victim or in some cases even to suicide. This makes educating children about the risks of sextortion as well as the need to seek help when victimised crucial.

5.6 » LIVE DISTANT CHILD ABUSE

Monetisation of online CSE is generally limited, as offenders are more often driven by a desire to obtain more CSEM than by financial gain. However, in a small number of cases offenders do seem to seek financial gain from online CSE. One method is hosting legitimate 'pay-per-click' advertisements on websites hosting CSEM. Especially when the CSEM is disguised, this increases the platform's click rate and the potential profits per click. There have also been instances of offenders sharing CSEM in exchange for money, but this is far less common than exchanging images for other images. On rare occasions, offenders also use SGEM to coerce victims for money instead of producing new CSEM. However, the most common form of commercial CSE is LDCA.

Because of growing internet speed in many third countries, offenders can watch live streams of CSE taking place on the other side of the world. In many cases, perpetrators pay for watching this kind of CSE. The Philippines remains the most prominent country in terms of location of the victims, although there are indications this is taking place in a larger number of countries. Contact is established in a variety of ways. In some cases, first contact takes place on commercial adult porn websites, after which conversations take place on encrypted messaging platforms. In most cases, the CSE is live streamed on online platforms with the possibility of video conference. Often perpetrators have the chance of orchestrating and directing the abuse in real time. Perpetrators generally pay via online payment methods, but cryptocurrencies are still rarely used. Some of the offenders also travel to third countries to engage in hands-on abuse.

case study

In May 2019, a British man was sentenced to five years in prison for attempting to incite minors under 13 to engage in sexual acts and planning to sexually abuse several minors in the Philippines. The offender was based as a teacher in Malaysia and Thailand at the time of the offences, but was convicted under a section of the British Sex Offences Act that allows British nationals to be prosecuted for offences committed abroad. He was arrested upon arrival in the United Kingdom after investigators found he had made money transfers to online payment accounts of members of a Filipino OCG involved in LDCA.

Evidence showed the offender had also sent money to a Filipino mother of two girls aged 7 and 11 and a boy aged 5, based in Cebu. The money was sent in order for her to buy food for her children, with the offender requesting pictures of her 11-year-old daughter in return. He subsequently also had direct conversations with the girl that were sexual in nature. After he sent more money, the offender expressed an interest in the 7-year-old child and indicated he would like to meet her in order to have sex with her. An arrangement was made to meet in Manilla, although there are no records of the offender actually travelling to the Philippines.

5.7 » FUTURE THREATS AND DEVELOPMENTS

The main threats related to online CSE have remained relatively stable over the last number of years and it is unlikely that there will be any major changes in this crime area in the foreseeable future. However, one development that could be of concern for online CSE is the ongoing improvements of so-called deepfakes. Deepfake technology is an AI-based technique that places images or videos over another video. It has already been used to place the faces of celebrities on existing pornographic videos. Although the technology is still relatively new, it is rapidly improving and becoming more accessible and easy to use. It may be a matter of time before the first deepfakes appear depicting online CSE, resulting in the generation of new 'personalised' CSEM. This can also have serious implications for law enforcement authorities, as it might raise questions about the authenticity of evidence and complicate investigations.

5.8 » RECOMMENDATIONS

Coordinated action with the private sector and the deployment of new technology, including Artificial Intelligence, could help reduce the production and distribution of online CSEM, facilitate investigations and assist with the processing of the massive data volumes associated with CSEM cases.

A structural educational campaign across Europe to deliver a consistent, high-quality message aimed at children about online risks is of the utmost importance to reduce the risks derived from SGEM such as sexual coercion and extortion.

As much CSEM, particularly that arising from LDCA, originates from developing countries, it is essential that EU law enforcement continues to cooperate with and support the investigations of law enforcement in these jurisdictions.

Fighting CSE is a joint effort between law enforcement and the private sector and as a common platform is needed in order to coordinate efforts and prevent a fragmented approach and the duplication of effort.

To prevent child sexual offenders from travelling to third countries to sexually abuse children, EU law enforcement should make use of PNR data accessible through the Travel Intelligence team within Europol.

CRIME PRIORITY

#6 payment fraud

6.1 » KEY FINDINGS

- CNP fraud continues to be the main priority within payment fraud and also continues to be a facilitator for other forms of illegal activity.
- Skimming continues to evolve with criminals continuously adapting to new security measures.
- Jackpotting attacks are becoming more accessible and successful.

6.2 » CARD NOT PRESENT FRAUD

CNP fraud is the main priority for investigators of payment card fraud within Member States. One law enforcement respondent specifically states 'it is the single most common form of fraud'. This follows the pattern from previous years, especially since the number of online transactions and the e-commerce industry continue to evolve. Within CNP fraud, fraud relating to the purchase of physical goods is at the top of the list. Member States mention the purchase of (high-value) electronic devices such as mobile phones, laptops and tablets several times. Another Member State specifically notes how the *modi operandi* in this area of cybercrime have not seen any major innovation during the last year. While there has been no major shift in 2018, according to private sector input, CNP is increasingly moving into other sectors such as travel (hotels, car rentals, etc.) postal services, giftcards, etc. Fewer cases have been reported to law enforcement since there is not yet the same level of awareness as in, for instance, e-commerce.

The data required to execute CNP fraud generally seems to originate from data compromise, including third-party breaches, phishing emails and scam text messages (see section 4.3). Magecart attacks, for example, briefly described in chapter 4, have hit nearly 17 000 e-commerce websites since April 2019. The criminals are able to exploit vulnerabilities that occur when website owners inadvertently misconfigure their Amazon Web Server (AWS) S3 storage servers. According to Farinelli, '[t]hese servers act as cloud-based "buckets" that store important data — including credit card numbers that are collected by e-commerce websites. AWS S3 servers are secure when their standard settings are used; however, many companies customize these settings. If the customisation is misconfigured, a security gap can occur[48].' This misconfiguration provides anyone with an AWS account with the opportunity to not only read the content of the 'bucket' but also develop new code — such as code to collect card data from an e-commerce site.

More interestingly, Magecart attacks now target smaller vendors that supply functionality services to large enterprise websites including analytics, browser display requirements, social media,

case study

In May 2018, a regional unit in a Member State uncovered the criminal activities of an organised group from Côte d'Ivoire and Morocco specialising in the theft of credit card numbers for the purpose of distance selling fraud. The *modus operandi* set up by the scammers consisted of obtaining credit card numbers (by phishing victims or following purchases on the Darknet) as well as connection identifiers to victims' internet boxes in order to schedule a call forwarding to the scammers. As a result, calls from banks to confirm purchases were forwarded directly to the criminals. Law enforcement recovered technological products purchased fraudulently. Intangible products (Western Union mandates and TransCash cards) were recovered in Morocco.

marketing and chatbots. This means that when the code from one of these vendors is compromised, the compromise affects all of the websites that contract with the vendor[49]. This also connects to the increasing threat and growing concern with respect to supply chain attacks (see Industry insight in section 4.3).

The European Central Bank (ECB) also recognises the 'ongoing shift of fraud from the card-present to the card not present environment'. Data seems readily available. 23 million stolen credit cards are for sale on the dark web in the first half of 2019[50]. With all the data available and accessible for criminals, the focus ought to be on monitoring and detection of accounts as a means to curb the number of frauds and the amount of damage. From that perspective, the ECB notes how 'the market has started to develop a plethora of fraud prevention and detection security tools with the objective of bringing online fraud rates down (e.g. implementation of 3D Secure, risk-based analysis, Tokenization)[51]'.

More detailed data to circumvent detection

Simultaneously, criminals expand on their existing repertoire of methods as the prevention and security measures of companies improve. One relatively new development, for example, is a crime-as-a-service facility where criminals provide a platform with available bots that contain a victim's real digital fingerprint, cookies, saved passwords and other personal information including bank and payment information. These fingerprints contain all the necessary information to enhance the possibility of avoiding detection mechanisms of companies, namely e-commerce. Criminals obtain the fingerprints as real-time fingerprints or generated when scratched by the bot from the user's device.

The platform provides a simple user-friendly interface which allows other criminals to set up a different digital identity. This way it is much easier for criminals to commit fraud compared to purchasing compromised credit card details or account details and risk the detection of security measures.

CNP fraud used to facilitate other forms of crime

Whereas we often discuss CNP fraud purely from a financial perspective, this type of crime also facilitates other types of illegal activity. Examples include the facilitation of illegal immigration and more specifically Trafficking in Human Beings (THB). Criminals do this through the purchase of plane tickets with compromised credit card credentials, booking hotels, rentals, etc. They do this through CNP fraud in combination with forged identification documents.

One of our cases illustrates how CNP fraud can underpin and facilitate other forms of illegal activity. In September 2018, with the support of Europol and Frontex, two suspects were arrested in a series of coordinated raids across Germany and Sweden in an investigation targeting a Syrian OCG suspected of cyber fraud. The arrestees are believed to be the key organisers of a cyber fraud gang.

6.3 » SKIMMING

The German Federal Criminal Police Office initiated operation Goldring in October 2017. The intelligence-led operation uncovered an OCG, composed of Syrian nationals, which was involved in fraudulently purchasing airline and train tickets. According to information from Germany, more than 493 fraudulent bookings were identified. The tech-savvy smugglers avoided detection by making the bookings using compromised corporate credit cards and credentials, purchased online from other criminals offering them for sale.

The private sector brought the fraudulent transactions to the attention of law enforcement, highlighting once again how instrumental public-private partnerships are in fighting this type of fraud. This effective working relationship has been established over the course of recent years as a result of Europol's Global Airport Action Day, a recurrent operation bringing together law enforcement, the airline industry and payment card companies to target airline fraud. As part of this operation, Europol and Frontex have jointly identified significant crossovers between payment card fraud and irregular migration and THB, leading to a number of arrests in recent years. The operational successes have confirmed this trend.

Skimming surfaced as the second priority as reported by investigators of payment card fraud within the Member States throughout 2018. As one Member State describes, 'the phenomena of credit card fraud continue to evolve with increasingly sophisticated skimming or shimming tools, often deployed by criminal groups from Central Europe or the Balkans, in real raids targeting the whole continent'. Industry also confirms the lingering threat of skimming. In general, the European Payment Council (EPC) echoes law enforcement reporting when it states how skimming remains one of the most common frauds[52]. The ongoing threat of skimming is the direct result of the fact that not all payment terminals and ATMs in Europe contain the necessary anti-skimming measures. This makes the copying of magnetic-stripe track data at Point of Sales terminals and ATMs possible and still a predominant type of fraud in Europe. Subsequent usage of a cloned magnetic-stripe payment card is hardly possible in the European area since the industry has secured cards with Europay, MasterCard and Visa (EMV) chip technology. On a global level, the situation is different especially with concern to countries that have yet to introduce EMV compliance. As a result, this remains a major concern for European card issuers.

Law enforcement provides the same perspective on the matter. As one respondent writes: 'The European card data collected is then resold, both on the Darknet and via traditional websites. Several cases by the judicial police have shown that this fraudulently acquired data is being reused in bank withdrawals, mainly in America and South-East Asia'. Other Member States echo this conclusion. As long as EMV compliance in those parts of the world remains absent, skimming cards and subsequently using the data remains profitable. The EPC confirms this when it writes: 'Concerning card payment fraud, as long as the mag-stripe is needed for international transactions, skimming will remain an issue[53]'.

Deep insert skimmers frequently used by criminals

With respect to the *modus operandi,* several Member States describe how suspects use deep insert skimmers in order to copy the data stored on the magnetic stripe. This type of skimmer is composed of metal or plastic. The criminal also installs a camera on the ATM in order to steal the PIN. Other Member States specifically report on investigations pertaining to criminals who actually prepare and distribute the devices for skimming. Different OCGs then use these devices to skim ATMs both in and outside the EU. Software skimming malware intercepts card and PIN data at the ATM, allowing the criminal to copy the data and later create counterfeit cards for use at non-EMV compliant ATMs. Alternatively, criminals send the skimmed data with the pin codes to other offenders to facilitate the unauthorised withdrawals from ATMs outside the EU.

6.4 » JACKPOTTING

Nowadays, jackpotting — also referred to as black-box attacks — to cash-out the ATM is the most widespread type of logical ATM attack. Criminals perform jackpotting in one of two ways. Either the criminal uses malware which sends commands to the dispenser, or uses their own 'black box' hardware device connected directly to the dispenser, to cash-out the ATM and empty it of cash. These attacks can only be performed against certain 'old' ATMs which, due to lower security standards, are vulnerable for these type of attacks.

Jackpotting attacks appear to be evolving

Compared to last year, jackpotting attacks appear to be evolving. Several Member States describe how perpetrators have committed these attacks or at least attempted to do so. This may also be due to the necessary equipment becoming more available and accessible. *WinPot* and *Cutlet Maker* are both available on the dark web[54]. This seems to be an unusual development, as ATM hackers have generally kept their work more protected[55]. According to one law enforcement respondent, 'attacks on ATMs using the "jackpotting" technique have diversified and intensified'. The same Member State describes how in 2018, its law enforcement unit recorded 39 cases, including 27 attempts, mainly in the capital region. The financial losses from such attacks can vary between EUR 2 200 and EUR 128 800 depending on the point of attack. Based on law enforcement intelligence, the authors of the malware appear to come from Romania, Moldova and Russia. The majority of reported jackpotting attacks have involved some physical access to the ATM. This is the main obstacle for criminals, since physical access increases the risk of being caught.

According to one Member State, the *modus operandi* of piercing the front of an ATM in order to connect a computer seems to have disappeared. Criminals appear to have started using different methods. The first method consists of disconnecting the front of the ATM from its base in order to allow direct access to the connections. The second method requires simply removing the screen from the ATM and a few technical operations in order to access also the connections of the server managing the cash registers. One Member State reported three cases of black box attacks in 2018, where the attacks involved melting a hole above the monitor of the ATM and plugging a USB cable into the ATMs printer cable. Other Member States confirm this *modus operandi.* Once criminals have gained physical access, they use, for example, the *Cutlet Maker* software. More recent cases involved criminals breaking the deposit slot plastic, opening the monitor and connecting the ATM USB cable. Subsequent withdrawal of cash occurred through usage of the software *ATMdesk*.

Some law enforcement respondents do indicate how in certain cases perpetrators get to the ATM without any damage, using the original key to install a laptop that connects to the USB output. The laptop is also connected to the internet via hotspot from a prepaid phone. The laptop is removed after withdrawing money. Overall, the time of the ATM attack is about 10 minutes.

6.5 » BUSINESS EMAIL COMPROMISE

One of the most economically damaging attacks is business email compromise (BEC). Several industry partners highlight that perpetrators aim more and more attacks at upper (C-level) level management, and that such attacks are becoming more professional and convincing. Such attacks were also a top priority for European law enforcement. According to the Internet Crime Complaint Centre, between December 2016 and May 2018, there was a 136 % increase in identified global exposed losses, and more than USD 12 billion in losses since October 2013[56].

While BEC is not a new phenomenon, criminals are finding new *modi operandi* to take advantage of this technique. The main or original techniques used by criminals are the use of social engineering strategies to impersonate a company staff member, usually a CEO or other staff member who can authorise transfers, and deceive employees and executives within the company. The target companies are usually firms with frequent wire transfers or with foreign suppliers. However, the attacks take place through different methods: the compromise of legitimate email accounts, social engineering or intrusion techniques.

BEC exploits the way corporations do business, taking advantage of segregated corporate structures, and internal gaps in payment verification processes. Such attacks vary by the degree of technical tools used. Some attacks can only successfully employ social engineering, while others deploy technical measures such as malware and network intrusion. This variety in *modi operandi* also requires a variety in response. At the low-tech end, where social engineering reigns, awareness and training for staff are key. BEC was part of the broader cyber scams campaign organised by EC3 as part of the cybersecurity month in 2018. Yet, even though creating awareness among employees can assist in detection of social engineering attacks as a means for criminals to engage in BEC, more high-tech methods such as malware and network intrusion require a different type of response. Those enterprises without the resources to enact such measures, such as many server message blocks, remain particularly at risk.

6.6 » FUTURE THREATS AND DEVELOPMENTS

The landscape of payment fraud demonstrates the resilience of certain criminal *modi operandi*. As a result, for payment fraud, the past and present are important indicators for what we can anticipate in the future. As long as CNP fraud as well as skimming remain profitable, criminals shall carry out such *modi operandi.* For CNP fraud the added problem is the role it plays in facilitating other forms of criminal activity.

With regard to jackpotting, some evolution is evident. The accessibility and availability of jackpotting-related malware may make jackpotting a more accessible crime. Authors of the malware also look for ways to reduce obstacles, better target their efforts in order to steal more money in a lesser amount of time[57]. Simultaneously, even if unsuccessful, jackpotting tries are still a problem as they cause considerable damage to the infrastructure. This makes it a particularly complex problem to tackle.

In the previous IOCTA, we reflected on the potential for instant payments to complicate fraud prevention and especially mitigation. Since 2017, a number of instant payment schemes have been launched; most recently, the ECB launched the TARGET instant payment settlement service in November 2018. Such schemes allow the settling of electronic payments between European banks (almost) instantly. While these provide clear benefits to the financial sector and commerce, they can also inadvertently expedite various frauds. Such transactions not only provide money launderers with better option for money mule accounts, but also make it harder for the financial sector to block suspect transactions.

CEO/BUSINESS EMAIL COMPROMISE (BEC) FRAUD

CEO/BEC fraud occurs when an employee authorised to make payments is tricked into paying a fake invoice or making an unauthorised transfer out of the business account.

HOW DOES IT WORK?

A fraudster calls or emails posing as a high ranking figure within the company (e.g. CEO or CFO).

They have good knowledge about the organisation.

They require an urgent payment.

They use language such as: 'Confidentiality', 'The company trusts you', 'I am currently unavailable'.

They refer to a sensitive situation (e.g tax control, merger, acquisition).

The employee is requested not to follow the regular authorisation procedures.

Instructions on how to proceed may be given later, by a third person or via email.

The employee transfers funds to an account controlled by the fraudster.

Often, the request is for international payments to banks outside Europe.

WHAT ARE THE SIGNS?

- Unsolicited email/phone call
- Direct contact from a senior official you are normally not in contact with
- Request for absolute confidentiality
- Pressure and a sense of urgency
- Unusual request in contradiction with internal procedures
- Threats or unusual flattery/promises of reward

WHAT CAN YOU DO?

AS A COMPANY

Be aware of the risks and ensure that **employees are informed and aware too**.

Encourage your staff to **approach payment requests with caution**.

Implement internal protocols concerning payments.

Implement a procedure to verify the legitimacy of payment requests received by email.

Establish **reporting routines** for managing fraud.

Review information posted on your company website, **restrict information and show caution** with regard to social media.

Upgrade and update technical security.

Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

AS AN EMPLOYEE

Strictly apply the security procedures in place for payments and procurement. **Do not skip any steps and do not give in to pressure**.

Always **carefully check email addresses** when dealing with sensitive information/money transfers.

In case of doubt on a transfer order, **consult a competent colleague**.

Never open suspicious links or attachments received by email. Be particularly careful when checking your private email on the company's computers.

Restrict information and show caution with regard to social media.

Avoid sharing information on the company's hierarchy, security or procedures.

If you receive a suspicious email or call, always inform your IT department.

Alongside instant payments, developments with respect to the Directive (EU) 2015/2366 of the European Parliament and of the Council[58] (known as the Payment Services Directive 2, PSD 2) are also ongoing. The implementation deadline of the Directive has passed however on 14 September 2019, financial service providers (from banks to Fintechs) must adhere to certain security requirements with respect to strong customer authentication. The European Banking Authority (EBA) has indicated that if needed providers can receive an extension. The EBA has a crucial role in the establishment of the security standards with respect to PSD 2. As the EBA notes in its opinion, '[o]ne of the fundamental changes introduced by PSD 2 is to formalise payment security requirements in national law. One such requirement is for PSPs to apply SCA to electronic transactions[59]'. In principle, if implemented, the SCA should enhance security; yet, the ability to file for an extension could in theory make certain providers more vulnerable to attacks in case criminals discover SCA is not yet in place by the deadline.

Other developments around the same date are relevant for the criminal landscape. As we reported last year, one of the central issues arising out of open banking revolves around the concept of screen scraping. Screen scraping allows third-party providers to access customers' interfaces and collect relevant data to gain access to a bank account. While aimed at improving consumer experience, screen scraping is susceptible to man-in-the-middle attacks and other forms of fraud. Given the number of security-related concerns, the European Commission has decided to ban screen scraping from September 2019 as part of the regulatory technical standards of PSD 2. If this goes through, it would be a positive development as it eliminates a criminal opportunity. Despite this, the overall open banking development remains one to monitor from a threat perspective and makes proper and timely implementation of SCA all the more important to manage fraud. As Fortuna notes, '[w]ith Open Banking, data will increasingly be passing through a client (a customer) to an open interface, becoming extremely vulnerable to attacks as there is no way to control the customer's device, whether that be a mobile phone or a web browser. By facilitating access to customer data, third-party providers also become targets for client-side attacks[60]'.

On a final note, the current legislative situation with respect to non-cash means of payment fraud is unsatisfactory to both private industry and law enforcement. However, Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment[61] (known as the non-cash-payment fraud (NCPF) Directive) — which Member States have two years to implement — will help in ensuring that a clear, robust, and technology-neutral legal framework is in place. It will help eliminate existing challenges to investigation and prosecution of fraud and is expected to make a very positive impact in the fight against NCPF. A particular focus of the NCPF Directive is on improving cooperation on cross-border fraud cases. Such cooperation requires a fertile environment which facilitates parties to engage in information exchange. Most often, criminals attack the financial sector as a whole rather than a specific institution. As such, information exchange of new *modi operandi* or ongoing criminal campaigns require information exchange between private parties as well as between public and private parties.

6.7 » RECOMMENDATIONS

Cooperation between the public and the private sector as well as within the sectors is crucial to come to fruitful results. To this point, speedy and more direct access to and exchange of information from the private sector is essential for Europol as well as its partners.

Organisations must ensure they train their employees as well as make their customers aware of how they can detect social engineering and other scams.

#7 the criminal abuse of the dark web

7.1 » KEY FINDINGS

- The dark web remains the key online enabler for trade in an extensive range of criminal products and services and a priority threat for law enforcement.
- Recent coordinated law enforcement activities, combined with extensive DDoS attacks, have generated distrust in the Tor environment. While there is evidence administrators are now exploring alternatives, it seems the user-friendliness, existing market variety and customer-base on Tor, makes a full migration to new platforms unlikely just yet.
- There are increases in single-vendor shops and smaller fragmented markets on Tor, including those catering for specific languages. Some OCGs are also fragmenting their business over a range of online monikers and marketplaces, therefore presenting further challenges for law enforcement.
- Encrypted communication applications enhance single-vendor trade on the dark web, helping direct users to services and enabling closed communications. Although there is no evidence of a full business migration, there is a risk the group functions could become increasingly used to support illicit trade.

Often used interchangeably are the terms Darknet and dark web. For the purpose of this report, the Darknet is the encrypted part of the internet accessed using specific software that in themselves are not criminal, such as the Tor browser. The dark web is the many criminal websites and services hosted on these networks.

Investigator feedback across all the crime areas in this report highlighted the dark web as a priority threat area. These reports related almost exclusively to the sale of criminal products and services, including drugs, weapons and explosives, compromised data and credit cards, malware, counterfeit goods and currency and fake documents. This highlights the extent to which this threat facilitates a range of criminality[62].

Highlighted each year is the volatility of the dark web ecosystem. This continues to be the case, intensified by effective coordinated law enforcement activity in early 2019. Authorities undertook global action against vendors in February, and Dream Market, arguably the largest market at that time, shut down voluntarily, after this. This was supposedly in response to a prolonged and persistent DDoS attack as discussed earlier in section 4.4. Soon after law enforcement announced the shutdown of two of the remaining top dark web markets, Wall Street Market and Valhalla, followed by Bestmixer, the mixing and tumbling service hosted in part on the dark web (see section 9.7). Lastly, law enforcement shut down the online dark web information resource DeepDotWeb after its administrators received millions of euros in kickbacks for referrals to dark web marketplaces selling fentanyl, heroin and other illegal goods.

The coordinated law enforcement efforts, together with continued DDoS attacks, have had a significant impact on the dark web in terms of generating distrust and, at the time of writing, the environment remains in a state of flux. The emergence of new multi-vendor top markets is apparent, however, as are increased exit scams, including some of those initially appearing to dominate. The apparent re-emergence of the Dream Market, which claims to have re-opened in July 2019 as Samsara Market has also taken place.

Evolution of online trade continues

Dark web reports almost exclusively refer to use of the Tor platform, although there is evidence of criminality on most similar privacy-orientated software i.e., Tor, I2P, Zeronet, Freenet, Openbazaar, etc. In previous reports, the suggestion was the succession of law enforcement takedowns and other security issues would push the dark web sites and services to these other platforms. The Libertas Market did briefly switch to solely operating on I2P following the recent law enforcement activities, only to cease operating shortly after due to a low customer base. There are no other examples of this type of move, therefore, while the risk of alternatives remains, it seems the user-friendliness, existing market variety and customer-base on Tor, makes a full migration from customers or markets to new platforms unlikely just yet.

case study

In May 2019, two prolific dark web marketplaces, the Wall Street Market and Valhalla (also known as Silkkitie), were taken down in simultaneous global operations by EU law enforcement.

After the takedown of the three largest markets in 2017, Wall Street was one of the largest remaining illegal online markets. At the time of its closure, it had over 1 150 000 users and 5 400 vendors. The German Federal Criminal Police Office, supported by the Dutch National Police, Europol, Eurojust, and a number of US government agencies, arrested three suspects in Germany. Police officers seized over EUR 550 000 in cash, as well as cryptocurrencies Bitcoin and Monero in six-digit amounts. Two of the markets highest-selling suppliers of narcotics were also arrested in the USA.

Finnish Customs seized the Valhalla marketplace server and its contents in close cooperation with the French National Police and Europol. As a result of the operation Finnish Customs also made a significant Bitcoin seizure. Valhalla was one of the oldest and internationally best-known Tor trade sites.

case study

In mid-2018, German authorities identified a Darknet market vendor selling various narcotic drugs, counterfeit currency and counterfeiting equipment. The vendor had been active for over two years on multiple marketplaces and was suspected to be living in Germany.

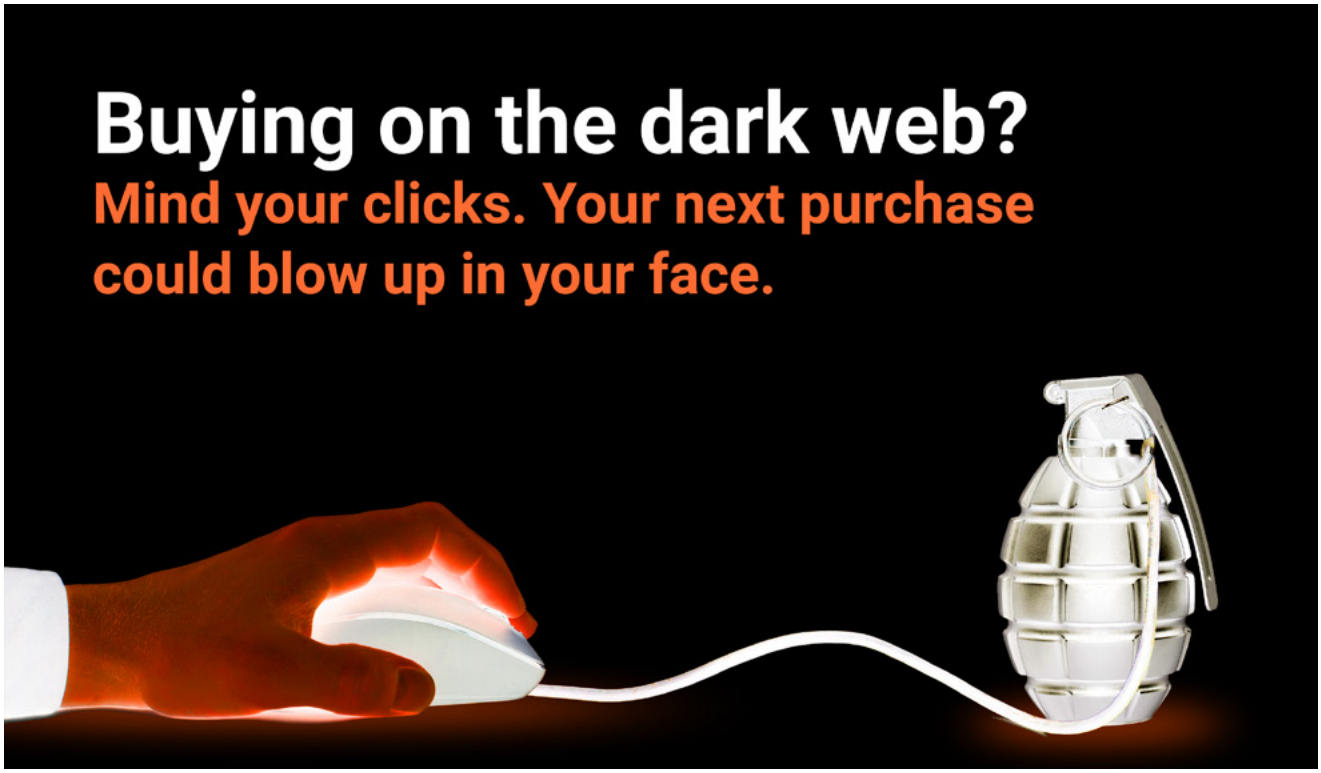
Officers trained in cryptocurrency investigation were able to identify the vendor as a 35-year-old German national and affect an arrest. The suspect had made over EUR 700 000 over the two years he was active.

However, for this market growth has been slow due to continued suspicion over law enforcement involvement. Finally, some markets have changed their policies to prohibit the sale of fentanyl and weapons and explosives in an attempt to avoid law enforcement attention, albeit the sale of these commodities continues under different guises and on other sites.

Instead, criminals are exploring alternative means of circumventing law enforcement within the Tor environment. In last year's report, the suggestion was the closure of larger marketplaces would result in a growth in the number of single-vendor shops and smaller fragmented markets. This forecast is indeed true with confirmed increases in single-vendor shops operating on independent .onion sites and smaller markets, including those catering for specific languages. However, not anticipated last year was the emergence of multi-identity business models, where OCGs maintain multiple profiles online, on multiple platforms, in order to operate as multiple distinct individuals rather than a single entity. By fragmenting their business over a range of online monikers on marketplaces and disparate vendor shops, it reduces the perception of the scale of the OCG, and keeps them under the radar of law enforcement, compared to the attention they might receive operating as a single multi-commodity vendor with a higher customer base. This creates further challenges for law enforcement, as in addition to the usual attribution issues associated with dark web investigations, investigators must also make these connections on order to determine the true scope and scale of an OCG.

In addition to circumventing law enforcement, criminal developers are also motivated by the need to increase trust with their customer-base on Tor, both in terms of anonymity but also by reducing the risk of exit scams. An example of such a market is Black Dog, scheduled for launch in August 2019. It claims to be the 'first ever truly decentralised crypto market' and depends on the Ethereum blockchain to facilitate transactions, without the need for a traditional marketplace GUI as found on Tor markets. The market also utilises the smart contracts component of the Ethereum blockchain to allow credible transactions without the need for a third party. As with alternative platforms, it is unclear how, and to what extent, cybercriminals will adopted this type of market model, again taking into account the effects of AMLD 5.

Separate to Darknet platforms, predicted last year was that some vendors might migrate their business to encrypted communications applications, running their shops within private channels/groups and even the encrypted messaging platforms evolving into functional marketplaces. Although there does appear to be an increased use of encrypted communications applications to enhance the single-vendor trade on the dark web, helping direct users to services and enabling closed communications, there does not appear to be a full business migration. There have been some instances where group functions have supported functional marketplaces with perpetrators selling different criminal commodities, much like the different sub-forums on a typical online forum. However, these markets, although simple to set up (as the platform provides the infrastructure) and easy to revive if taken down, offer little in the way of security for their customers, i.e. there is no escrow or similar services. They can also be less technically challenging than a Tor-based site to take down, as they sometimes only require an abuse notification sent to the provider, who, if they respond to such requests (not always the case), can ban or delete the group. It is therefore unclear how and to what extent cybercriminals may adopt this market approach, and much of which depends on law enforcement relationships with industry partners in this sector and the ability to locate and effectively take them offline once identified.



The currency of the dark web enterprises remains virtual and an estimated USD 1 billion has been spent on the dark web this year alone[63]. Bitcoin remains the most frequently used currency, believed to be a consequence of familiarity within the customer base (see also section 9.4). However, there has been a more pronounced shift towards more privacy-orientated currencies, a trend that it is anticipated will continue as criminal users become more security aware.

7.2 » RECOMMENDATIONS

More coordinated investigation and prevention actions targeting the dark web as a whole are required, demonstrating the ability of law enforcement and deterring those who are using it for illicit activity. An improved real-time information position must be maintained to enable law enforcement efforts to tackle the dark web. The capability will enable the identification, categorisation and analysis through advanced techniques including machine learning and artificial intelligence.

An EU-wide framework is required to enable judicial authorities to take the first steps to attribute a case to a country where no initial link is apparent due to anonymity issues, thereby preventing any country from assuming jurisdiction initiating an investigation.

Improved coordination and standardisation of undercover online investigations are required to de-conflict dark web investigations and address the disparity in capabilities across the EU.

#8 the convergence of cyber and terrorism

8.1 » KEY FINDINGS

- The wide array of OSPs exploited by terrorist groups presents a significant challenge to disruption efforts.
- Terrorist groups are often early adopters of new technologies, exploiting emerging platforms for their online communication and distribution strategies.
- With sufficient planning and support from sympathetic online communities, terrorist attacks can rapidly turn viral, before OSPs and law enforcement can respond.

8.2 » THE USE OF THE INTERNET BY TERRORIST GROUPS

The loss of the Islamic State's (IS) territorial control into core areas of Iraq and Syria denied the group one of its most potent propaganda assets. IS' online capabilities in 2018 reflect the overall collapse of the physical caliphate, previously the central pillar of its project. However, this collapse combined with the group's battlefield attrition did not stop the group's online sympathisers from exploiting the internet to advance their cause.

In parallel, the 15 March 2019 right-wing extremism (RWE) motivated terrorist attack on two mosques in Christchurch, New Zealand, has brought about unprecedented elements in the exploitation of the internet for terrorist purposes. The attack's recorded livestreaming video and the gunman's manifesto rapidly went viral and gained digital depth, highlighting new challenges in the fight against terrorist content online.

Terrorist groups boast a diversified online infrastructure

Terrorist groups continue to expand and diversify their conduits for the dissemination of their propaganda online. In doing so, they exploit a wide array of OSPs, which are spread across multiple jurisdictions and differ greatly in terms of size, services offered, business models, and abuse policies. While certain platforms are more abused than others, the sheer number of OSPs exploited for terrorist purposes presents a challenge for disruption efforts. These include forums, file-sharing sites, pastebins, video streaming/sharing sites, URL shortening services, blogs, messaging/broadcast applications, news websites, live streaming platforms, social media sites and various services supporting the creation and hosting of websites (including registries* and registrars**). The ongoing abuse of legitimate services by terrorist groups extends also to VPNs, anonymised cryptocurrencies and DDoS mitigation services.

Faced with the loss of its state-building project and increasingly hostile attitudes towards its online propaganda machine, IS continues to reconfigure its tactics to remain relevant online. In spite of intensified takedown campaigns in 2018 by law enforcement and social media platforms — including Telegram — the group still boasts a highly diversified online infrastructure for the dissemination of its propaganda and persists in publishing on a wide array of media and file-sharing sites, especially smaller platforms with reduced capacity for disruptive actions[64].

Similarly, the spread of terrorist content linked to the Christchurch attack involved the concurrent exploitation of multiple kinds of OSPs by different communities of Internet users, spurred by different motives but a common purpose: making this type of terrorist content viral and resilient.

IS propagandists strive to remain relevant online

IS' critical situation in 2018 had a significant impact on its digital capabilities: propaganda produced by official IS media outlets has visibly declined[65]. The only publication that continued to be issued on a regular basis throughout 2018 was the group's official Arabic weekly newsletter al-Naba' (The News). In their quest for virtual survival, IS and its supporters responded to frequent deletions of content in 2018 by promoting ways to enhance online resilience. Pro-IS media outlets, including the *al-Saqri Corporation for Military Sciences, Horizons Electronic Foundation* and the *United Cyber Caliphate* became more prolific in providing guidelines on cyber and operational security. The instructions ranged from suggesting

* A registry is an organisation that manages the administrative data for the TLD domains and subdomains under its authority, including the zone files that contain the addresses of the name servers for each domain. Source: Google Domains Help, "About registrars and registries", https://support.google.com/domains/answer/3251189?hl=en, 2019.

** A registrar is an organisation that manages the registration of domain names for one or more top-level domain (TLD) registries. Source: Google Domains Help, "About registrars and registries", https://support.google.com/domains/answer/3251189?hl=en, 2019.

secure browsers and privacy-oriented applications to promoting the use of the Tor browser and decentralised platforms. These unofficial but increasingly specialised media outlets also provided advice on how to circumvent account suspension, with suggestions including using channel names and profile pictures that cannot be associated with IS. Additionally, IS sympathisers created multiple versions of the same account, allowing them to swiftly rebound from account suspensions. IS-affiliated websites that act as repositories for the organisation's propaganda responded to recurrent suspensions by creating new domain names and re-emerging at new locations from backup copies, including from and to the dark web. Yet despite its advantageous features in terms of privacy and resilience, the exploitation of the dark web for propaganda dissemination purposes remained limited and propagandists continued to prefer the visibility and reach afforded by the surface web.

IS continue to seek out new vectors for their online propaganda

Terrorist groups continue to lay claim to a degree of technological adaptability and are often early adopters of new technologies. A case in point is IS' seemingly coordinated and near-synchronous shift to open source, decentralised platforms***. In the aftermath of an intense suspension campaign carried out by Telegram in late 2018, IS supporters on Telegram started advocating for the use of alternative platforms and software. Since then, the IS has established a presence on a number of open source, decentralised platforms. Accounts and pages disseminating mostly official IS propaganda have been created on Mastodon, Nextcloud, Rocket.Chat and ZeroNet. The resilient character of these platforms, coupled with multiple options for anonymity and enhanced usability, are all features that play into the online communication and distribution strategies of terrorist groups.

However, jihadist activities on these platforms failed to gain traction in 2018. This is probably due to the alternative platforms' smaller user base and weaker outreach capabilities. Thus, Telegram remains the platform of choice for terrorist sympathisers, who continue to exploit its advantageous encryption and file-sharing capabilities.

Terror goes viral with Christchurch mosques attack

The Christchurch attack marks a defining point in the fight against terrorist content online: the attack was livestreamed and its recording, alongside the gunman's manifesto, spread rapidly online. The exceptional virality, velocity and volume of the materials' online diffusion points to a savvy use of internet technologies and communication, not only by the attacker, but by multiple communities of internet users, beyond RWE sympathisers.

The interplay of online communities who share the same Internet slang and memes contributed to the widespread dissemination of the content and its digital endurance.

Internet users have adopted different techniques to circumvent disruption efforts by OSPs. In particular, edited versions of the Christchurch video appeared to fly under the radar of detection measures enforced by OSPs. Reponses by practitioners and OSPs could not measure up to the scale of online dissemination and with the existing cooperation frameworks keeping terrorist content at bay remains challenging.

8.3 » RECOMMENDATIONS

Limiting the ability of terrorists to carry out transnational attacks by disrupting their flow of propaganda and attributing online terrorism-related offences requires continued and heightened counterterrorism cooperation and information sharing across law enforcement authorities, as well as with the private sector.

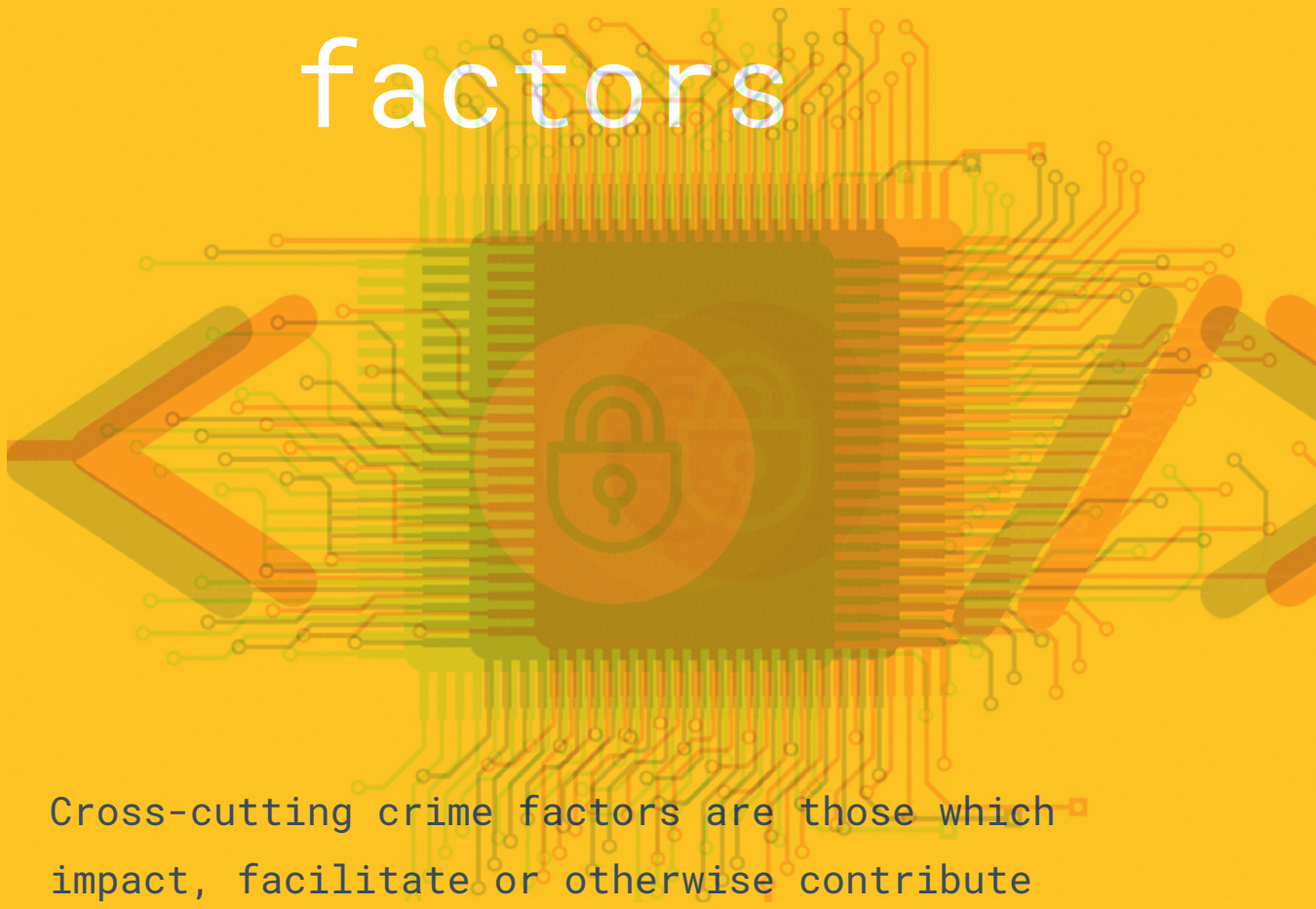
Any effective measure to counter terrorist groups' online propaganda and recruitment operations entails addressing the whole range of abused OSPs, especially start-ups and smaller platforms with limited capacity for response.

Cross-platform collaboration and a multi-stakeholder crisis response protocol on terrorist content online would be essential to crisis management the aftermath of a terrorist attack.

A better understanding of new and emerging technologies is a priority for practitioners. Upcoming policy debates and legislative developments should take into account the features of these technologies in order to devise an effective strategy to prevent further abuse.

*** Decentralised systems are a particular type of distributed system where no single entity is in control of the underlying infrastructure. Source: Blockstack PBC, *Blockstack Technical Whitepaper v2.0*, 2019.

#9 cross-cutting crime factors



Cross-cutting crime factors are those which impact, facilitate or otherwise contribute to multiple crime areas but are not necessarily inherently criminal themselves.

9.1 » KEY FINDINGS

- Phishing remains an important tool in the arsenal of cybercriminals for both cyber-dependent crime and NCPF.
- While cryptocurrencies continue to facilitate cybercrime, hackers and fraudsters now routinely target crypto-assets and enterprises.

criminal case study

GDPR entered into effect across the EU in May 2018 (see also section 4.3). Prior to this, many companies sent out emails to their customers, detailing privacy policies and the rights of their customers concerning their data. It was not long before criminals exploited these legitimate messages with a wave of copycat phishing emails. These malicious emails would typically contain links to fake sites that would then capture victims' data to be used or sold by the cybercriminals.

case study

In March 2019, the Spanish Civil Guard, as part of operation Neptuno, dismantled a criminal organisation dedicated to scamming victims through phishing. The investigation originated in September 2018, when an increase in complaints related to banking scams were detected, whose common link was the withdrawal of money from the bank accounts of the victims. The perpetrators sent out phishing emails pretending to be one of six banks.

The operation has resulted in 11 people arrested, aged between 17 and 28 years of age. In addition, police seized several laptops, more than 20 mobile phones, EUR 7 500 in cash, notes with identity documents and access codes to online banking, virtual currencies (bitcoin) and bankcards.

9.2 » SOCIAL ENGINEERING

Social engineering, and in particular phishing, overwhelmingly represented the most significant cross-cutting cyber-threat faced by both European cybercrime investigators, and the most significant cyber-threat overall by Europol's private sector partners.

Phishing — a core attack method for all cybercrime

Both investigators of cyber-dependent crime and NCPF highlighted phishing as a key threat. In cases related to NCPF, perpetrators primarily used phishing to gather personal banking credentials, payment card data, or other login credentials. Criminals either sell such data on underground markets, or use it directly to commit fraud.

In cases related to cyber-dependent crime, criminals also use phishing to gain login credentials. However, as highlighted in section 4.2, it is also currently the dominant malware delivery method, through either malicious attachments, or links to malicious URLs. Either may ultimately lead to attackers gaining unauthorised access to a private network.

Some law enforcement respondents note how criminals use some phishing attacks for extortion. Attackers can create a pretext either based on genuine data found on the internet from a previous data breach, or a purely fictitious scenario to extort money from a victim. Such extortions are often of a sexual nature.

While the financial sector is, and always will be, a significant target for such attacks, industry reporting indicates that most phishing attacks are currently targeting Software-as-as-Service such as cloud services, and webmail[66].

Even though phishing remains an ongoing challenge, certain solutions or mitigating measures do exist. Domain-based message authentication, reporting and conformance (DMARC) is one such option, which has been introduced years ago. DMARC is an email authentication, policy, and reporting protocol. DMARC makes it easier for email senders and receivers to determine whether or not a given message is legitimately from the sender and what to do if it is not. This makes it easier to identify spam and phishing messages and keep them out inboxes. Yet, according to one study, DMARC adoption is non-existent at 80 % of organisations[67]. This is a missed opportunity as the United Kingdom National Cyber Security Centre (UK NCSC) demonstrates

65 % of targeted attack groups used spear phishing as the primary infection vector [70]

32 % breaches involve phishing [73]

48 % of malicious email attachments are office files [71]

1 in 3 207 emails are phishing emails [74]

IN 2018

up to 0.55 % of all incoming emails were phishing emails [72]

phishing was present in 78 % of cyber espionage incidents [75]

how it has achieved recent success by using 'Synthetic DMARC.' This 'works by assigning a DMARC record for all domains attempting to pass-off as gov.uk domains, by analysing and vetting non-existing subdomains against DNS records and building on authentication systems of the past[68].' Because of the technology, the UK NCSC has been able to stop 140 000 separate phishing attacks in the last year and has taken down a record 18 067 phishing sites. This is a noticeable improvement when compared to the takedown rate of 14 124 in 2018[69]. The technology comes with its challenges, namely from an interoperability perspective, but still provides promising results for those able to implement it.

9.3 » MONEY MULES

Money mule activity continues to support all aspects of cybercrime

The use of money mules to launder criminal funds was the second most prominent cross-cutting threat highlighted by European law enforcement. Again, this pertained to both cyber-dependent crime and NCPF investigations, although the majority of references related to the latter.

While this was a top threat, law enforcement did not identify new *modi operandi* this year. Instead, they confirmed the use of typical recruitment methods such as job advertisements targeting disadvantaged or low-income individuals. In some instances, perpetrators recruited mules with a stronger financial standing, allowing them to open corporate accounts through which the funnelling of international funds may attract less attention.

case study

In 2018, over the course of three months, law enforcement and private sector partners from over 30 countries participated in the fourth European Money Mule Action (EMMA). Europol, Eurojust, the EBF and more than 300 banks supported the initiative.

The action resulted in the identification of over 1 500 money mules and 140 money mule organisers, and over 168 arrests. Financial sector participants reported 26 376 fraudulent money mule transactions, preventing an estimated loss of over EUR 36 million.

The campaign also raised awareness of the dangers of becoming a money mule throughout the participating nations.

“I thought it was part of the job”

MONEY MULING HELPS PERPETRATE CRIME

IGNORANCE IS NO EXCUSE

Criminals will try to dupe innocent victims into laundering money on their behalf by making the job offer seem as legitimate as possible.

Be wary of adverts that are poorly written with grammatical errors and spelling mistakes.

#dontbeaMule

Created by Europol

EUROPOL EC3 European Cybercrime Centre

EUROJUST

EBF European Banking Federation

9.4 » THE CRIMINAL ABUSE OF CRYPTOCURRENCIES

In previous years' reports, we have extensively highlighted the criminal abuse of cryptocurrencies across all areas of cyber-related criminality due to the perceived level of anonymity they provide. This trend persists as investigators of cyber-dependent crime and NCPF report that these currencies continue to pose investigative challenges for law enforcement. Crypto investigations are now a core part of daily business for law enforcement. As a result, investigators require training to ensure they have the appropriate skills to handle such investigations.

Predominantly, such currencies play an essential role in the underground economy. They are used for most criminal to criminal (C2C) payments on criminal forums and marketplaces. In addition to C2C payments, many attackers demand payment from victims for attacks such as ransomware or DDoS extortion by cryptocurrencies. Such criminally obtained funds, while already inherently challenging to trace, are often further laundered through mixing services, which serve to obfuscate the financial trail.

Crypto-assets now routinely targeted by fraudsters

The most apparent development with regards to cryptocurrencies, first highlighted in last year's report, is that attacks and frauds which historically targeted other payment systems or fiat currencies have now been adapted to incorporate cryptocurrencies. As such, we now routinely see malware and phishing targeting crypto-investors and enterprises, and new frauds, such as investments frauds related to cryptocurrency investment. Such approaches may be more successful due to the lower levels of knowledge potential victims are likely to have about these assets.

Cryptojacking remains an issue, but not a priority

Cryptojacking remains an issue. The activity appears to have peaked in 2018 and decreased throughout 2019, partially due to the shut down of Coinhive, the most popular mining script, in March. The most suitable cryptocurrencies were those that are memory intensive, meaning that they are suitable for CPU or GPU mining, and that are difficult to trace; Monero ticked both boxes, as such it was the first choice for this type of abuse. Although these incidents affect many, the damage per victim is typically low and thus such abuse is rarely reported (see also 4.7).

While we have previously reported a small shift towards more privacy-focused cryptocurrencies such as Monero, Bitcoin still remains the currency of choice for both legitimate and criminal use. The main developments regarding this trend are on the Darknet markets, several of which also accept Monero, or in some cases exclusively trade in it.

case study

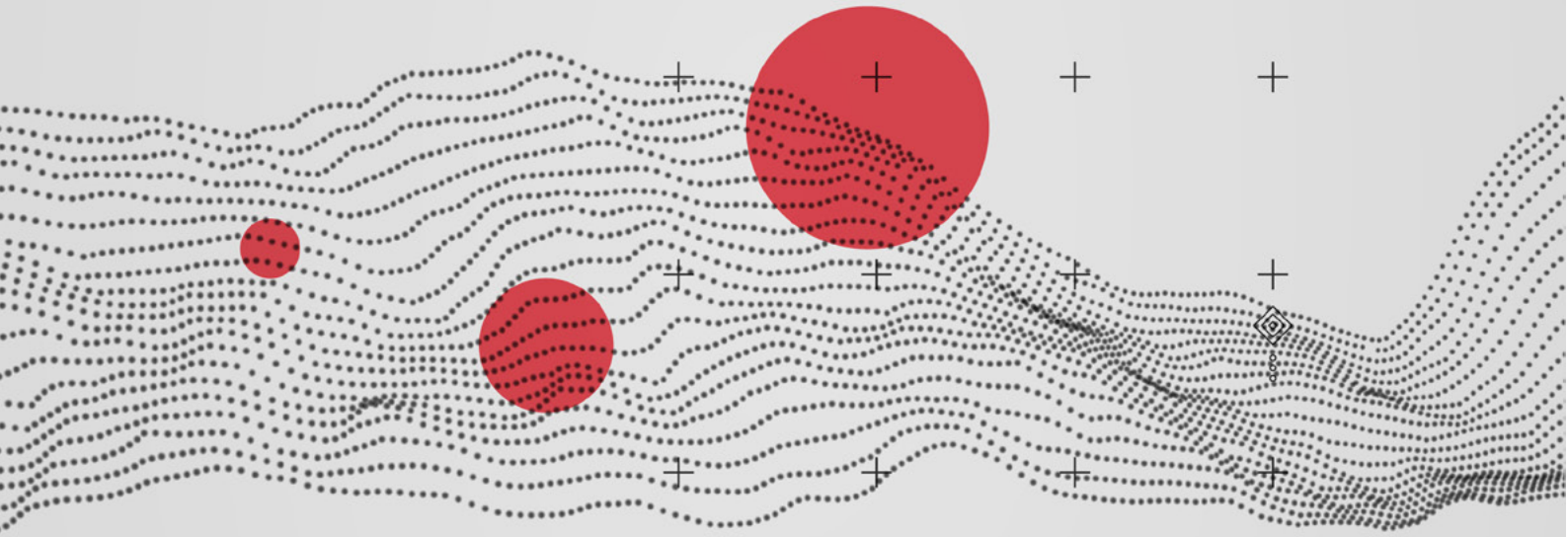
In June 2019, six offenders were arrested in the UK and the Netherlands after a 14-month investigation into phishing activities that netted the perpetrators over EUR 24 million in cryptocurrencies. The phishing relied on typosquatting, where a large number of websites belonging to well-established cryptocurrency wallets and exchanges were recreated by criminals with the sole purpose of stealing users' credentials and funds.

While phishing is commonplace across both traditional financial as well as cryptocurrency sector, what makes this operation unique was the scale — over 4 000 victims had their funds stolen with the numbers continuing to grow.

The operation was another demonstration of exemplary cooperation between law enforcement and the private sectors, particularly security researchers and cryptocurrency exchanges.

> Global uptakes of digital currencies, combined with proliferation of AI-based applications, are gradually becoming the main means of exchanging goods and services. The key challenge for law enforcement agencies and other stakeholders such as national/international authorities and financial services are to protect public and economy against full spectrum of criminal acts using artificial intelligence and digital currencies (e.g. cyber-enabled fraud, misuse of personal data, money laundering, serious and organised crime to CSE).

— PROFESSOR BABAK AKHGAR, DIRECTOR OF CENTRIC, UK



> As technology continues to become more complex and distributed systems even more intertwined fewer people understand the dependencies and interaction patterns. One particularity interesting form of distributed systems are cryptocurrencies and smart contracts. They are based on assumptions some of which are still poorly understood. There is a risk in wide-spread adoption because attacks have huge immediate financial implications; correctly working financial incentives are, however, a basic building block of public blockchains. Attacks can be executed globally at unprecedented speeds and difficult to fix.

— DR EDGAR WEIPPL, SBA RESEARCH, AUSTRIA

9.5 » COMMON CHALLENGES FOR LAW ENFORCEMENT

Much of the IOCTA is focused on the threat posed by criminal actors and their *modi operandi.* At the same time, it is crucial to reflect on how law enforcement can and does respond to these threats, and what barriers the law enforcement and judicial community encounter in responding. In June 2019, Europol and Eurojust revisited their joint 2017 paper on the *Common Challenges in Combatting Cybercrime* with a fresh look at how these challenges developed over the preceding two years. Many of these challenges are not unique to cybercrime and cut across all areas of serious organised crime and terrorism.

These challenges are extremely relevant to this assessment and therefore we will summarise some of the most pertinent issues. For full details, including ongoing activities and open issues, readers should refer to the full report[76].

The key challenges remain unchanged and fall into five main areas of discussion.

The loss of data

This refers to several legislative changes and technologies that effectively either deny law enforcement access to data or have resulted in there being limited or no data for law enforcement to access for a criminal investigation. The overturning of the Data Retention Directive in 2014 and the implementation of the GDPR in 2018 has deprived law enforcement of a number of key sources of data, namely communications data and WHOIS data. In contrast, the wide-scale implementation of carrier-grade network address translation technologies by internet service providers results in often prohibitively large volumes of data (as one IPv4 address may be shared by multiple end-users at one).

In last year's report, we highlighted the impact of WHOIS 'going dark', particularly in the scope of cyber investigations. In September 2018, ICANN published the draft results of a survey that directly measured the impact of the unavailability of WHOIS data. Almost 26 % of respondents indicated that it had resulted in investigations being discontinued, with a further 52 % indicating that it delayed investigations to some degree. Moreover, only 33 % of respondents indicated that WHOIS (at least partially) met their investigative needs, compared to 98 % prior to the changes[77].

Encryption, while recognised as an essential element of our digitised society, also facilitates significant opportunities for criminals. Investigative techniques, such as lawful interception, are becoming increasingly ineffective (or even impossible) as criminals exploit encrypted communication services, applications and devices. Similarly, criminals can deny forensic

investigators access to critical evidence by encrypting their data. The criminal abuse of encryption technologies, whether it be anonymisation via VPNs or Tor, encrypted communications or the obfuscation of digital evidence (especially in cases of CSEM), was a significant threat highlighted by respondents to this year's IOCTA survey.

Cryptocurrencies are another application of encryption technology, and, as outlined in 13.4, also present significant challenges for law enforcement[78].

The loss of location

The increasing level of criminal use of encryption and/or anonymisation tools, crypto-currencies and the Dark Web, as well as the growing use of cloud-based technologies, have also led to situations in which law enforcement may no longer (reasonably) establish the physical location of perpetrators, criminal infrastructure or electronic evidence. The territoriality-based investigative powers and jurisdiction of the competent national authorities offer no appropriate tools to tackle these situations.

Challenges associated with national legal frameworks

Differences between domestic legal frameworks in the member states and international instruments continue to be a serious impediment to the international criminal investigation and prosecution of cybercrime. The main differences relate to the criminalisation of conduct and provisions to investigate cybercrime and gather e-evidence. For example, should legislation that regulates law enforcement presence and action in an online environment be harmonised at EU level, this would allow for more effective joint operational actions such as large-scale botnet takedowns, or increased possibilities to monitor criminal activities online and to lawfully collect critical evidence on the Deep Web and Dark Web.

Obstacles to international cooperation

The lack of a common legal framework which exists for the expedited sharing of evidence continues to hamper criminal investigations and judicial proceedings, with the current process of Mutual Legal Assistance being perceived as too slow to gather and share electronic evidence effectively. The use of the European Investigation Order (EIO) may go some way towards addressing these issues for the majority of Member States, but may not provide the speed that is required to capture electronic evidence.

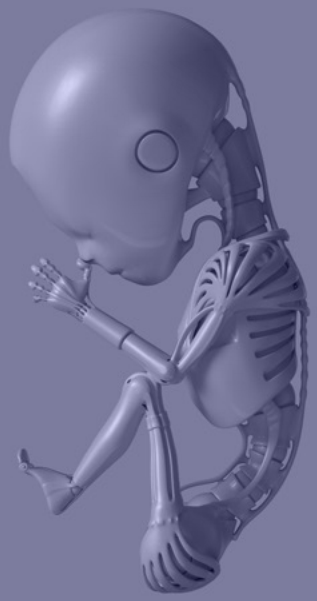
Another issue under this banner is law enforcements ability to respond to large-scale cyber-attacks, particularly where such attacks rapidly affect multiple industries across a range of sectors and geographies, such as the WannaCry and NotPetya attacks of 2017. Such attacks constitute a specific challenge to international cooperation.

Challenges of public-private partnerships

The private sector plays a key role in many cyber investigations and cybersecurity activity, being the custodians of crucial data, having essential capabilities in the takedown of criminal infrastructures and removal of illicit content. Public-private partnerships also play a key role in mitigating cybercrime and increasing cybersecurity through prevention and awareness. There is, however, little consensus on the legal framework that is required to facilitate effective and trust-based cooperation with the private sector, while at the same time regulating legal and transparency issues surrounding that cooperation.

This challenge also includes those associated with new and emerging technologies. The criminal misuse of technology has become an engine of cybercrime, although many of these technologies can be equally dual-purposed to assist law enforcement. Technologies such as quantum computing, and artificial intelligence may have applications at both ends of the lawful spectrum*.

* For a more extensive description of these please see: Europol & Eurojust, *First Report of the Observatory Function on Encryption,* 2019.



> If the speed of developments with regard to quantum computing continues (currently already exceeding 50 qubit) this has the potential to end the effectiveness of currently used encryption methods within the next five years. Within the same time period, it is likely that while artificial intelligence is not capable to fully draw level with human strengths it is surpassing what is necessary to exploit human weaknesses. As a consequence we will most likely see an increasing use of artificial intelligence in areas of crime where it is currently not utilised.

— PROFESSOR DR MARCO GERCKE, UNIVERSITY OF COLOGNE, GERMANY

9.6 » FUTURE THREATS AND DEVELOPMENTS

To combat phishing, leading platform providers are investing in engineering to deploy machine learning and other AI-based approaches, leveraging the newest technologies to protect consumers. However, enterprise adoption and deployment of these technologies is slow, therefore phishing is likely to continue to be a primary attack vector for attack for the near future. Equally, criminals will apply such methods too to bypass these systems.

The incorporation of innovation, as part of an effective crime response, however, is not exclusively a private sector affair. Europol already works together with industry partners and the European Commission to identify challenges and opportunities for law enforcement arising from new and emerging technologies, such as 5G. However, to tackle previously identified as well as future challenges, one consideration is to establish a hub for law enforcement innovation, bringing together the most relevant partners, tailored to the needs of Member States' law enforcement authorities. Such an entity could enhance the EU's ability to articulate an operational vision of innovation with-in the realm of internal Security, to decide on key partnerships, critical investments and be ready for future disruptions. The objective would be to identify and categorise common challenges in the area of innovation and emerging technologies in order to provide guidance and opportunities for EU Law Enforcement in these areas as well as to inform research priorities[79].

In July 2018, the 5th EU Anti-Money Laundering Directive (AMLD 5) entered into force. With 18 months to transpose the new Directive into national legislation, all member states should adopt the Directive by the closure of 2019. One of the key changes proposed by the Directive was the regulation of virtual currency platforms (exchanges) and custodian wallet providers (wallet services where the service holds its users' private keys). Such entities will be required to apply full customer due diligence, thereby de-anonymising their clients, and to report suspicious transactions to financial intelligence units.

While this new legislation may capture a significant proportion of cryptocurrency users, those using hardware or software wallets, or trading via other peer-to-peer exchange systems, can still operate largely anonymously[80]. Similarly, users of privacy-orientated cryptocurrencies such as Dash and Monero, until they are required to interact with a virtual currency exchange or add their holdings to a custodian wallet provider can also remain anonymous.

How the criminal community will react to these developments remains to be seen. However, it is likely we will see the rise of criminal exchange services operating on the digital underground, exchanging fiat and cryptocurrencies outside the regulated sector.

case study

In May 2019, the Dutch Fiscal Information and Investigation Service (FIOD), in close cooperation with Europol and the authorities in Luxembourg, took down on one of the world's leading cryptocurrency mixing service Bestmixer.io. The operation, which was initiated in 2018 by the FIOD with the support of the internet security company McAfee, resulted in the seizure of six servers in the Netherlands and Luxembourg. Bestmixer.io was one of the three largest mixing services for cryptocurrencies and offered services for mixing bitcoins, bitcoin cash and litecoins. The service started in May 2018 and achieved a turnover of at least USD 200 million (approx. 27 000 bitcoins) over one year.

The operation had a significant impact on the mixer community, resulting in at least one other mixing service voluntarily shutting down[81].

9.7 » RECOMMENDATIONS

Law enforcement and the judiciary must continue to develop, share and propagate knowledge on how to recognise, track, trace, seize and recover cryptocurrency assets.

Law enforcement must continue to build trust-based relationships with cryptocurrency-related businesses, academia, and other relevant private sector entities, to more effectively tackle issues posed by cryptocurrencies during investigations.

Despite the gradual implementation of AMLD 5 across the EU, investigators should be vigilant concerning emerging cryptocurrency conversion and cash-out opportunities, and share any new information with Europol.

REFERENCES

1 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

2 Europol, *European Union Serious and Organised Crime Threat Assessment: Crime in the age of technology,* 2017.

3 McGuire, M & Dowling, S., "Cyber crime: A review of the evidence", *UK Home Office Research Report 75*, 2013.

4 Symantec, *Internet Security Threat Report (ISTR) Vol. 24, 2019; IBM, X-Force Threat Intelligence Index, 2019; Microsoft, Microsoft Security Intelligence Report Vol. 23*, 2018.

5 EC3 Advisory Groups.

6 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

7 Symantec, *Internet Security Threat Report (ISTR) Vol. 24*, 2019.

8 https://blog.erratasec.com/2019/05/almost-one-million-vulnerable-to.html#.XUvgvm9LiUk

9 https://www.zdnet.com/article/cyberattacks-against-industrial-targets-double-over-the-last-6-months/#ftag=RSSbaffb68

10 https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks-for-ransom/

11 Newman, L., "Ransomware Hits Georgia Courts as Municipal Attacks Spread", https://www.wired.com/story/ransomware-hits-georgia-courts-municipal-attacks-spread/, 2019.

12 https://www.zdnet.com/article/louisiana-governor-declares-state-emergency-after-local-ransomware-outbreak/

13 Liska, A., "Early Findings: Review of State and Local Government Ransomware Attacks", https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf, 2019.

14 Jay, J. "Formjacking attacks compromised over 50,000 retailer websites in 2018", https://www.scmagazineuk.com/formjacking-attacks-compromised-50000-retailer-websites-2018/article/1526282, 2019; Stone, J. "British Airways fined $229 million under GDPR for data breach tied to Magecart", https://www.cyberscoop.com/british-airways-gdpr-fine-magecart/, 2019.

15 https://www.zdnet.com/article/at-t-employees-took-bribes-to-plant-malware-on-the-companys-network/

16 https://www.scmagazine.com/home/security-news/capital-one-breach-exposes-not-just-data-but-dangers-of-cloud-misconfigurations/; https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/

17 Weinbaum, N, "The GDPR- One Year Later", https://securingtomorrow.mcafee.com/business/data-security/the-gdpr-one-year-later/, 2019.

18 King, A. & Weaver, R., "GDPR One Year Later: What We've Learned So Far", https://www.fireeye.com/blog/executive-perspective/2019/05/gdpr-one-year-later-what-we-ve-learned-so-far.html, 2019.

19 O'Flaherty, K., "British Airways Hit With Record Fine Following 2018 Cyberattack", https://www.forbes.com/sites/kateoflahertyuk/2019/07/08/british-airways-hit-with-record-fine-following-2018-cyberattack/#795491d21f8e, 2019.

20 Sweney, M., "Marriott to be fined nearly £100m over GDPR breach", https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico, 2019.

21 Van der Meulen, *Investing in Cybersecurity*, 2015.

22 Boiten, E., "Nearly £100m for Marriott, £138m for BA- what is the take home message from these sudden massive ICO fines?", https://www.computing.co.uk/ctg/opinion/3078677/gdpr-marriott-ba-ico-massive-fines, 2019.

23 Symantec, Internet Security Threat Report (ISTR) Vol. 24, 2019.

24 Microsoft, "Attack inception: Compromised supply chain within a supply chain poses new risks", https://www.microsoft.com/security/blog/2018/07/26/attack-inception-compromised-supply-chain-within-a-supply-chain-poses-new-risks/, 2018.

25 Zetter, K., "Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers", https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers, 2019.

26 Cimpanu, C. "Dark web crime markets targeted by recurring DDoS attacks", https://www.zdnet.com/article/dark-web-crime-markets-targeted-by-recurring-ddos-attacks/, 2019; Crawley, K. "What about all those Dark Web DDoS attacks?", https://www.peerlyst.com/posts/what-about-all-of-those-dark-web-ddos-attacks-kimberly-crawley, 2019.

27 Europol, "Authorities Across the World Going After Users of Biggest DDoS-for-hire Website", https://www.europol.europa.

eu/newsroom/news/authorities-across-world-going-after-users-of-biggest-ddos-for-hire-website, 2019.

28 Akamai, "Memcached DDoS explained", https://www.akamai.com/us/en/resources/our-thinking/threat-advisories/ddos-reflection-attack-memcached-udp.jsp.

29 Cloudflare, "Memcached DDoS Attack", https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/.

30 Shani, T., "Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important", https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/, 2019.

31 European Commission, *Communication from the Commission to the European Parliament, the European Council and the Council: Nineteenth Progress Report towards an effective and genuine Security Union,* 2019; Fiott, D. & Parkers, R., *Protecting Europe: the EU's response to hybrid threats,* 2019.

32 Group-IB, "Two hacker groups attacked Russian banks purporting to be Central Bank of Russia", https://www.group-ib.com/media/cbrf-double-attack/, 2019.

33 Canellis, D., "North Korean hacker crew steals $571M in cryptocurrency across 5 attacks", https://thenextweb.com/hardfork/2018/10/19/cryptocurrency-attack-report/, 2018.

34 Stolarchuk, J., "Hackers hit government agencies and banks hard in Singapore", http://theindependent.sg/hackers-hit-government-agencies-and-banks-hard-in-singapore/, 2019.

35 Chainalysis, *Crypto Crime Report: Decoding increasingly sophisticated hacks, darknet markets, and scams,* 2019; CipherTrace, *Cryptocurrency Anti-Money Laundering Report,* 2018.

36 CERT-EU, *Threat Landscape Report Q1 2019,* 2019.

37 Zamora, W. "TrickBot takes over as top business threat", https://blog.malwarebytes.com/101/2018/11/trickbot-takes-top-business-threat/, 2018.

38 IBM, *X-Force Threat Intelligence Report,* 2019.

39 Palmer, D., "This new cryptomining malware targets Business PCs and servers", https://www.zdnet.com/article/this-new-cryptomining-malware-targets-business-pcs-and-servers/, 2018.

40 Symantec, *"Beapy: Cryptojacking Worm Hits Enterprises in China",* https://www.symantec.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china, 2019.

41 Wikipedia, "Memcached", https://en.wikipedia.org/wiki/Memcached, 2019.

42 Akamai, *State of the Internet Report,* 2018.

43 Trend Micro, "2018 Mobile Threat Landscape", https://www.trendmicro.com/vinfo/in/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape, 2019.

44 Inhope, *Inhope Statistics 2018,* 2019; Internet Watch Foundation, *Once upon a year,* 2018; Netclean, Netclean *Report 2018: A report about child sexual abuse crime,* 2018.

45 Analysis Project Twins.

46 Internet Watch Foundation, *Once upon a year,* 2018; Netclean, *Netclean Report 2018: A report about child sexual abuse crime,* 2018.

47 Analysis Project Twins.

48 Farinelli, B., "Could a Magecart Attack Hit Your E-Commerce Website?", https://blog.clear.sale/could-a-magecart-attack-hit-your-e-commerce-website, 2019; see also: Cimpanu, C., "New Magecart attacks leverage misconfigured S3 buckets to infect over 17K sites", https://www.zdnet.com/article/new-magecart-attacks-leverage-misconfigured-s3-buckets-to-infect-over-17k-sites/, 2019.

49 Alberts, A., "Why Online Fraud Prevention Controls are Failing", https://medium.com/@aalberts/why-online-fraud-prevention-controls-are-failing-ba90d7036c4f, 2019.

50 Preminger, B., "23 Million Stolen Credit Cards for Sale on the Dark Web in the First Half of 2019", https://www.cybersixgill.com/stolen_credit_cards/, 2019.

51 European Central Bank, "Card Fraud Report", https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html, 2019.

52 European Payments Council, *2018 Payment Threats and Fraud Trends Report,* 2018.

53 European Payments Council, *2018 Payment Threats and Fraud Trends Report,* 2018.

54 Barret, B., "ATM Hacking Has Gotten So Easy, The Malware's A Game", https://www.wired.com/story/atm-hacking-win-pot-jackpotting-game/, 2019.

55 Barrett, "ATM Hacking Has Gotten So Easy, The Malware's A Game", 2019.

56 Federal Bureau of Investigation, "Business e-mail compromise the 12 billion scam", https://www.ic3.gov/media/2018/180712.aspx, 2018.

57 Seals, T., "ATM Jackpotting Malware Hones Its Heist Tools", https://threatpost.com/atm-jackpotting-malware-win-pot/141960/, 2019.

58 Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

59 European Banking Authority, *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2,* 2019.

60 Fortuna, P., "Is Security The Loser As Open Banking Takes Hold?", https://www.infosecurity-magazine.com/opinions/security-loser-open-banking/, 2019.

61 Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA.

62 Europol, *Do Criminals Dream of Electric Sheep?,* 2019, p. 13.

63 Kharif, O., "Bitcoin Criminals Set to Spend $1 Billion on Dark Web This Year", https://www.bloomberg.com/news/articles/2019-07-01/bitcoin-criminals-set-to-spend-1-billion-on-dark-web-this-year, 2019.

64 Europol, *European Union Terrorism Situation and Threat Report,* 2019, p. 39.

65 Europol, *European Union Terrorism Situation and Threat Report,* 2019, p. 34.

66 APWG, *Phishing Activity Trends Report*, 1st Quarter 2019; Europol Advisory Groups.

67 Seals, T., "ThreatList: DMARC Adoption Nonexistent at 80 % of Orgs", https://threatpost.com/dmarc-adoption-nonexistent/146751/, 2019.

68 Abbott, C. & Aggromito, M., "The Battle Against Phishing", https://www.natlawreview.com/article/battle-against-phishing, 2019.

69 National Cyber Security Centre, *Active Cyber Defence: The Second Year,* 2019.

70 Symantec, *Internet Security Threat Report Vol. 24,* 2019.

71 Symantec, *Internet Security Threat Report Vol. 24,* 2019.

72 Microsoft, *Microsoft Security Intelligence Report Vol. 23,* 2018.

73 Verizon, *Data Breach Incident Report,* 2019.

74 Symantec, *Internet Security Threat Report Vol. 24,* 2019.

75 Verizon, *Data Breach Incident Report,* 2019.

76 Europol & Eurojust, "Common challenges in combatting cybercrime", https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime, 2019.

77 ICANN, *Registration Directory Services (RDS)-WHOIS2 Review,* 2019, p. 24.

78 Europol, *Do Criminals Dream of Electric Sheep?,* 2019, p. 13.

79 Europol, *Do Criminals Dream of Electric Sheep?,* 2019, p. 21.

80 European Parliament, *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion,* 2018.

81 Redman, J., "Mixing Service Bitcoin Blender Quits After Bestmixer Takedown", https://news.bitcoin.com/mixing-service-bitcoin-blender-quits-after-bestmixer-takedown/, 2019.

IOCTA
[2019]

EUROPOL | EC3 European Cybercrime Centre

www.europol.europa.eu