European
Payments Council

[x] Public – [] Internal Use – [] Confidential – [ ] Strictest Confidence
Distribution:

2018 PAYMENT THREATS AND FRAUD

TRENDS REPORT

Abstract	This new edition of the threats trends report reflects the recent development concerning security threats and fraud in the payments landscape over the past year.
Document Reference	EPC211-18
Issue	Version 1.0
Date of Issue	1 December 2018

Table of Contents

List of Tables

Executive Summary

The overall purpose of the EPC is to support and promote European payments integration and development, notably the Single Euro Payments Area (SEPA) (see Annex I and http://www.epc-cep.eu). Since security is one of the cornerstones of customers' trust in payment systems, the EPC decided to devote a yearly report to the latest trends in security threats impacting payments while also giving an insight on how these (could) create payment fraud and how to mitigate these risks. By developing this report, the EPC aims to enhance the security awareness amongst the various stakeholders in the payment ecosystem.

The document provides an overview of the most important threats in the payments landscape, including social engineering and phishing, malware, Advanced Persistent Threats (APTs), mobile device related attacks, (Distributed) Denial of Service ((D)DoS), botnets and threats related to cloud services, big data, Internet of Things (IoT) and virtual currencies. For each threat, apart from a definition and description, an analysis is made on the impact and context and suggested controls and mitigations are described. An overview matrix listing the threats with the main controls and mitigation measures is provided in Annex II.

The description of the threats is followed by a section that elaborates on fraud related to payment instruments (cards, SEPA Credit Transfers and SEPA Direct Debit), while conclusions are presented in the final section.

The following main conclusions concerning payment threats may be derived from this report:

- The organisation and sophistication of recent cyberattacks have shown a greater degree of professionalism of cybercriminals.
- The main attack focus has shifted slightly away from malware to social engineering attacks, except for attacks aimed at companies.
- Social engineering attacks and phishing attempts are still increasing and they remain instrumental often in combination with malware, with a shift from consumers, retailers, SMEs to company executives, employees (through "CEO fraud"), financial institutions and payment infrastructures.
- Malware remains a major threat, more in particular ransomware has been on the rise during the past year, requiring new mitigating measures.
- One of the most lucrative types of payment fraud now and for the future seems to be Advanced Persistent Threats (APTs). It must be considered as a potential high risk not only for the payment infrastructures but also for all network related ecosystems.
- More and more, mobile devices are becoming an attractive target for cyber criminals, along with the IoT devices.
- The number of (D)DoS attacks is still growing and they are frequently targeting the financial sector.
- There is a continuation of botnets and because of the high volume of infected consumer devices (e.g. PCs, mobile devices, etc.) severe threats remain.
- The adoption of cloud services and big data analytics technologies which results in data stored "everywhere" are bringing new opportunities to businesses but new risks too.

- Another phenomenon that is appearing in the market is "cybercrime-as-a-service", causing huge challenges in view of the automation level achieved.
- Multi-vector attacks are becoming commonplace and have been targeting a number of financial institutions over the past year.

Next to the threats, there remains a competitive market drive for user-friendliness and simplicity which leads to increased pressure on security resources and difficult trade-offs to be made by payment service providers (PSPs). The challenge will be to find the right balance between the user-friendliness and the security measures needed.

As security becomes more regulated (NIS Directive [5], GDPR [6], PSD2 [6]), payments also face a new regulatory landscape in Europe, which on one hand increases the security barrier with respect to fraud (e.g. customer authentication) but at the same time also "opens up" the payment value chain which introduces new security challenges for all stakeholders involved.

The following main conclusions concerning payment fraud may be derived from this report:

- Concerning card payment fraud, as long as the mag-stripe is needed for international transactions, skimming will remain an issue. Criminals are changing their approach to fraud. Not only by changing to more high tech frauds like APT, but also a part of the criminals is reverting to old school types of fraud such as lost and stolen. As e-commerce is still on the rise, CNP fraud remains a significant factor for fraud losses.
- For SEPA Credit Transfer and Direct Debit transactions, the criminals' use of impersonation and deception scams, as well as online attacks to compromise data, continue to be the primary factors behind fraud losses. Hereby criminals target personal and financial details which are used to facilitate fraudulent transactions.

An important aspect to mitigate the risks and reduce the fraud related to payments is the sharing of fraud intelligence and information on incidents amongst PSPs. However, often this is being limited by existing regulations related to data protection, even more so in the case of cross-border sharing. It is to be expected that the new EBA guidelines on fraud reporting [2] will support an improved information sharing and more accurate fraud figures.

Moreover, new mechanisms should be put in place to enable cybercriminal prosecution within the European Union and internationally.

Finally, PSPs must understand the emerging threats, the possible impacts and should keep investing in appropriate security and monitoring technologies as well as in customer awareness campaigns.

1 Document information

1.1 Structure of the document

This section describes the structure of this report. Section 1 provides the references, definitions, and abbreviations used in this document. The next section provides some general information about the EPC and its vision, scope and audience of the document. Section 3 analyses threats which are encountered nowadays in payment contexts and are causing fraud. Section 4 elaborates on fraud related payment instruments. Conclusions of this report may be found in Section 5. Annex I provides a brief overview on the SEPA payment instruments. Finally, Annex II contains a summary of the threats and the main suggested controls and mitigation measures for each threat.

1.2 References

This section lists the main references mentioned in this document. Square brackets throughout this document are used to refer to a document in the list. Other references are included as footnotes throughout the document.

Ref nr	Document	Author
[1]	EBA/GL/2017/17 Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)	EBA
[2]	EBA/GL/2018/05 Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2)	EBA
[3]	Payment Services Directive (PSD2) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payments 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	EC
[4]	Commission delegated regulation (EU) 2018/189 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as 'RTS')[1]	EC
[5]	Network Information Security Directive (NIS Directive)	EC

[1] See also EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC,

(https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf)

	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	
[6]	General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC	EC
[7]	ECB - Draft Recommendations for the security of mobile payments (draft document for public consultation)	ECB
[8]	ECSG 001-17 – SEPA Cards Standardisation Volume	ECSG
[9]	EMV Payment Tokenisation Specification	EMVCo
[10]	ISO/IEC 14443: Identification cards - Contactless integrated circuit cards - Proximity cards - Parts 1-4.	ISO

Table 1: Bibliography

1.3 Definitions

Throughout this document, the following terms are used.

Term	Definition
Acquirer	A PSP contracting with a payee to accept and process card-based payment transactions, which result in a transfer of funds to the payee.
Authentication	The provision of assurance that a claimed characteristic of an entity is correct. The provision of assurance may be given by verifying an identity of a natural or legal person, device or process.
Automated Teller Machine (ATM)	An unattended physical POI that has online capability, accepts PINs, which allows authorised users, typically using machine-readable plastic cards, to withdraw cash from their accounts and/or access other services (e.g., to make balance enquiries, transfer funds or deposit money).
Beneficiary	See Payee
Cardholder	A customer who has an agreement with an issuer for a mobile card payment service.
Card Not Present	A card transaction with no physical interaction between the card and a POI at the time of the transaction, also referred to as a remote card transaction.
Consumer	A natural person who, in payment service contracts covered by the PSD2, is acting for purposes other than his or her trade, business or profession [6].

Contactless Technology	A radio frequency technology operating at very short ranges so that the user has to perform a voluntary gesture in order that a communication is initiated between two devices by approaching them. It is a (chip) card or mobile payment acceptance technology at a POI device which is based on ISO/IEC 14443 (see [10]).
Customer	A payer or a beneficiary which may be either a consumer or a business (merchant).
Credential(s)	Payment account related data that may include a code (e.g., mobile code), provided by the PSP to their customer for identification/authentication purposes.
Credit transfer	A payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the PSP which holds the payer's payment account, based on an instruction given by the payer [6].
Digital wallet	A service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc.). A digital wallet is sometimes also referred to as an e-wallet.
Direct debit	A payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's PSP or to the payer's own PSP [6].
Dynamic authentication	An authentication method that uses cryptography or other techniques to create a one-per-transaction random authenticator (a so-called "dynamic authenticator").
EMVCo	An LLC formed in 1999 by Europay International, MasterCard International and Visa International to enhance the EMV Integrated Circuit Card Specifications for Payments Systems. It manages, maintains, and enhances the EMV specifications jointly owned by the payment systems. It currently consists of American Express, Discover, JCB, MasterCard, Union Pay and VISA.
Gigabit per second (Gbps)	A unit of data transfer rate equal to 1,000 megabits per second or 1,000,000,000 bits per second.
(Card) Issuer	A PSP contracting to provide a payer with a payment instrument to initiate and process the payer's card-based payment transactions. Note: This PSP can be a member of a card payment scheme.
In-app payment	These are payments made directly from within a mobile application (e.g., a merchant app). The payment process is completed from within the app to enhance the consumer experience.

Instant payment	Electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer (within seconds of payment initiation). This is irrespective of the underlying payment instrument used (credit transfer, direct debit or payment card) and of the underlying clearing and settlement arrangements that make this possible.
Merchant	The beneficiary within a mobile payment scheme for payment of the goods or services purchased by the consumer. The merchant is a customer of their PSP.
Mobile device	Personal device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth, etc. Examples of mobile devices include mobile phones, smart phones, tablets.
Mobile Network Operator (MNO)	A mobile phone operator that provides a range of mobile services, potentially including facilitation of NFC services. The MNO ensures connectivity Over the Air (OTA) between the consumer and their PSP using their own or leased network.
Mobile wallet	A digital wallet accessed through a mobile device. This service may reside on a mobile device owned by the customer (i.e. the holder of the wallet) or may be remotely hosted on a secured server (or a combination thereof) or on a merchant website. Typically, the so-called mobile wallet issuer provides the wallet functionalities but the usage of the mobile wallet is under the control of the customer.
Payee	A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction [6].
Payer	A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order [6]. Note: In case of card-based payments this may also be referred to as cardholder.
Payment account	An account held in the name of one or more payment service users which is used for the execution of payment transactions [6].
Payment scheme	A single set of rules, practices, standards and/or implementation guidelines for the execution of payment transactions and which is separated from any infrastructure or payment system that supports its operation, and includes any specific decision-making body, organisation or entity accountable for the functioning of the scheme.
Payment Service Provider (PSP)	A body referred to in Article 1(1) of [6] or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of [6].

Payment transaction	An act, initiated by the payer or on his behalf or by the payee (beneficiary), of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee (as defined in [6]).
Personal Identification Number (PIN)	A personal and confidential numerical code which the user of a payment instrument may need to use in order to verify their identity.
POI device	"Point of Interaction" device; the initial point where data is read from a customer device or where consumer data is entered in the merchant's environment. As an electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a customer to perform a payment transaction. The merchant controlled POI may be attended or unattended. Examples of POI devices are POS, vending machine, ATM.
Terabit per second (Tbps)	A unit of data transfer rate equal to 1,000 gigabits per second.
Third Party Payment Service Provider (TPP)	A third party that offers payment services which are different to the Account Servicing PSP (ASPSP) such as a Payment Initiation Service Provider (PISP), Account Information Service Provider (AISP) and Trusted Party Payment Instrument Issuer (TPPII) (see [6]).
(Payment) Tokenisation	The usage of payment tokens instead of real payer related account data in payment transactions
(Payment) Token	Payment Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for payer account related data (e.g., the PAN for card payments, the IBAN for SCTs). Payment Tokens must not have the same value as or conflict with the real payment account related data. Examples include the EMVCo Token, see [9].

Table 2: Definitions

1.4 Abbreviations

Throughout this document, the following abbreviations are used.

Abbreviation	Term
APT	Advanced Persistent Threat
ATA	Advanced Targeted Attacks
ATM	Automated Teller Machine
ATP	Advanced Threat Protection
BIC	Business Identifier Code
BYOA	Buy Your Own App(lication)
BYOD	Bring Your Own Device

CAP	Chip Authentication Program
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CISO	Chief Information Security Officer
CNP	Card Not Present
DoS	Denial of Service
DDoS	Distributed Denial of Service
DNS	Domain Name System
EBA	European Banking Authority
EC	European Commission
ECSG	European Cards Stakeholders Group
EPC	European Payments Council
Gbps	Gigabit per second
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS
IBAN	International Bank Account Number
IDS	Intrusion Defense System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Preventions System
ISO	International Organization for Standardization
IT	Information Technology
NFAT	Network Forensic Analysis Tool
NIS	Network Information Security
OTP	One-Time Password
PAN	Primary Account Number
PIN	Personal Identification Number
PLC	Programmable Logic Controllers
POI	Point of Interaction
POS	Point of Sale
PSD	Payment Services Directive
PSP	Payment Service Provider
RAT	Remote Access Trojan
RTS	Regulatory Technical Standard
SCT	SEPA Credit Transfer
SCT-Inst	Instant SCT
SDD	SEPA Direct Debit

SDK	Software Development Kit
SEPA	Single Euro Payments Area
SIEM	Security Information and Event Management
SIM	Subscriber Identification Module
SMS	Short Message Service
SQL	Structured Query Language
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAN	Transaction Authentication Number
Tbps	Terabit per second
TLS	Transport Layer Security
TPP	Third Party Payment Service Provider
UEBA	User and Entity Behaviour Analytics
URL	Uniform Resource Locator
USB	Universal Serial Bus

Table 3: Abbreviations

2 General

2.1 About the EPC

The European Payments Council (EPC), representing payment service providers (PSPs), supports and promotes European payments integration and development, notably the Single Euro Payments Area (SEPA). The EPC is committed to contribute to safe, reliable, efficient, convenient, economically balanced and sustainable payments, which meet the needs of payment service users and support the goals of competitiveness and innovation in an integrated European economy. It pursues this purpose through the development and management of pan-European payment schemes and the formulation of positions and proposals on European payment issues in constant dialogue with other stakeholders and regulators at the European level and taking a strategic and holistic perspective. The primary task of the EPC is to manage the SEPA Credit Transfer, Instant SEPA Credit Transfer and SEPA Direct Debit Schemes in close dialogue with all stakeholders. The EPC is an international not-for-profit association which makes all of its deliverables available to download free of charge on the EPC Website. Further information may be obtained from www.epc-cep.eu.

2.2 Vision

The vision of the EPC is to contribute to the evolution of an integrated market for payments. Payment transactions enabled by different devices and channels are built on existing SEPA Scheme Rulebooks and on SEPA Cards. Therefore, the EPC assists in specifying standards and guidelines to create the necessary environment so that PSPs can deliver secure, efficient and user-friendly solutions to access the SEPA payment instruments. The EPC aims to enhance the security awareness amongst the various stakeholders in the payment ecosystem through the production of this yearly payments threats and fraud trends report.

2.3 Scope and objectives

The present document aims to provide an insight in the latest developments during the last years on threats affecting payments, including cybercrime. It further provides an insight into the payments fraud, resulting from criminal attacks. However, it does not endeavour to be a complete report on all criminal activities. It only attempts to create awareness on these matters in order to allow stakeholders involved with payments to decide on possible actions in this respect in order to maintain the trust in their payment solutions.

2.4 Audience

The document is intended for PSPs as well as for other interested parties involved in payments, such as:

- Third Party Payment Service Providers (TPPs)
- Equipment manufacturers (POIs, consumer devices, etc.);
- Merchants and merchant organisations;
- Consumers;
- Application developers;
- Public administrations;
- Regulators;

- Standardisation and industry bodies;
- Payment schemes;

and

- Other interested stakeholders.

3 Main threats today

3.1 Social Engineering

3.1.1 Definition

Social engineering is a primarily non-technical method of intrusion used by attackers to target users to provide access and information rather than the attacker directly attacking the system. Through a variety of techniques it manipulates people into carrying out actions which may result in the theft of information, compromise of credentials or system compromise.

Social engineering attempts that can impact payments can take place across many channels, including email, SMS, calls and social media channels. Any communication channel used to communicate with customers and users can be exploited by an attacker, with varying degrees of sophistication required to carry out the attack.

Social engineering attacks range from mass email attempts that can be relatively easy to identify as an attempt to defraud a customer, through to attacks that target one or two individuals in an organisation and impersonate senior employees within that organisation, an attack known as CEO Fraud or Business Email Compromise (BEC).

The ultimate goal of the social engineering attempt varies; it may be to gain access to a system via tricking the user into revealing their credentials, carrying out an action that compromises a system, perhaps by installing malware, or even manipulating the user to make a payment to an account under the attackers control.

3.1.2 Fraud Description

Social engineering is the art of manipulating people so they give up confidential information or their card / security device. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick them into giving their credentials or other sensitive information, or to access their device to secretly install malicious software. This software aims to give the attackers access to passwords and bank information as well as getting control over customer devices. Criminals use social engineering tactics because it is usually easier to exploit an individual's natural inclination to trust than it is to discover ways to hack software.

As mentioned above, one of the most important targets are the commonly used customer authentication methods in on-line banking sessions and for remote payments which are based on passcodes, chip-card based OTP methods (e.g., EMV-CAP) or paper based TAN-methods (e.g., the indexed paper-based iTAN) or mobileTAN (an SMS TAN linked to a specific transaction).

Common social engineering attacks include the following:

- *Email from a friend.* If a criminal manages to hack or socially engineer one person's email password they have access to that person's contact list–and because most people use one password everywhere, they probably have access to that person's social networking contacts as well. Once the criminal has that email account under their control, they send emails to all the person's contacts or leave messages on all their friends' social pages, and possibly on the pages of the person's friends' friends. These messages typically contain a link the persons trust and click causing an infection of their device with malware so the criminal can take over their machine and collect information or contain a download–pictures, music, movie, document, etc., that has malicious software embedded. In addition, these messages may create a compelling story or pretext: e.g., urgently ask for help or ask to donate to their charitable fundraiser, or some other cause. They may also be more targeted and concentrated and take over an active dialogue with the PSP.

- A special case of “Email from a friend” is *CEO fraud* where an attacker sends an email that appears to come from the CEO, or some other powerful executive in the organisation, using social engineering to coerce employees to transfer money to a given beneficiary. The attackers spoof the email of the CEO, CFO or other high-level executive by either compromising their real email account or creating an account that looks almost identical to the real one. The use of the CEO's name is key to these attacks, it lends an air of authenticity and authority to the scams. Employees tend to take requests from the CEO seriously[2].
- *Recovery agent fraud.* Happens when former fraud victims are told the money they have previously lost can be recovered. Targeting former fraud victims, the fraudster poses as a legitimate organisation, claiming they can apprehend the fraudster and recover any monies lost - for a fee. Criminals use social engineering tactics either by phone or email, posing as a lawyer, a law enforcement officer or an official working for a government agency in another country. If the fraud victim responds to their offer of help, they will ask him or her for various fees, such as release and administration fees. If fraud victims pay these fees, they will keep coming back with another fee that has to be paid, before the money can be returned[3].
- *Phishing attempts.* Typically, a phisher sends an email, instant message, comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution. These messages usually have a scenario or story:
    - The message may explain there is a problem that requires the receiver to “verify” information by clicking on the displayed link (which may look very legitimate) and providing information in their form. An example of SMS phishing may notify “Your online banking account is locked. You need to unlock it at the link provided”, once you click on the link, it will lead you to a fake bank website that asks you to enter your personal information. The fake site looks identical to the bank’s real homepage. However, when you attempt to log in to your account, the site asks for information that the real site never would. It may ask, for example, your account number, password or card PIN. These types of phishing scams often include a warning of what will happen if you fail to act soon, because criminals know that if they can get the individual to act before they think, they more likely will fall for their phish.
    - The message may notify that you’re a “winner”. Maybe the email claims to be from a lottery, or a dead relative, or the millionth person to click on their site, tax refund, etc. In order to give you your “winnings” you have to provide personal or bank information. These are the ’greed phishes’, leading to emptied bank account or identity theft.

[2] https://www.trustwave.com/Resources/SpiderLabs-Blog/CEO-Fraud-Scams-and-How-to-Deal-With-Them-at-the-Email-Gateway/

[3] http://www.actionfraud.police.uk/protect-yourself/fraud-recovery-fraud

- o The message may ask for help…. Preying on kindness and generosity, these phishes ask for aid or support for whatever disaster, political campaign, or charity is hot at that moment.
- o Response to a question the receiver never had. Criminals may pretend to be responding to a “request for help” from a company while also offering more help. They pick companies that millions of people use like a software company or PSP. If the individual does not use the product or service, they will ignore the email, phone call, or message, but if they do happen to use the service, there is a good chance they will respond because they probably do want help with a problem.
- o The message may offer a “more secure” or “functionality enhanced” card, requesting the customer to send their outdated card to a certain physical address and requesting in addition that the customer also sends their PIN to a given email address.

Whilst mass mailing social engineering attempts continue, recent years have seen a dramatic increase in more targeted attempts, known as spear phishing. By obtaining personal information on the targets, perhaps through social media etc. it enables the attacker to produce an attempt that is significantly harder to identify as fraudulent.

Attackers can also use people’s desire to access their smart phones, particularly whilst travelling by creating fake access points in high-traffic public locations such as coffee shops, libraries and airports. Once the access point has been created, the attacker chooses a name to encourage users to connect i.e. “Free Airport Wi-Fi”. Once a user has connected to this access point the attacker will then be able to monitor all network traffic and potentially further compromise the device. A variant on this attack is for the attacker to use the name of established free Wi-Fi providers in the hope that the settings of users devices will allow automatic connection to known access points.

Typical examples of social engineering attacks related to financial transactions include the following:

- Attacks using malware to try to persuade the customer to carry out a “security update” or type in a number of TANs because of an alleged “security incident”.
- So-called “reverse Trojan horse” attacks working as follows: the customer’s device is infected with a Trojan horse which falsifies the customer’s online bank statement so that it appears as if a large sum of money has been transferred by e.g., the tax authorities to the customer’s account. The customer then receives an email, allegedly from the local tax office, asking him or her to return the amount credited “in error”, while the customer is in fact “reimbursing” the money to a fake account.
- Vishing (the word is a combination of "voice" and phishing) - exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations known to the telephone company, and associated with a bill-payer. Typically, the phishing link sends the victim to a fake helpdesk that attempts to scam the user into surrendering private information that will be used for identity theft.
- The angler phishing attack involves hackers creating fake Twitter accounts, posing as customer support staff, to trick customers into handing over their personal details. The scam entails hackers monitoring bank customers’

interactions with their banks on Twitter. They then hijack conversations users attempt to have with genuine support staff of banks, and redirect the customers to a fake support page.

- Fake apps[4] that cause malicious activities such as the installation of a fake user interface that is laid over the genuine banking app when it is opened by the customer. As soon as the customer's bank details are entered they are collected by the criminal (see also section 3.4.1.1).

3.1.3 Impact & Context

Social engineering techniques have greatly increased over the last two years as attackers increasingly target users rather than technology. All types of social engineering attacks continue to be used by attackers of varying levels of capabilities, with particular increase in Business Email Compromise emails and phishing emails that result in malware being deployed on computers.

Phishing plays a key role in carrying out targeted digital attacks. Some users are not able to recognise phishing emails. However, the implementation of DMARC by organisations (see section 3.1.4) to stop phishing emails have experienced a quite big take-up in some countries and have proven to be successful[5]. Nevertheless, phishing continues to be a low-threshold and effective method for attackers.

Phishing is also sometimes used in combination with distribution of specific malware called ransomware. This is a type of malware designed to encrypt data and block access to a computer system until a sum of money is paid.

Social engineering and phishing attack trends in 2018:

- According to a release by the FBI in July 2018[6]:
  - Business Email Compromise attacks continue to grow and evolve, targeting small, medium, and large business and personal transactions. Between December 2016 and May 2018, there was a 136% increase in identified global exposed losses.
  - The scam has been reported in 160 countries, with monies transferred to 115 countries.
  - Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in the United Kingdom, Mexico and Turkey have also been identified recently as prominent destinations.

[4] see for example:
https://blog.avast.com/mobile-banking-trojan-sneaks-into-google-play-targeting-wells-fargo-chase-and-citibank-customers
https://www.hackread.com/catelites-android-malware-poses-as-2200-bank-apps/

[5] https://hmrcdigital.blog.gov.uk/2016/11/25/combatting-phishing-a-very-big-milestone/
http://www.itproportal.com/news/hmrc-blocked-500000-phishing-emails-in-2015/

[6] https://www.ic3.gov/media/2018/180712.aspx

    - According to the FBI, more than 78,000 complaints have been made globally between October 2013 and May 2018. Targeted individuals and businesses lost or could have lost $12.5 billion.

- According to the Proofpoint Human Factor Report 2018[7]:
    - "About 55% of social media attacks impersonated customer support accounts, this trend, known as 'angler phishing', predominantly targeted customers of financial services companies. Phishing attacks increasingly hijacked victims computers to mine for cryptocurrency.
    - Dropbox phishing was the top lure for phishing attacks. Twice as many phishing messages used the file sharing service than the next most popular lure."

- According to Financial Threats Review 2018: An ISTR Special Report (Symantec)[8]:
    - "Spear phishing is the number one infection vector employed by 71 percent of organised groups in 2017."

- Kaspersky Lab identified the following trends in the first quarter of 2018[9]:
    - "Facebook users are one of the juiciest targets for cyber fraudsters looking to launch mass phishing attacks. Last year Facebook was one of the Top 3 most exploited company names. The schemes are numerous, but fairly standard: the user is asked to "verify" an account or lured into signing into a phishing site on the promise of interesting content.
    - Cybercriminals are exploiting the interest in cryptocurrencies and Initial Coin Offerings (ICO), potential investors are targeted and sent fraudulent messages prior to official ICO starts about the start of pre-sales with a list of crypto-wallets to which money should be transferred.
    - A large amount of spam messages related to GDPR.
    - The country with the largest percentage of users affected by phishing attacks in Q1 2018 was Brazil (19.07%)."

3.1.4 Suggested Controls and Mitigation

A continuous exchange of intelligence information about attacks and countermeasures among the IT experts of PSPs is considered to be an important defence against these types of attacks.

In addition, PSPs need to put the appropriate transaction filtering and monitoring systems in place and use customer profiling to detect suspicious payment transactions.

However, a very important aspect to counter the social engineering attacks is continued awareness raising campaigns. PSPs need to have a proper customer education system in place, not only addressing individual clients but also including SMEs and large corporates, explaining the risks in layman words. In some countries coordinated campaigns are being set up where the financial industry cooperates with public or semi-

[7] https://www.proofpoint.com/sites/default/files/pfpt-uk-tr-the-human-factor-2018.pdf

[8] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[9] https://securelist.com/spam-and-phishing-in-q1-2018/85650/

public agencies. In addition, it is as important for companies and organisations (including PSPs) to also adequately educate and create awareness amongst their own staff (e.g., related to CEO fraud).

Information published by security companies is an important source. Such companies regularly offer trainings and provide dedicated educational material. It is necessary to combine human with criminal intelligence and complement those with specific know-how about the on-line banking systems and business processes.

Among the technical measures that can mitigate phishing, the following may be considered as best practices[10]. Sender Policy Framework (SPF), which is an email-validation system designed to detect email spoofing. It is the first step in securing the mail channel. The next protection is to use DomainKeys Identified Mail (DKIM)[11], which is an email authentication method designed to detect email spoofing by providing receiving mail exchangers to check that the incoming mail from a domain is authorised to be sent by that domain's administrators. And then the final step to be implemented is Domain-based Message Authentication, Reporting and Conformance (DMARC)[12] which is an email-validation system designed to detect and prevent email spoofing. DMARC is built on top of the existing mechanisms mentioned before, SPF and DKIM and enables the blocking of spoofed mails.

There are even companies offering takedown of phishing websites as a service. Specialist companies might be able to limit access to and finally stop phishing sites. In addition it might also be possible sometimes to collect stolen data from phishing servers. The victim’s PSP might then be able to reduce the consequences by contacting the customer and blocking the card or account.

Recently also country-based initiatives are starting to set up closed sharing platforms between PSPs related to CEO/President fraud including fields such as the sender IP, sender domain and fraudulent beneficiary account (IBAN/BIC).

3.1.5 Final Considerations/Conclusions

Authentication methods are only a small part of the whole security chain within payment systems and PSPs are able to early recognise many attacks through monitoring systems. However, social engineering is an important attack factor which is increasing while targeting not only individual customers but also CEOs / Presidents of large companies. It is often used in combination with other types of attacks and is already migrating to the mobile world. Therefore appropriate education remains a crucial factor to combat phishing and social engineering attacks.

3.2 Malware

Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software. Cybercriminals design malware to compromise computer functions, steal data, bypass access controls, and otherwise cause harm to the host computer, its applications or data.

[10] see for instance: https://www.ncsc.gov.uk/blog-post/making-email-mean-something-again

[11] see for instance: https://www.gov.uk/government/publications/email-security-standards/domainkeys-identified-mail-dkim

[12] see for instance: https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc

3.2.1 Definition

One of the major threats against cyber security today is malicious software, often referred to as malware. Malware comes in a wide range of flavours, such as virus, worms, remote access tools, rootkits, Trojans, spyware and adware. The latest addition to the malware family is ransomware, also known as cryptoware. Malware exploits software vulnerabilities in browsers, third party software and operating systems to gain access to the device and its information and resources. To spread, malware uses also social engineering techniques to trick users into installing and running the malicious code.

Trojan horse

It is maybe the largest category of the malware family. It consists of a large variety of exotic names. However they all have one thing in common; they bypass the security measure on the system to infect it. Their main purpose is, stealing valuable information from the system and gaining control of the system itself.

Spyware, Adware & Banking Trojans

Spyware and adware, which are categorised as malware, are less dangerous for the users. Spyware is often classified into the following categories, *browser hijackers, tracking cookies* and *system monitors*, in some cases *adware* is seen as the fourth category of spyware. These types of malware are all trying to track and store the usage and behaviour of the users, serving them with pop-ups ads when connected to the Internet. Based on the same approach, attackers are installing malware (Banking Trojan) targeting the victim while using e-banking services. Banking Trojans are capable of hijacking the browser and tampering financial transactions or stealing user credentials during the use of E-banking services.

Ransomware

Is a type of malicious software designed to encrypt files on the device or deny access to the device, which is the reason for it to be known as cryptoware. It holds data up for ransom, blackmailing the user to pay a ransom to get back their data or access to their device. A surprising fact is that this kind of attacks seems to be more profitable to the attackers than the traditional banking Trojans.

While traditional malware such as banking Trojans, spyware, and keyloggers requires the cybercriminal to oversee multiple steps before revenue is delivered to their bank account, ransomware makes it a seamless, automated process. Script kiddies (hackers with little or no coding skills) can even buy turnkey ransomware kits known as "Ransomware as a Service" (RaaS) that take all the hassle out of digital thievery.

Advanced Persistent Threats

Another important category of malicious software is the one that is being abstractly described as Advance Persistent Threat. The reader is referred to section 3.3 for more information.

Remote Access Trojans (RATs)

A Remote Access Trojan is a piece of malware that allows a remote actor to control a system as if they have physical access to it. Use of a RAT may provide cybercriminals with unlimited access to the victims' computers. Using the victim's access privileges, the RAT can perform critical functions or steal sensitive data. RAT technology is also commonly used by Advanced Persistent Threats (see section 3.3) to bypass strong authentication and get access to important data.

3.2.2 Fraud Description

Malware is spread in two main ways, namely by sending the virus via simple email to the victim's device who activates it by clicking or by luring the victim to specific webpages where malicious code will search for vulnerabilities on the victim's device, or even executing vulnerable software such as out-of-date Microsoft Office, Acrobat Reader, etc.

The first method even though the oldest and the less elegant one, is still very efficient. The normal way to spread the virus is to send it to a large number of victims at the same time, a so-called widespread attack. The attacker hopes to hit something without knowing much about their victims. The other way is to cleverly target the victim, this is often achieved by spinning a story about why the victim should expect this specific attachment or link to a malicious website and why it is important to open it. This is a targeted attack, often called spear phishing.

The second method is more advanced and can, if perfectly executed, affect many thousands of victims within a short timeframe. This method consists of first adding malicious code to a webpage, then luring the victim to that page. This malicious code can be spread via an exploit kit, which is a piece of software designed for finding and utilising vulnerabilities which are available on the device. These kits ensure a smooth infection of customer devices. Some of the most well-known exploit kits are "Angler", "Neutrino" and "Rig". When the page is visited, the code will automatically search for known vulnerabilities and infect the victim's device, often with no sign for the victims themselves. This is sometimes referred to as "malvertising" - the malware is hidden inside ads on popular web-pages. As payments operation through mobile applications grows in popularity, also increase malware generation for mobile devices.

Another way to spread malware takes advantage from people vulnerabilities. Social engineering is used to manipulate people to infect individuals or a whole company. Due to its increasing role in many attacks, a specific section is dedicated to this topic (see section 3.1).

Finally, ATM malware threats are still affecting and evolve. More details are provided in section 4.2.

3.2.3 Impact & Context

Whether the infection is targeting a private user, a SME or a multinational company the effects of a successful malware attack can cause significant damage, and every prevention and mitigating method should be utilised. As an example, in May 2017 the WannaCry[13] ransomware malware strain gained infamy by crippling entire networks, across more than 150 countries, with hundreds of thousands of Windows computers infected.

[13] https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

In the case of PSPs, all necessary steps to prevent ransomware attacks should be taken. Ransomware attacks could affect encrypting or selling payment information, PANs and other information necessary for PSP business execution.

Ransomware has typically no impact on the users banking credentials, however the case of banking Trojans have managed to extort a significant amount of money from users.

According to the Proofpoint Q1 2018 Threat Report[14]: The first months of 2018 were marked by increasing diversity in the threat landscape even as ransomware stopped appearing in the massive campaigns that characterised much of 2016 and 2017. Without the disproportionately large ransomware campaigns of the last two years, banking Trojans, information stealers, downloaders, remote access Trojans (RATS), and more filled the void in the email space. Social engineering was pervasive, with email fraud attacks continuing to grow and evolve while the vast majority of web-based threats included social engineering techniques as well. For the first time since Q2 2016:

- Banking Trojans displaced ransomware as the top malware in email, accounting for almost 59% of all malicious email payloads in Q1.
- Emotet was the most widely distributed banking Trojan, accounting for 57% of all bankers and 33% of all malicious payloads.
- The bulk of the remaining malicious payloads included credential stealers and downloaders, comprising 19% and 18% of malicious email, respectively.

For the private users spyware and adware are a large threat towards their privacy, as this type of malware looks for patterns of the users and tries to profile their individual behaviour for monetisation purposes. Similar things might happen for companies, but normally this type of malware targets individual behaviour, in fact that is their goal to group the individual by their own definitions, it is therefore not a direct threat towards corporate users. The general advice would however be to utilise specialised software to remove and protect against adware, as they also could use resources on the computer.

Virus normally search the infected machine for all information that can be monetised; for private users this is typically credentials related to e-banking (mobile and web), credit card credentials are of similar high value. For private users the amount of information that can be sold to other parties is relatively small. Such information is easier to find in companies as each company retains databases of customers information or intellectual property, information which can be used to blackmail or to give an advance in a competitive market. The above case has a significant impact in larger organisations or even governmental organisations where information is one of the most valuable assets.

3.2.4 Suggested Controls and Mitigation

To prevent malware attacks, users should first minimise the number of installed programs on their device (and from trusted resources only), as the number of vulnerabilities will decrease accordingly. Secondly, one of the best ways to ensure that the system or device does not become infected with malware is to regularly update the installed software and to remove software that does no longer have any use. PSPs should use every opportunity to inform their customers that it is very important to keep their software updated, and hence reduce the risk for malware infection significantly. Even companies sometimes struggle with that topic but this can be mitigated by installing automatic patching software.

[14] https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

Script blockers are another viable mitigation of malware, by installing such blocking software, the device becomes less exposed to the risk, and therefore the risks of infections are smaller.

All critical files should be regularly backed up so that they can be recovered in the case of unauthorised alteration, encryption or destruction.

Also the monitoring of files/software (executables) behaviour is an additional mitigating measure that can help to block certain threats such as ransomware. This is generally referred to as “malware behaviour blocking”[15].

Another mitigation is the limited use of administrative rights; this is mostly applied by companies and security aware users, as most users would not see the benefit of it in their everyday needs. However, it is clear that this is still one of the most efficient ways to mitigate the risk of being infected.

Firewall and antivirus on consumer devices might not be as efficient as they used to be. The threats are still increasing and it is impossible to cover with these tools every vulnerability aspect from supplied software. They are however still able to mitigate a large part of the attacks, and at least the most common ones. They should be regularly updated otherwise they are not able to fully operate. It is also strongly recommended to enable further controls provided by the endpoint security mechanisms, such as the IPS/IDS capability on the device[16], when applicable.

Another advice is to ensure that macros cannot run on the systems while opening attachments or documents in general. This is typically the case for most large companies, however smaller companies and private users largely depend on the patches that are automatically installed by the office suite software provider as they do not understand the threat. Allowing the execution of only signed macros can be the solution to securely execute malware without losing functionality or breaking business needs.

Against the widespread attack, awareness is a great asset to prevent infection. If the victim knows about the dangers of opening attachments (sent by unknown or untrusted parties), and knows about the deceptions he can suffer through Social Engineering most of these attacks could be stopped before they happen.

Last but not least, investing in Advanced Threat Protection technologies, which are based on sandboxed analysis of the web traffic and the emails content, is a must for combating 0-day and more sophisticated malware attacks. These technologies use virtual machines in order to safely open or execute the transferred data in order to identify potential malicious indicators. It has been proven that the traditional signature-based techniques of security technologies are becoming obsolete. Advanced Threat Protection solutions combined with Threat Intelligence and Analytics services can provide an early alert for suspicious indications, preventing the exploitation of an attack.

[15] http://docs.trendmicro.com/all/ent/officescan/v10.5/en-us/osce_10.5_aegis.pdf

[16] Intrusion Prevention Systems / Intrusion Defense Systems are security mechanisms deployed on servers or devices which monitor in real-time for entries representing a security violation. Some common abilities of such mechanisms include integrity checking, policy enforcement, rootkit detection, detection of variations in system configuration. They offer the ability to identify intrusion attempts and actively prevent malicious or anomaly activity on the host system. IPS/IDS could be deployed at the network level too.

3.2.5 Final Considerations/Conclusions

Malware is a major threat against cyber security for all of us. The problem is increasing in some countries while decreasing in others. However, simple best practices and security rules will help mitigate most of the malware attacks. The problem is to make the ordinary customer understand why these advices are crucial and why they should be followed. Therefore PSPs should keep investing in customer awareness campaigns. On the other hand, PSPs should continue to invest in new security technologies, such as the Advanced Threat Protection ones, for combating state-of-the-art and 0-day malware attacks, including ransomware.

3.3 Advanced Persistent Threats (APTs)

3.3.1 Definition

An Advanced Persistent Threat (APT) is a sophisticated, targeted malicious attack aimed to a specific individual, company, system or software, based on some specific knowledge regarding the target. It pursues its objectives repeatedly over an extended period of time, adapts to defenders' efforts to resist and is determined to maintain the level of interaction needed to execute its objectives[17].

APTs, according to Symantec's detailed report on the subject[18], are different from other targeted attacks in the following ways:

Customised attacks - In addition to more common attack methods, APTs often use highly customised tools and intrusion techniques, developed specifically for the campaign. These tools include zero-day vulnerability exploits, viruses, worms, and rootkits. In addition, APTs often launch multiple threats or "kill chains" simultaneously to breach their targets and ensure ongoing access to targeted systems, sometimes including a "sacrificial" threat to trick the target into thinking the attack has been successfully repelled.

***Low and slow* -** APT attacks occur over long periods of time during which the attackers move slowly and quietly to avoid detection. In contrast to the "smash and grab" tactics of many targeted attacks launched by more typical cybercriminals, the goal of the APT is to stay undetected by moving "low and slow" with continuous monitoring and interaction until the attackers achieve their defined objectives.

Higher aspirations - Unlike the fast-money schemes typical of more common targeted attacks, APTs are designed to satisfy the requirements of international espionage and/or sabotage, usually involving covert state actors. The objective of an APT may include military, political, or economic intelligence gathering, confidential data or trade secret threat, disruption of operations, or even destruction of equipment. The groups behind APTs are well funded and staffed; they may operate with the support of

[17] National Institute of Standards and Technology (NIST), Special Publication 800-39, Managing Information Security Risk, Organization, Mission, and Information System View, USA, 2011

[18] *Symantec, Advanced Persistent Threats:A Symantec Perspective* https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf Part of this report is presented verbatim below.

military or state intelligence.

Specific targets - While nearly any large organisation possessing intellectual property or valuable customer information is susceptible to targeted attacks, APTs are aimed at a much smaller range of targets. Widely reported APT attacks have been launched at government agencies and facilities, defence contractors, and manufacturers of products that are highly competitive on global markets. In addition, APTs may attack vendor or partner organisations that do business with their primary targets. But government-related organisations and manufacturers are not the only targets. Ordinary companies with valuable technology or intellectual property are now being targeted by nation-states. With the globalisation of world economies, national security and economic security have converged. Moreover, organisations that maintain and operate vital national infrastructure are also likely targets.

3.3.2 Fraud description

APTs can often be seen as an outstanding category of malware. Attackers demonstrate a continuously improving set of skills, in bypassing security mechanisms, providing often a state-of-the-art attack that changes the roadmap and trends of the security industry. This is also known as zero-day attacks, since no normal signatures exist from the antivirus / antimalware tools.

How do APT attacks work?

Phase 1: Incursion

In targeted attacks, hackers typically break into the organisation's network using social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods. These methods are also used in APTs, often in concert. The main difference is that while common targeted attacks use short-term, “smash and grab” methods, APT incursions are designed to establish a beachhead from which to launch covert operations over an extended period of time. Other characteristics of APT incursions include the following:

- **Reconnaissance** - APT attacks often employ large numbers of researchers who may spend months studying their targets and making themselves familiar with target systems, processes, and people, including partners and vendors. Information may be gathered both online and using conventional surveillance methods. In the case of the Stuxnet attack on organisations believed to be operating Iranian nuclear facilities, the attack team possessed expertise in the design of the programmable logic controllers (PLCs) used for uranium enrichment that were targeted in the attack.
- **Social engineering** - Incursion is often accomplished through the use of social engineering techniques, such as inducing unsuspecting employees to click on links or open attachments that appear to come from trusted partners or colleagues. Unlike the typical phishing attack, such techniques are often fed by in depth research on the target organisation. In one case, a small number of human resource employees were targeted using an apparently innocuous attachment, a spreadsheet on hiring needs that appeared to come from a job listing website. In the case of Hydraq, targeted users were led to a picture-hosting website where they were infected via a drive-by download.

- **Zero-day vulnerabilities** - Zero-day vulnerabilities are security loopholes that are unknown to the software developer and may therefore be exploited by attackers before the developer can provide a patch or fix. As a result, the target organisation has zero days to prepare; it is caught off-guard. Since it takes significant time and effort to discover zero-day vulnerabilities, only the most sophisticated attacker organisations are likely to take advantage of them. APTs often use one zero-day vulnerability to breach the target, switch to a second and then a third as each point of attack is eventually fixed. This was the case with Hydraq. The Stuxnet attack was exceptional in that four separate zero-day vulnerabilities were exploited simultaneously.
- **Manual operations** - Common or massive attacks employ automation to maximise their reach. “Spray and pray” phishing scams use automated spam to hit thousands of users in hopes that a certain percentage will click on a link or attachment and trigger the incursion. On the other hand, while APTs may deploy spam, more often they target distinct individual systems and the incursion process is tightly focused—not the automated process used in non-APT attacks.

Phase 2: Discovery

Once inside, the attacker maps out the organisation's systems and automatically scans for confidential data or, in the case of some APTs, operational instructions and functionality. Discovery may include unprotected data and networks as well as software and hardware vulnerabilities, exposed credentials, and pathways to additional resources or access points. Here again, where most targeted attacks are opportunistic, APT attacks are more methodical and go to extraordinary lengths to avoid detection.

- **Multiple vectors** - As with incursion, APTs tend to use multiple discovery techniques in combination. Once malware is present on host systems, additional tools can be downloaded as needed for the purpose of exploring software, hardware, and network vulnerabilities.
- **Run silent, run deep** - Since the goal of the APT is to remain inside the organisation and harvest information over the long-term, discovery processes are designed to avoid detection at all cost. Hydraq (also known as the Aurora or Google attacks) used a number of obfuscation techniques to keep itself hidden inside victim organisations. Specifically, it used spaghetti code, a technique used to make analysis and detection of the malware more difficult.
- **Research and analysis** - Discovery efforts are accompanied by research and analysis on found systems and data, including network topology, user IDs, passwords, and so on.

Phase 3: Capture

In the capture phase, exposed data stored on unprotected systems is immediately accessed. In addition, rootkits may be surreptitiously installed on targeted systems and network access points to capture data and instructions as they flow through the organisation. In the case of Duqu, which seems to be the precursor to a future, Stuxnet-like attack, its sole purpose was to gather intelligence, which could be used to give attackers the insight they need to mount future attacks. While Duqu was not widespread, it is highly targeted, and its targets include suppliers to industrial facilities.

- **Long-term occupancy** - The APT is designed to capture information over an extended period. For example, a large-scale cyber spying operation called GhostNet, discovered in March 2009, was able to infiltrate computer systems in 103 countries, including embassies, foreign ministries, and other government offices, and the Dalai Lama's Tibetan exile centers in India, London, and New York City. According to a report by the Information Warfare Monitor, GhostNet began capturing data on May 22, 2007, and continued at least through March 12, 2009. On average, the amount of time that a host was actively infected by an APT was 145 days, with the longest infection span being 660 days.

- **Control** - In some cases, APTs entail the remote ignition or shutdown of automated software and hardware systems. As more and more physical devices are controlled by embedded microprocessors, the potential for mayhem is high. In fact, Stuxnet went well beyond stealing information. Its purpose was to reprogram industrial control systems—computer programs used to manage industrial environments such as power plants, oil refineries, and gas pipelines. Specifically, its goal was to manipulate the physical equipment attached to specific industrial control systems so the equipment acted in a manner programmed by the attacker, contrary to its intended purpose. Command-and-control servers may covertly seize control of target systems and even destroy them depending on the APT game plan.

Phase 4: Exfiltration

Once the intruders have seized control of target systems, they may proceed with the theft of intellectual property or other confidential data.

- **Data transmission** - Following command-and-control signals, harvested data may be sent back to the attack team home base either in the clear (by Web mail, for example) or wrapped in encrypted packets or zipped files with password protection. Hydraq used a number of novel techniques for sending the stolen information back to home base. One of these was the use of Port 443 as a primary channel for upload of stolen data. It also established connections that resembled an SSL key exchange dialogue, but did not result in a fully negotiated SSL channel. Lastly, it used private ciphers to encrypt content as it left the victim organisations.
- **Ongoing analysis** - Whereas stolen credit card numbers from a targeted attack are quickly packaged for sale, information captured by APTs is often studied at length for clues to strategic opportunities. Such data may be subject to manual analysis by field experts to extract trade secrets, anticipate competitive moves, and plan counter manoeuvers.

Recognising an APT[19]

Because APT hackers use different techniques from ordinary hackers, they leave behind different signs. Over the past two decades, Roger Grimes discovered the following five signs most likely to indicate that a company has been compromised by an APT. Each could be part of legitimate actions within the business, but their unexpected nature or the volume of activity may bear witness to an APT exploit.

[19] https://www.csoonline.com/article/2615666/security/security-5-signs-you-ve-been-hit-with-an-advanced-persistent-threat.html Parts of this article are presented verbatim below.

- **Increase in elevated log-ons late at night -** APTs rapidly escalate from compromising a single computer to taking over multiple computers or the whole environment in just a few hours. They do this by reading an authentication database, stealing credentials, and reusing them. They learn which user (or service) accounts have elevated privileges and permissions, then go through those accounts to compromise assets within the environment. Often, a high volume of elevated log-ons occur at night because the attackers live on the other side of the world.

- **Widespread backdoor Trojans -** APT hackers often install backdoor Trojan programs on compromised computers within the exploited environment. They do this to ensure they can always get back in, even if the captured log-on credentials are changed when the victim suspects an attack.

- **Unexpected information flows** - Inspection for large, unexpected flows of data from internal origination points to other internal computers or to external computers should be done. It could be server to server, server to client, or network to network.

  Those data flows might also be limited, but targeted -- such as someone picking up email from a foreign country. Every email client should have the ability to show where the latest user logged in to pick up email and where the last message was accessed. Some email systems already offer this.

  This has become harder to perform because so much of today's information flows are protected by VPNs, usually including TLS over HTTP (HTTPS). Although this used to be rare, many companies now block or intercept all previously undefined and unapproved HTTPS traffic using a security inspection device chokepoint. The device "unwraps" the HTTPS traffic by substituting its own TLS digital and acts as a proxy pretending to be the other side of the communication's transaction to both the source and destination target. It unwraps and inspects the traffic, and then re-encrypts the data before sending it onto the original communicating targets. If something similar does not happen, the ex-filtrated data leak will be missed.

  Of course, to detect a possible APT, one should be able to understand what the legitimate data flows look like before the environment is compromised.

- **Unexpected data bundles** - APTs often aggregate stolen data to internal collection points before moving it outside. Look for large (gigabytes, not megabytes) chunks of data appearing in places where that data should not be, especially if compressed in archive formats not normally used by your company.

- **Focused spear-phishing campaigns** - One of the best indicators of an APT attack would be focused spear-phishing email campaigns against a company's employees using document files (e.g., Adobe Acrobat PDF files, Microsoft Office Word, Microsoft Office Excel files, or Microsoft Office PowerPoint files) containing executable code or malicious URL links. This is the original causative agent in the vast majority of APT attacks.

> The most important sign is that the attacker's phish email is not sent to everyone in the company, but instead to a more selective target of high-value individuals (e.g., CEO, CFO, CISO, project leaders, or technology leaders) within the company, often using information that could only have been learned by intruders that had already previously compromised other team members.
>
> The emails might be fake, but they contain keywords referring to real internal, currently ongoing projects and subjects. Instead of some generic phishing subject, they contain something very relevant to an ongoing project and come from another team member on the project.

APT attacks may target financial institutions with the aim to compromise the network or payment system e.g., to perform unauthorised transactions and steal money. Some examples of APT attacks are provided in the next section.

3.3.3 Impact & context

The APT is advanced and stealthy, often possessing the ability to conceal itself within the enterprise network traffic, interacting just enough to get what it needs to accomplish its job. This ability to disguise itself and morph when needed can be crippling to security professionals' attempts to identify or stop an APT attack. The APT's single-minded persistence on pursuing its target and repeated efforts to complete the job for which it has been created with malicious intent, makes that the attack will not go away after one failed attempt. It will continually attempt to penetrate the desired target until it meets its objective.

In recent years not only criminal but also state organised APT attacks have been seen around the globe, all targeting financial institutions. Criminal organisations seem to originate from Russia but targeting also financial institutions in other regions around the Globe. Although parties like Europol[20] and Interpol have done proper jobs with arresting gang members, criminal organisations such as Cobalt[21] and Moneytaker have been very active in 2018 attacking financial institutions. The modus operandi of these gangs varies by doing field research on the financial institutions to spear phishing on staff members with mail infected with malware.

In most cases vulnerabilities are exploited from Windows system. The attack vector could be transfer of money (preferably by SWIFT), cash out of the ATMs of the financial institutions or usage of changing the balance of cards to unlimited[22].

Toward the end of April 2018, it was revealed that Mexico's financial system was the victim of a cyberattack in which hackers hit the interbank electronic payment system and stole over 300 million pesos ($15 million) from domestic banks[23]. The attack

[20] https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

[21] https://www.europol.europa.eu/publications-documents/carbanak/cobalt-infographic

[22] see for example https://www.group-ib.com/resources/threat-research/money-taker.html

[23] https://www.reuters.com/article/us-mexico-cyber/thieves-suck-millions-out-of-mexican-banks-in-transfer-heist-idUSKCN1IF1X7

presents many similarities with past attacks against the SWIFT systems. The attackers managed to make unauthorised transfers to accounts created for this purpose from legitimate accounts. To get their hands on the money, the cybercriminals had to go through several steps, including extracting some of the ill-gotten funds from ATMs at different locations.

GootKit is a notable APT example for its evasiveness and the stealthy way it steals confidential data and sends it back to the operators of its command and control (C&C) server. Primarily targeting European bank account holders, the malware has been known to capture videos of victims' desktops and dynamically inject fraudulent web content into the browsing sessions of users when they attempt to access their banking websites. To prevent detection by security tools, it checks for the presence of virtual machines that may be used by cybersecurity researchers to study the malware's behaviour[24].

3.3.4 Suggested Controls and Mitigation

APT is deemed a serious threat because of its nature to stay undetected for a long duration. APT malware is designed to evade detection from conventional perimeter security defences (firewalls, IDS, IPS, endpoint protection platforms and secure Web gateways) used by most organisations. APT mitigation and detection capabilities need to be incorporated in a security defence-in-depth strategy and architecture, to protect enterprises from attacks of this complexity. The traditional defence-in-depth components are still necessary, but are no longer sufficient in protecting against advanced targeted attacks and advanced malware.

Identifying possible causes of attacks and understanding what the attacker could be looking for can lead to formulating a plan to prevent APTs by locating, blocking and fixing compromised Internet enabled systems and/or IP-enabled devices. In general, however, the newest APT threats are better countered through the use of behaviour analysis tools that can not only scan for known threats but can also identify a series of actions that could be the result of a stealthy intrusion.

Spear phishing has become a very common method used by those launching APTs as an entry point to an enterprise. Often email filters are not effective enough to identify these well-designed spear-phishes and then it takes only a single user to click a link and open an attachment for an APT to begin to execute its first phase of an attack. Adding the human factor to a threat class that is not based on known vulnerabilities makes defence and prevention even more challenging.

Clearly, no single security control is able to provide effective, efficient protection, states Gartner, an IT research and advisory firm, noting that Advanced Targeted Attacks (ATAs) and advanced malware continue to plague enterprises. An APT defence strategy needs to include real-time advanced security data analytics that can identify patterns of invasive behaviour and threat intelligence for detection-remediation-prosecution, or attribution to stop attacks at an early stage.

Today’s APTs are well coordinated, organised, and methodical, which makes them particularly difficult to detect by network security administrators, as many APTs use custom-developed code and/or target zero-day vulnerabilities. Nonetheless, by using technologies of early detection with real-time reporting and visualisation, network

[24] https://www.esecurityplanet.com/threats/how-to-stop-advanced-persistent-threats.html

security administrators can try to perceive penetration as it happens before it disappears through the aspects of the system. Also, incorporating security threat intelligence into infrastructures and utilizing best-practice mechanisms and procedures may help find the malware carefully hidden by cybercriminals inside enterprise networks.

To confront such cyber-attacks will require system users to evaluate weak links in their infrastructure and employ defence controls that may recognize signs that something appears out of place. IT security managers need to look for patterns of events characteristic of APT methodologies. Tools such as a SIEM[25] solution through security logs to detect any unauthorised or suspicious object access, or else OSSEC[26] and honeypots can detect host-based attacks on computers and allow early detection of APT behaviour. Also, they can find any cyber-attacks that bypass signature-based tools and common sandboxes.

User and entity behaviour analytics (UEBA) is an indispensable tool in uncovering APTs. Increasingly employing artificial intelligence (AI), they monitor and analyse how users interact with an organisation's IT systems and can detect when they engage in anomalous behaviour, often a sign that their accounts were hacked and an attacker has infiltrated the network.

Turning the table on attackers, deception technology lures attackers into attacking fake servers, services and many other networked IT resources that are found in the typical enterprise network. When attackers waste time and energy attempting to ex-filtrate valuable data, security researchers gather valuable information about the methods they use, including insights into an attacker's kill chain, and adjust their network defences accordingly[27].

To be able to effectively defend against today’s new breed of cyber adversaries, and be able to counter APT and protect data from inappropriate access, it requires – apart from taking standard security countermeasures e.g. security hardening and patching of systems, and minimising the attack surface - strengthening existing authentication flaws (password weaknesses) and properly utilising proprietary security hardware/software. An advanced IP scanner application, for example, can help clean any form of malware, including spyware; whereas, an APT scanner device that focuses on the detection of attacker activity can be of use should antivirus software and firewalls inevitably fail.

Furthermore, to test existing defences and prepare advanced security preparedness, security professionals use the Red Team / Blue Team approach (used also by the military to test force-readiness) to identify vulnerabilities as part of the offensive attack activities, determine areas for improvement in the defensive incident response processes, identify opportunities to improve prevention and detection capabilities and develop response and remediation activities to return the IT landscape to a secure status. The Red Team is an independent internal or third party group that assesses the organisation security readiness, tests active controls and countermeasures within a

[25] **Security Information and Event Management (SIEM)** technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources.

[26] OSSEC is a platform to monitor and control your systems. It mixes together all the aspects of HIDS (host-based intrusion detection), log monitoring, and Security Incident Management (SIM)/Security Information and Event Management (SIEM) together in a simple, powerful, and open source solution.

[27] https://www.esecurityplanet.com/threats/how-to-stop-advanced-persistent-threats.html

given operational environment and validate security defences as well as the ability of internal security resources to detect and respond to advanced security threats. The Blue Team consists of internal security resources with the mission to defend the operating environment against real or simulated cyberattacks over a significant period of time by the Red Team. This is accomplished by emulating the behaviours and techniques of likely attackers in the most realistic way possible. Based on the simulation findings, recommendations are provided to increase the organisation's cybersecurity readiness posture.

To support the cybersecurity professionals in their fight against Advanced Targeted Attacks, known as ATAs, Gartner[28] has developed the Five Styles of Advanced Threat Defence Framework, which are:

- Style one – Network Traffic Analysis: The style considers inspecting Domain Name System (DNS) flow traffic in analysis; in other words, conducting in-depth network traffic monitoring and analysis with NetFlow Traffic Analyser software.
- Style two – Network Forensics: The style considers using a Network Forensic Analysis Tool (NFAT) to detect and analyse security incidents solutions that mount efficient and effective post-incident response investigations.
- Style three – Payload Analysis: The style deems this technique can provide detailed reports about malware behaviour from sandbox analysis, either as a solution on-premises or cloud-based.
- Style four – Endpoint Behaviour Analysis: The style sees Endpoint Security and Control that provide intelligence and correlation for behaviour analysis to block malware and fend off zero-day attacks, if not as a strategy for Advanced Threat Analytics defence.
- Style five – Endpoint Forensics: The style serves as an endpoint security tool that helps detect hidden malware and other signs of compromise or irregular activities on endpoints across the enterprise. It can be used to identify attacker behaviour, investigate and respond to cyber-attacks on the endpoint before critical data loss occurs.

The most effective approach, Gartner says, is to use a combination of styles. For example, one can use network/payload, payload/endpoint or network/endpoint.

3.3.5 Final Considerations / Conclusions

One of the most lucrative payment fraud forms now and for the future seems to be APT. It must be considered as a potential high risk not only for the payment infrastructure but for all network related ecosystems. With a minimal of involved criminals a maximum result can be established. Therefore all users who are normally cautious when operating their company computers but often tend to be less careful when using their smartphones or mobile devices will need to consider utilising new defence mechanisms in order to hide their data.

As more business owners utilise networked computers on the Internet, engage in cloud computing, or use personal mobile devices (BYOD) and apps (BYOA), new security threat implications are to be considered. Endpoint and network defences, as well as using the latest anti-virus software and next-gen firewalls, are effective but may not be enough for companies to keep them from being hacked. A mixed approach made of traditional tools, new advanced behaviour-based detection solutions with improved

[28] http://www.gartner.com/newsroom/id/2595015

automated monitoring, correlation and analysis, and improved incident response capabilities can aid system security administrators in identifying these hard-to-detect intrusions.

APTs have become a significant challenge for many cybersecurity professionals around the world. However, using awareness and identifying agile security solutions that can dynamically provide needed protection for Advanced Targeted Attacks (ATAs) – i.e., to achieve a deeper insight into attacker tools and tactics – can make it possible to detect and respond to APTs before they happen. What organisations can do in advance is take a proactive approach towards security and identify possible perpetrators and targets before attacks are actually carried forward. With evidence of more complex APTs in front of us as the threat landscape evolves, learning to detect – and stop - even the most advanced threats is paramount[29].

3.4 Mobile device related attacks

The use of mobile devices for both online banking and the purchase of goods and services (both online and in person) is still increasing. With this increase in usage there is a corresponding increase in the threats affecting these payments, this section is designed to provide an insight into these threats.

A mobile app(lication) is a computer program designed to run on mobile devices such as smartphones and tablet computers. Most of these devices are sold with several apps included as pre-installed software, such as a web browser, email client, calendar, mapping program, an app for buying music or other media, etc. A mobile payment usually involves a dedicated mobile app.

During the last decade, the evolution in mobile devices resulted in the deployment of more innovative mobile payments methods. Users of mobile devices can use mobile wallets, payments applications based on NFC[30] technology, peer-to-peer payment apps and others[31].

A mobile wallet is a service accessed through a mobile device, which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications. This service may reside on a mobile device owned by the consumer (i.e. the holder of the wallet) or may be remotely hosted on a secured server (or a combination thereof) or on a merchant website. Typically, the so-called mobile wallet issuer provides the wallet functionalities but the usage of the mobile wallet is under the control of the consumer. Mobile wallets are frequently used for m-commerce.

Innovations in mobile payment options facilitate adoption of the technology by consumers and businesses, but also increase the interest of fraudsters to steal money, payment card information or history of operations. Attacks aided by AI, sophisticated social engineering techniques and the exponential growth of connected devices, are just a few of the factors that paved the way in the year 2018 of unprecedented threat to the enterprise. According to Wandera “Understanding the mobile threat landscape in 2018” report, in 2017 we saw 95% growth in mobile security breaches, 88% rise in business

[29] http://resources.infosecinstitute.com/current-trends-apt-world/#gref

[30] A contactless protocol specified by ISO/IEC 18092

[31] Innovative Mobile Payment Apps according to Practical Ecommerce: http://www.practicalecommerce.com/articles/87765-11-Innovative-Mobile-Payment-Apps

targeted by mobile ransomware, and mobile threats became the #1 challenge for security teams.

The principal payments and banking activities carried out using mobile devices are:

- To carry out online banking activities through mobile apps and mobile browsers;
- To make purchases online through mobile apps and mobile browsers;
- To receive out of band authentication mechanisms (i.e. SMS Based Authentication, or push messages);
- To make in person purchases of products and services via proximity based mechanisms (e.g. contactless NFC payments[32]);
- To make person to person (P2P)[33] and person to business (P2B) payments via an app.

The principal threats which these devices are facing include:

- Malicious apps purporting to be banking apps;
- SIM swap based attacks;
- Cloning of SIM cards;
- To exploit new contactless payment methods in which a traditional payment mechanism, e.g. a credit card, is stored on a mobile device for contactless transactions;
- To obtain SMS based verification and/or validation messages e.g., payment verification, set up of new payee, digital wallet provisioning, etc.;
- Phishing and Vishing attacks specifically targeting the mobile device;
- Malware infecting the mobile device, compromising the legitimate use of the device, including rooting the device to facilitate further attacks, and stealing credentials etc.;
- Spoofed SMS messages to people purporting to be from their PSP to encourage them to call a compromised number or visit a malicious website.

[32] A contactless/NFC payment is a service accessed through a mobile device equipped with a Near Field Communication (NFC) antenna or sticker and a mobile payment application. The payment transaction is processed over the app that functions as a contactless credit card. Thus the user can use its mobile phone to pay at the point of sale terminals and/or to withdraw cash from an ATM. The mobile application can store encrypted card information on the SIM card (HW solution - Secure Element (SE)) or on a secure central server environment (SW solution - Host Card Emulation (HCE)).

[33] A Person-to-Person payment allows an individual to transfer money to another individual's account without knowing their payment account via the Internet. But new P2P apps use a different approach based on mobile applications. The beneficiary is designated by email or by phone number. Once the transfer has been initiated by the payer, the beneficiary receives a notification to use the P2P app to input payment account information and a routing number where the funds may be transferred to. A P2P payment method is frequently used to transfer money between friends or to split bills.

- Smishing SMS messages to people purporting to be from a trusted source (e.g. Bank) to encourage them revealing their mobile/internet banking credentials to crooks.

For the purpose of this document, the threats identified above will be grouped into two categories; attacks targeting the mobile device (and its use, including mobile applications and mobile wallets) and SIM swap based attacks.

3.4.1 Attacks Targeting the Mobile Device

3.4.1.1 Impact & Context

RiskIQ discovered 21,948 blacklisted mobile apps across 120 mobile app stores and the open internet.

“There is a large number of secondary and affiliate stores, primarily serving the Android market, which provide an opportunity for malicious actors to compromise legitimate apps and launch fake apps,” the RiskIQ report warned. “Organisations must do more to monitor the app store ecosystem for stores hosting their apps without permission and for apps impersonating their brand. Users should stick to the primary app stores where possible and be vigilant in researching apps they want to download,” the report said.

Mobile security, according to JR Raphael of ‘CSO from IDG’[34], is at the top of every company's worry list these days, because nearly all workers now routinely access corporate data from smartphones, and that means keeping sensitive info out of the wrong hands is an increasingly intricate puzzle. The stakes are higher than ever: The average cost of a corporate data breach is $21,155 *per day*, according to a 2016 report by the Ponemon Institute.

The truth is that mobile malware infections are uncommon in the real world. That's thanks to both the nature of mobile malware and the inherent protections built into mobile operating systems.

The more realistic mobile security hazards, according to JR Raphael, lie in the following easily overlooked areas, all of which are expected to remain relevant in the coming years:

Data leakage

Data leakage is widely seen as being one of the most worrisome threats to enterprise security for 2018. It's a matter of users inadvertently making ill-advised decisions about which apps are able to see and transfer their information.

"The main challenge is how to implement an app vetting process that does not overwhelm the administrator and does not frustrate the users," says D. Zumerle, research director for mobile security at Gartner. He suggests turning to mobile threat defense (MTD) solutions. Such utilities scan apps for "leaky behavior," Zumerle says, and can automate the blocking of problematic processes.

Of course, even that won't always cover leakage that happens as a result of overt user error — something as simple as transferring company files onto a public cloud storage service, pasting confidential info in the wrong place, or forwarding an email to an unintended recipient.

[34] https://www.csoonline.com/article/3241727/mobile-security/5-mobile-security-threats-you-should-take-seriously-in-2018.html Parts of the article are presented verbatim below.

Data Loss Prevention (DLP) tools are designed explicitly to prevent the exposure of sensitive information, including accidental scenarios.

Social engineering

Despite the ease with which one would think social engineering cons could be avoided, they remain astonishingly effective.

A staggering 90% of data breaches observed by Verizon's Enterprise Solutions division are the result of phishing, according to the company's 2017 Data Breach Investigations Report. While only 7% of users fall for phishing attempts, Verizon says, those gullible guys tend to be repeated offenders: The company estimates that in a typical organisation, 15% of users who are successfully phished will be phished *at least* one more time within the same year.

What's more, numerous bits of research suggest users are more vulnerable to phishing from mobile devices than desktops — by as much as three times, according to an IBM study, in part because a phone is where people are most likely to first see a message. "We do see a general rise in mobile susceptibility driven by increases in mobile computing overall [and] the continued growth of BYOD work environments" says PhishMe’s J. Robinson.

Robinson notes that the line between work and personal computing is also continuing to blur. More and more workers are viewing multiple inboxes — connected to a combination of work and personal accounts — together on a smartphone, he notes, and almost everyone conducts some sort of personal business online during the workday. Consequently, the notion of receiving what appears to be a personal email alongside work-related messages doesn't seem at all unusual on the surface, even if it may in fact be a ruse.

Wi-Fi interference

A mobile device is only as secure as the network through which it is transmitting data. In an era where we are all constantly connecting to public Wi-Fi networks, that means our info often is not as secure as we might assume.

According to new research, being released by enterprise security firm Wandera, corporate mobile devices use Wi-Fi almost three times as much as they use cellular data. Nearly a quarter of devices have connected to open and potentially insecure Wi-Fi networks, and 4% of devices have encountered a man-in-the-middle attack — in which someone maliciously intercepts communication between two parties — within the most recent month.

"These days, it's not difficult to encrypt traffic," says prof. Kevin Du of Syracuse University who specialises in smartphone security. "If you don't have a VPN, you are leaving a lot of doors on your perimeters open."

Selecting the right enterprise-class VPN, however, is not so easy. As with most security-related considerations, a tradeoff is almost always required. "The delivery of VPNs needs to be smarter with mobile devices, as minimizing the consumption of resources — mainly battery — is paramount," Gartner's Zumerle points out. An effective VPN should know to activate only when absolutely necessary, he says, not when a user is accessing a news site, for instance, or when a user is working within an app that is known to be trustworthy and secure.

Out-of-date devices

Smartphones, tablets and smaller connected devices — commonly known as the internet of things (IoT) — pose a new risk to enterprise security in that unlike traditional work devices, they generally do not come with guarantees of timely and ongoing software updates. This is true particularly on the Android front, where the vast majority of manufacturers are not so effective at keeping their products up to date — both with operating system (OS) updates and the smaller monthly security patches between them — as well as with IoT devices, many of which aren't even designed to get updates in the first place.

"Many of them don't even have a patching mechanism built in, and that's becoming more and more of a threat these days," Du says.

Again, a strong policy goes a long way. There *are* Android devices that do receive timely and reliable ongoing updates. Until the IoT landscape becomes less of a wild west, it falls upon a company to create its own security net around them.

Physical device breaches

Last but not least is something that seems silly but remains a disturbingly realistic threat: A lost or unattended device can be a major security risk, especially if it doesn't have a strong PIN or password and full data encryption.

In a 2016 Ponemon Institute study, 35% of professionals indicated their work devices had no mandated measures in place to secure accessible corporate data. Worse yet, nearly half of those surveyed said they had no password, PIN, or biometric security guarding their devices — and about two-thirds said they didn't use encryption. 86% of respondents indicated they sometimes shared passwords across personal and work accounts accessed via their mobile devices[35].

According to Kaspersky Security Bulleting predictions for 2018 “Novice mobile banking users will be a new prime target for criminals. Digital banks will continue revolutionizing the financial sector on a global scale, especially in emerging markets. For example, in Brazil and Mexico, these banks are gaining more and more momentum and this, of course, has attracted cybercriminal attention. We are sure that the world of cybercrime will see increasing attacks against this type of banks and their customers. Their main feature is the complete absence of branches and traditional customer service. All communication between the bank and its customers actually occur through a mobile application. This can have several consequences.

The first is a decrease in the number of Windows Trojans, aimed at stealing money through traditional internet banking. The second is that the growing number of digital financial institutions will lead to organic growth in the number of users that are easy targets for cybercriminals: people without any mobile banking experience, but with banking applications installed on their mobile devices. These people will be the main targets for both malware attacks, such as Svpeng, and schemes completely built on social engineering. Persuading a customer to transfer money through a mobile application is much easier than forcing them to go to a physical bank and make a transaction”[36].

[35] https://www.csoonline.com/article/3241727/mobile-security/5-mobile-security-threats-you-should-take-seriously-in-2018.html

[36] https://securelist.com/cybercriminals-vs-financial-institutions/83370/

In the Q1 2018 McAfee Mobile Threat Report, it is stated that "One of the most significant concerns we have come across in the last 12 months is the evolution of targeted attacks moving to mobile devices. It took 20 years to reach two million malware samples on the PC. It took just five years to do the same on mobile.

Banking Trojans target both large multinationals and small regional banks using specially crafted mobile apps or phishing campaigns. Take, for instance, the Android/MoqHao malware aimed at major Korean banks. This threat spreads via SMS using a clever social engineering lure—asking the recipients to verify a picture of themselves. Once the recipient clicks on the malicious link, it installs a fake banking app and then scans for and deletes legitimate banking apps on the user's phone. McAfee Labs detected over 16 million mobile malware infestations in the third quarter of 2017 alone, nearly doubling the number we saw a year earlier.

In 2017 we saw an increase in malicious banking Trojans, such as the Android/Marcher malware. We have also seen mobile banking Trojans delivered as fake updates or through targeted email or SMS phishing. But the most sophisticated so far has been the Android/LokiBot malware, which takes all the functions of Android/Marcher and adds crypto ransomware capabilities, among other malicious activities. Android/LokiBot has targeted more than 100 financial institutions around the world. By our estimate LokiBot has generated close to $2 million in revenue from kit sales on the "dark web"[37].

Fake Banking Apps

During the last 2-3 years there have been a number of instances where fake copies of banking mobile apps have been released in an attempt to try and get users to install the application and then use the app to attempt to connect to their PSP; some attacks with fake non-PSP apps have also been seen. In most instances, these apps are found on "grey market" sites rather than official app stores such as iTunes or Google Play, but there have been isolated instances where a fake banking app has been uploaded to an official market place (Google Play). One of the most famous example is FANDA SDK[38], a variant of Android malware that poses as a fake banking app to trick users into compliance, after which it locks users out of their smartphones and sets about emptying their accounts, while victims scramble to access their phones again. It has been around since December 2015.

Fake Social Media and Messaging Apps

As well as fake banking apps there has also been an increase in fake apps that purport to be social media or messaging apps such as WhatsApp, in one case in 2017 a fake version of WhatsApp was downloaded over a million times before being identified[39]. In this particular instance the fake app appeared to being used to deliver advertising to make money for the creators, but the app could as easily have been used to deliver further malware.

[37] McAfee Mobile Threat Report Q1, 2018

[38] http://www.ibtimes.co.uk/android-malware-masquerading-fake-bank-app-empties-accounts-by-locking-users-out-their-phones-1562499

[39] https://www.zdnet.com/article/fake-whatsapp-app-fooled-million-android-users-on-google-play-did-you-fall-for-it/

Mobile Malware

Malware targeting mobile devices continues to proliferate. Mobile malware is now one of the top priorities for every company, considering the increased number of cyberattacks and incidents. As per a survey by McAfee Labs, more than 20 million mobile malware incidents were registered in the first quarter of 2018, which includes over 2.5 million new and unfamiliar mobile malware attacks[40].

Spoofed SMS Messages

This attack is very successful as most users believe that an SMS is more secure than an email, users are aware of the fact that spam and phishing mails exists but so far the awareness of a similar and even worse problem existing on SMS is not something that the public is aware of. An SMS is not only seen as more trustworthy than an email, it is also something which is personal, and which requires almost immediate action. The fact that an SMS can easily be spoofed and that it can be intercepted and read by external parties is often not realised by the end users.

Criminals are increasingly sending SMS messages which appear to come from the victim’s PSP in an attempt to steal personal or financial information (also known as smishing). The texts encourage people to call a number or visit a website, often claiming some sort of urgency. However, the telephone number or website is actually controlled by the fraudster, enabling them to steal security details that can be used to access the victim’s bank account and steal money.

Attackers utilise software to alter the ID of the sender of the message so that it appears as the name of the PSP, with many current smartphones, this means that the message will be displayed together with previous, legitimate messages from the PSP, increasing the likelihood that the message will be considered genuine. Very few techniques to prevent this exist, but it seems that Germany is very well protected as the telecom operators have set up a whitelisting protection. This could be used as inspiration for other countries.

As well as pointing users towards compromised websites, attackers are also utilising land line numbers and simply asking recipients to ring the number to contact their PSP, this is in the hope that the victim will phone the number from which the text was sent, which is controlled by the fraudster, rather than the PSP’s regular customer service telephone number.

Phishing Attacks

Phishing attacks against mobile devices continue to grow, in an attempt to gain a foothold on the device and either enable malware to be installed on the device, or to lure the user to a malicious URL. Enabling an exploitation of the mobile devices, namely smaller screens that can make it more difficult to review the URL, and simple user interfaces for logging into applications can be easy to mimic.

Other types of attacks on mobile applications

There are also several types of methods used over mobile applications which are worth describing. These are becoming the norm and make use of different attack vectors. Some have already been described above such as the use of fake applications or the tampering of applications.

[40] McAfee Mobile Threat Report Q1, 2018

- Poor application and Operating System security:
  - Poor consumer data protection on device (visibility of authentication information, transaction history, personal data and other sensitive information to attackers once they have gained access to a device or application).
  - Usage of not properly secured third party code libraries to speed up mobile application development (for example Heartbleed exploit).
  - Meet-in-the-middle Attack – connection hijacking.
  - Man-in-the-middle Attacks are increasing when using web browsers (i.e. Dridex type) in mobile devices.
  - Vulnerabilities not patched quickly enough in Applications and OS.
- Lack of user awareness:

  Smartphone users are often not aware about practicing adequate security habits (i.e. no device access control, easy to hack passwords or lack of them, connections to unsecure WiFi and/or Bluetooth always activated, download of malicious applications, phishing (see also section 2.2 – Phishing Attacks), social engineering, device OS tampering (jailbroken, rooted), credentials storage, etc...).
- Abuse of Privacy:
  - A great variety of applications can access private and personal information with the permission of the user. In this case the application may not be malicious but the customers are granting access to the application developer's company without being aware that very sensitive information is being shared or who will eventually have access to this information (as an example, games asking access to the agenda, location, photos, etc...).
  - Mobile phones are mixing personal and corporate usage.
  - Mobiles are gathering more and more information from the customer, which aggregated could help to carry out sophisticated attacks.
- Enrolment process:

  Fraudsters are taking advantage of the high volume of new enrolments occurring nowadays. Certain global payment apps have been exploited in that respect during the past years.
- Biometric authentication:

  Numerous studies and frauds have shown that biometric authentication in payments without a second factor can be weak and result in frauds, especially if the fraudster can access physically the smartphone.
- Duplicated or cloned SIMs:
  - There is an increasing trend from fraudsters to duplicate SIMs so as to commit fraud. This attack is similar to SIM swapping (see section 3.4.2) but with the difference that cloning will preserve the original SIM card and therefore could be more difficult to be detected by the victim.
  - Only older SIMs are cloneable, and the process is both time-consuming, technically difficult and requires a provider which uses old authentication algorithms. The cloning process also leaves the risk of rendering the original SIM card inoperative. A successfully cloned SIM will allow the attacker to receive SMS messages and calls instead of the victim.

3.4.1.2 Suggested Controls and Mitigation

There are a number of measures that users can implement to mitigate the threats related to mobile devices, these include:

- Update the software running on your mobile device with the latest security patches and upgrades, these should be sent to you by your network / operating system provider.
- Use a secure lock screen, set a password, PIN or fingerprint to unlock your device.
- Do not allow applications to be installed from unknown / untrusted sources.
- Do not allow jailbroken or rooted devices.
- Add a PIN or Passcode to the voicemail on your mobile device.
- Do not use a PIN code which is your date of birth or which is part of an otherwise well-known information.
- Install anti-virus software on your mobile device.
- If asked to call your PSP via a number given in a text message, call your PSP on a number that you trust, for example via the number on the back of your bank card.
- Remember that your PSP will never contact you to ask for your card PIN or online banking credentials, or to transfer money to a new account for fraud reasons.
- Create aware campaigns to educate consumers on how to avoid the previous explained fraud scenarios.
- Monitor App stores and Internet for fake applications.
- Implement anti tampering controls.
- Protect app code with code signing and / or obfuscation.
- Implement strong sensitive data encryption on device.
- Perform Application Penetration testing.
- Do not consider frequently used third-party libraries as secure and validate them before using them.
- Implement controls to protect communication channel.
- Implement device owner/user verification.
- Implement mobile device verification.
- Use two-factor authentication when the risk is high.

3.4.2 SIM swapping

3.4.2.1 Definition and fraud description

SIM (Subscriber Identification Module) swapping is a legitimate service operated by mobile network operators. Historically the main reason for carrying out the swap has been in order to provide consumers flexibility in moving to other mobile network operators whilst keeping their existing mobile number and/or efficiently resuming a customers' mobile service following a lost or stolen mobile device. However, the ongoing development of smartphones has seen a movement in SIM card size from standard through to micro, and now nano SIM size. This change in size has resulted in an increased number of legitimate SIM swaps as consumers upgrade their mobile devices.

Fraudsters obtain and utilise a customer's replacement SIM card to acquire security messages and one-time passwords (OTP) sent to the customer by the PSP. Using the OTP, criminals are able to change, add beneficiaries and transfer money out of the customer's account using their personal information that they would have obtained through phishing. During a normal online banking session, a PSP (using out-of-band SMS or voice authentication) will send the customer a One-Time Password (OTP), also known as a Mobile Transaction Authorisation Number (MTAN), via SMS or voice call to their mobile telephone number. The customer is then prompted to relay back the MTAN. Typically a PSP will initiate this service during the online banking login stage or when a payment transfer is requested.

With the continuing rise of new payment mechanisms on mobile devices, SIM swaps are also being used to exploit these mechanisms, to ensure that verification and validation messages are not received by the legitimate owner. By utilising a SIM swap fraudsters are able to provision a stolen credit card onto certain types of smartphones and then make payments. The total fraud via this mechanism may potentially be much larger than for other mobile contactless transactions as some solutions have no limit on the transaction.

A SIM swapped mobile phone (the victim's) would cease to work properly and would report an error such as “unable to connect to network” or “emergency service only” on screen.

3.4.2.2 Impact and Context

Legitimate SIM swaps are increasing due to the movement to smaller SIM cards (micro and nano cards), which is providing malicious attackers with legitimate activities to cover their actions under. However, it is very difficult to obtain accurate figures on fraud committed in part through the use of exploiting weaknesses in the SIM swapping process. During 2017 main stream media have also reported issues on the SMS protocol (SS7) [41] which have then been denied by the potential affected telecommunication company.[42]

In a recent article of February 2018 from “The Guardian” The security procedures of a giant mobile phone company have been branded “totally inadequate” after fraudsters hijacked a customer's phone and tried to empty his bank account[43].

3.4.2.3 Suggested Controls and Mitigation

There are a number of controls that end users can implement to try and prevent, or at least quickly detect, SIM swapping:

- Enquire with your mobile operator if you have no network connectivity and you are not receiving any calls or SMS for unusually long periods;

[41] http://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

[42] https://www.telekom.com/en/company/details/ss7-security-vulnerability-dt-customers-not-affected-493758

[43] https://www.theguardian.com/money/2018/feb/10/ee-sim-card-swap-fraud-security

- Keep personal details that would be useful to a fraudster, i.e. phone number, date of birth etc. off Social Media sites;
- Ask your PSP to give you details of every financial transaction through two channels - for instance, SMS as well as email alerts;
- A PSP can negotiate with the mobile operators that the PSP is informed about the SIM swaps. This can help in monitoring the usage of the account.

Previous cybercrime reports have recommended that a movement away from MTAN authentication to hardware token authentication be advised[44], however during the period since the last report there has been a considerable increase in the use of the mobile device, whether via SMS, call or application as the authentication mechanism. It is highly unlikely that a large scale movement to hardware based tokens to be used in conjunction with mobile devices could be achieved.

Technological solutions to try and secure the mobile device and enable out-of-band authentication via the device continue to be developed and implemented, however, as of today these remain relatively niche offerings.

3.4.3 Final Considerations/Conclusions

Consumers spend increasingly more time on internet and mobile every day (a daily average use time across European countries ranging between 4:09h and 3:26h on laptop and desktop, between 2:08h and 1:08h on mobile phone) and the smartphone constitutes an immediate reliable channel between the bank and its customers.

The growing use of mobile devices to surf the web and make online payments has caused a steady rise in the number of targeted attacks. Every year, fraud-related incidents are generating increasingly heavy costs for banking establishments and the techniques employed are becoming more sophisticated.
Mobile banking security must be ensured at all levels, namely:

- During on-boarding, when the basic minimum requires the formal validation of the future client's identity. Additional verification is needed to fine-tune customer scoring and thus ensure the client presents no significant risk for the bank. This should, however, be carried out in an intelligent manner so as not to lose the future client.
- Every time clients access their banking services: a progressive authentication mechanism should be implemented to match the level of transaction risk. This mechanism may be supplemented with basic techniques such as token binding. Transparent user-ID authentication technologies, such as behavioural biometrics, can also be used to streamline the user experience.
- During sensitive transactions, for which Machine Learning can be used to automatically identify suspicious data flows requiring in-depth verification. The optimisation and automation of these mechanisms considerably reduces the level of fraud criticality[45].

[44] http://www.eweek.com/security/nist-says-sms-based-two-factor-authentication-isn-t-secure
https://pages.nist.gov/800-63-3/sp800-63b.html

[45] Efma report: Building the future of mobile banking report
https://www.efma.com/study/detail/27241

Attacks targeting the mobile device and their use will continue to develop and increase as more and more activities, including financial transactions, are carried out using these devices. Mobile devices and their applications are becoming the most used way to connect customers with their PSP to the detriment of the browser. From a security perspective this is a crucial change, whilst before customers had to “go to their PSP” through the browser, currently customers download applications on their smartphones from their PSPs or even dedicated stores “go to their PSP” (in analogy to “fat” clients on PCs).

Both for browser access and mobile apps, PSPs will need to define security policies and maintain appropriate infrastructures. The suggested controls to mitigate fraud should be considered as part of a risk management governance. For effective risk management and protection against threats, it is imperative that an organisation have full insight and visibility into how devices are being used. Attackers will utilise all methods available, including social engineering attempts on the end user, malware on the mobile device, and even attempts to subvert the communication mechanism in an attempt to compromise the device. Mitigation activities should focus on all of these channels in a collaborative manner: continued end user awareness programmes to inform them of the risks, the implementation of anti-malware and virus controls on the devices and have a security solution monitoring device traffic at all times, ensuring that insecure Wi-Fi connections are flagged, traffic to phishing sites is detected and blocked at the proxy level and vulnerabilities are examined before they can be used against the organisation.

3.5 Denial of Service

3.5.1 Definition

A *Denial-of-Service* (DoS) attack is an attempt to make a system / application or network resource unavailable to its users for their intended purposes, such as to interrupt or suspend services of a host connected to the Internet. A successful DoS attack directly affects the availability of a network system (server, system, platform etc).

Most of the DoS attacks are “*Distributed Denial of Service*” attacks (DDoS attacks). A DDoS attack is an attack in which multiple computer systems attack a target, such as a server, website or other network resource, and potentially causes a denial of service for users of the targeted resource.

According to security companies, in the period between 2012 and 2016 the main responsibility for the increase in frequency and power of DDoS attacks lay with websites that offer DDoS attacks as a service, also called booters.

3.5.2 Fraud Description

DoS attacks cause the victims’ systems to reset or to exhaust their resources, be it communication bandwidth, memory, processing or any other resource, that leads the targeted system to fail or to be put out of service. It usually consists of a concerted effort by one or multiple persons / systems to prevent an Internet site or service from functioning normally. Recent developments show that Internet of Things (IoT) devices are often not sufficiently secured and can well be infected by criminal organisations in order to “participate” in a Distributed DoS attack.

The ease for criminals, “script kiddies”, etc. to prepare and execute a DoS attack is increasing. It is relatively easy and not expensive to “buy” attack capabilities on the

Internet. Two categories of perpetrators may be distinguished: “old school hackers” or “hacktivists” who just want to have a name or defend an ideology and the “hackers that essentially pursue financial gain”. The latter ones use all means, human or technical failure, available to create blackmail or massive fraud. Moreover, DoS attacks are also used to conceal other attacks and distract the defenders.

DoS attacks are in general DDoS attacks. These attacks are performed by many – sometimes hundreds of thousands – nodes at the same time.

Note that a (D)DoS attack has a potential for collateral damage – where other components than the originally targeted for (D)DoS are also impacted and potentially taken down.

Distinction can be made between three basic types of (D)DoS attacks:

The flooding attack

The term ‘flood’ is a collective term used to describe the most basic form of (D)DoS attacks, namely those attacks that focus on making it impossible to gain access to a system or service, by exceeding the maximum bandwidth available. Exceeding the maximum available bandwidth means there is not enough bandwidth left for the legitimate data traffic.

A special form of a flooding attack is the so called amplification attack, for example a DNS-amplification attack. In an DNS-amplification attack, the attacker spoofs look-up requests to domain name system (DNS) servers to hide the source of the exploit and direct the response to the target. Through various techniques, the attacker turns a small DNS query into a much larger payload directed at the target network.

The size of attacks is increasing caused by the number of infected end points. Moreover, the possibility to increase the size of an attack by combining it with a amplification attack is worrying.

The protocol attack

Another way of causing a (D)DoS attack is to send data packets that take advantage of weaknesses in the communication protocols and other protocols used by mainly network devices as routers and firewall’s. These devices receive packets for processing that lead to unexpected results. For example a large number of communication sessions are opened without being properly closed in due time, this way consuming the resources of the network device; as a result they can no longer accept any new sessions. Well known examples of protocol-attacks are SYN floods, fragmented packet attacks, Ping of Death and Smurf-attacks. The number of SYN-flooding attacks is increasing. In many cases the botnets used contain so called Internet of Things (IoT) devices. Examples of these devices are consumer electronics like home-routers, IP-cameras and smart-TV’s. There are a lot of these devices nowadays and most of them are badly administered, resulting in non-patched systems and default administrator credentials.

The application-layer attack

An application layer DDoS attack is named after the OSI-layers’ Application Layer (layer 7). The attacker is aiming at a specific function of a layer 7 protocol like http and misuses that function to exhaust the service. An example is the misuse of the GET/POST-function of http, performing a so called slow attack which causes the webserver to wait for a long time before answering the request of a web browser. An attack is disguised to look like legitimate traffic, except it targets specific function of the protocol it attacks. There is often not much bandwidth consumed and the e.g. webserver just crashes. Application-layer attacks cannot be recognised as a DoS-attack during the encrypted transport. Only after decryption an application-layer attack can be recognised and mitigated.

Combined attacks

At present combined attacks are becoming more frequent, using for example floodings and application-layer attacks at the same time, making mitigation of the attacks more complex.

3.5.3 Impact & Context

In 2016 there has been a number of very large scale attacks on non-PSPs. The one on “Krebsonsecurity” was a long lasting attack of approximately 650 Gbps. However, in March 2018 a memcached[46] amplification attack broke a new DDoS record at 1.7 Tb/s.

The attacks mentioned above were possible, because of the fact that many IoT devices were infected. Corero Network Security reported in Q3 2017 that organisations experienced, mainly due to infected IoT devices, an average of 237 DDoS attack attempts per month - or eight per day. These numbers represent a 91% increase from Q1 2017. Troubling to security experts was that the attackers relied on Mirai, an easy-to-use program that allows even unskilled hackers to take over online devices and use them to launch DDoS attacks[47].

Also in 2017 a number of European PSPs have experienced (D)DoS attacks. In a number of cases these PSPs have encountered a relatively small (D)DoS attack and received a blackmail attempt via email. The only correct practice is to not “give-in”. Also PSPs in Europe have seen larger attacks, even over 100 Gbps. The current scrubbing services are (assuming sufficient capacity has been bought by the PSP) able to handle this size of attacks. Most scrubbing services have increased their capabilities after the large scale attacks in 2016.

PSPs have seen an increase in more complex types of attacks, like combined attacks (flooding and application-layer attacks using HTTPS) are gaining in popularity. One example was the combined attack on the Moscow stock exchange. PSPs should take mitigating measures, also on application-layer attacks.

The potential impact of a (D)DoS attack is twofold. On the one hand it can lead to the temporary unavailability of a PSP, including all its services, e.g. Internet banking, mobile banking, but also non-payment related services. And that can again lead to a form of blackmail by the attacker and/or – caused by a focus of many on re-establishing the service – a potential increase in successful fraud attempts. On the other hand, a consequence can be damage to the reputation of the attacked PSP, where e.g. the Internet banking service is “again” not available.

It is clear that (D)DoS attacks are not a PSP specific issue, but it is also a threat to the financial sector. The threat is well known now in the sector and most PSPs have taken mitigating measures against these kind of threats (see below).

[46] Memcached is a database caching system for speeding up websites and networks.

[47] see http://usat.ly/2eB5RZA

3.5.4 Suggested Controls and Mitigation

PSPs have controls and mitigating measures in place against (D)DoS attacks.

PSPs should preferably set up a (DDoS) security control framework. In general terms a PSP should have controls in place in order to be able to identify, protect, detect, respond, recover, assess and adjust possible DDoS attacks. The table below gives a high level of description of these controls[48].

Level	Description
Identify	Develop the organisational understanding to manage DDoS risk to systems, assets, data and capabilities
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
Detect	Develop and implement the appropriate activities to identify the occurrence of a DDoS attack
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
Recover	Develop and implement the appropriate activities to maintain plans for resilience to restore any capabilities or services that were impaired due to a DDoS event
Assess	Determine whether the previous functions performed/functioned effectively
Adjust	Determine which changes need to be made, based on the assessment made

Table 4: High level dynamic DDoS security control framework

The Internet Engineering Task Force (IETF) established a new working group DDoS Open Threat Signalling (DOTS). The aim of DOTS is to develop a standards based approach for the real time signalling of DDoS related telemetry and threat handling requests and data between elements concerned with DDoS attack detection, classification, trace-back, and mitigation.

In general, PSPs are expected to have implemented a so-called "*(D)DoS mitigation scrubbing service*". This is a service to filter the fraudulent traffic of the (D)DoS attacks. Scrubbing is more specifically a good mitigating measure against flooding attacks and sometimes mitigating protocol-attacks. Scrubbing services are provided by third party service providers.

Since protocol- and application attacks comply with the standard for the protocol in question, it is more difficult to counteract such attacks. PSPs have implemented or should implement mitigating measures against application level attacks including for instance application-level security products, application level key completion indicators; filtering capabilities, etc.

[48] more details may be found in chapter 5 in http://www.vurore.nl/images/vurore/downloads/scripties/2040-Def.scriptie_LarsDrost.pdf

PSPs can simulate attacks on their environment in order to prove that mitigating measures (including organisation and personnel) are adequate. Moreover, every entity should also test periodically their anti (D)DoS measures (e.g. through (D)DoS simulations). This testing should cover both the technical and the organisational aspects (e.g. procedures).

One additional set of countermeasures is to organise security intelligence. It is important to know what types of DDoS and what type of actors and motivations are around; it helps to take accurate measures and to determine the (residual) risk of the organisation of getting hit by DDoS-attacks. Security intelligence can be received from a commercial organisation and/or a governmental or industry specific Computer Emergency Response Team (CERT), which are a good answer to deter the effects of (D)DoS activities. The so called initiative NoMoreDDoS is being discussed in the Netherlands at this moment. The aim is to work together with the national police.

PSPs should consult their upstream (telecom) provider and the local Law Enforcement Agency to check whether the logging capabilities of the PSP and the monitoring solutions of the PSP offer sufficient capabilities for the PSP to be *"forensic ready"* for law enforcement.

3.5.5 Final Considerations/Conclusions

(D)DoS attacks have been an increasing threat in the past few years, given the fact that the number of infected end points available is increasing and so is (in a number of cases) the size of the attack. Though in 2017 the DDoS attacks seem to be relatively light in number and size, it is realistic to test and possibly upgrade measures, as there are more and more opportunities to misuse IoT devices and it remains simple to "buy" DDoS attack capabilities for less than 100 euros. The expected future, and already seen in some countries, is that more sophisticated combined attacks will take place. Measures to mitigate the basic kind of (D)DoS attack should be common – and seem to be common – to all financial institutions. Moreover, (D)DoS attacks are not specific to the financial sector. Targeted organisations include a wide range: government and related organisations, police, military, security sector organisations and organisations perceived to be against the ideologies of certain hacktivists groups.

Over the past years, attackers aimed at little financial gain through these attacks. However, it is realistic to assume that criminals will use (D)DoS as a means for blackmailing or stealing confidential (corporate) information.

A further development could be that a successful (D)DoS attack could distract the PSPs attention from fraudulent transactions, leading to more "successes" for criminals with phishing and/or malware attacks on Internet banking.

It is probable that (D)DoS attacks will continue in the near future and that financial institutions remain potential targets. One may not ignore that the probability of these attacks continuing in the near future is high (e.g., in view of the increased usage of IoT devices) and that financial and payments sector organisations remain potential targets. This could potentially lead to very large scale DDoS attacks. In a number of countries telecom providers are investigating filtering capabilities on a country level or a "trusted telecom provider" level in order to be able to mitigate also these very large scale attacks. A possible approach to defend organisations against DDoS attacks is common in the US military, the Defense Readiness Condition. For DOS attacks it would mean that DEFCON 5 defines that all systems work normally and no countermeasures are in use. And DEFCON 0 defines that the continuity of the vital infrastructure is seriously at stake and internet service providers can decide to shut down all external links. Furthermore one could evaluate whether the current security architecture and countermeasures are still sufficient.

Several reports about DDoS conclude that collaboration is critical for effective DDoS mitigation and making the financial sector more resilient. On a national level this would mean that PSP's, universities, internet service providers, internet exchanges, responsible governmental cyber authorities, and the central bank have to work together. To reduce the number of DDoS attacks the national police force has to be involved as well by exchanging information, collecting evidence, intervening in payments to DDoS-as-a-service suppliers and so on. The measures investigated at least in the Netherlands is to develop a 'firewall for the country' solution[49]. Governance is of course an issue of this initiative. Also Europol sees this as an issue and organised a first meeting with an international scope on this subject in 2018.

3.6 Botnets

3.6.1 Definition

The word "botnet" is a combination of the words "robot" and "network"; botnets are recently distinguished between *traditional* and *IoT* ones.

Traditional Botnets - A traditional botnet (also known as "zombie army") is a collection of Internet-connected devices, mainly computers, which have been compromised, are remotely controlled and each of which is running one or more "bots", i.e. a software application that runs automated tasks (scripts) over the Internet. The owner of a botnet called "botmaster" or "bot herder", can control the botnet using command and control (C&C) software.

IoT Botnets - An IoT botnet is a collection of compromised IoT devices, such as cameras, routers, DVRs, wearables and other embedded technologies, infected with malware. This malware allows an attacker to control the devices, carrying out tasks just like a traditional botnet. Unlike traditional botnets, infected IoT devices seek to spread their malware, persistently targeting more and more devices. While a traditional botnet may consist of hundreds of thousands of devices, an IoT botnet is larger in scale, with several millions of compromised devices.

3.6.2 Fraud Description

The top attacked industry (39%), according to the IBM "MSS alert data"[50], is Financial Services.

The main motivation for the operation of botnets is to generate financial profit from the activities they allow. Further generation of profits comes from offering botnet services to third parties (crime-as-a-service). Other possible motivations include political or even military interests. Botnets can be used as a means to accomplish several types of

[49] see for instance https://www.dcboard.nl/home

[50] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03086USEN

criminal or fraudulent actions (as stated in the ENISA report "Botnets: Detection, Measurement, Disinfection and Defense"[51]):

Keylogging & Identity Theft

A major use of botnets, with the intention of gaining financial benefits, is for the automated extraction of user data and credentials from infected hosts.

Spam email

One of the most popular uses of botnets is spamming. The ability of botnets to use bots' IP addresses to hide the true originator of the spam email complicates countermeasures such as the blacklisting of suspicious IP addresses.

Click Fraud and Pay-Per-Install

The attacker sets up an account with an online advertiser, who pays for page visits or for additional advertising links by, for example, clicking on a banner. Then, the attacker uses the controlled bots to visit those pages and to generate clicks on the target banners. With the pay-per-install (PPI) method the botmaster offers to install software on target machines for his customers.

CAPCHA Solving

Capcha bypass is a botnet attack that makes attempts to solve the capcha puzzle.

Source of Anonymity

A method to hide the botmaster's real address and location.

Distributed Denial of Service (DDoS)

Botnets usually consist of such large numbers of remote machines that their cumulative bandwidth can reach hundreds of gigabytes of upstream traffic per second. This enables botmasters to start targeted sabotage attacks against websites.

Harvested Data

Many botnets have functionality for automatically harvesting sensitive data like: email addresses, product serial numbers stored, credentials and information enabling financial fraud and classified documents or general information and internal business data from victim machines and submitting it to drop zones.

Brute Force Attacks

Cybercriminals can scan a range of IP addresses to find a specific port, and then bombard the service —FTP, Telnet, RDP (Remote Desktop Protocol) or other—

[51] https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defense

with rapid-fire authentication credentials from a list they've developed or bought in the underground.

Malware Distribution

Botnets are very successful at spreading additional malware. Most utilize backdoor capabilities and methods to download and execute files over HTTP, FTP (File Transfer Protocol) and TFTP, allowing a malicious actor to spread a computer worm, for example, simply by finding a single vulnerable host.

Warez, Illegal Downloads, and Cryptocurrency Mining

Hackers can control thousands of computers via botnets solely to use their combined bandwidth and disk space, often to host software and multimedia files such as illegally obtained movies or music or, to use a term coined in the underground, "warez." Botmasters infect a large number of PCs with Bitcoin-mining malware and create a "farm" of harvesters to continually collect Bitcoins without the infected user ever knowing about it.

Manipulation of Online Polls

Because every bot within a botnet army has its own distinct IP address, it's very easy to leverage botnets to manipulate the online polls or surveys that have become so popular over the last few years. Because each bot can mimic a unique user, it will appear that every vote cast by an infected user came from a legitimate voter.

In the years to come, in the area of botnets, we will most likely see the rise of the IoT botnets, or "Thingbots".

There are a number of critical reasons attackers target IoT devices.

- Embedded devices are easily exploited (e.g., default credentials, exposed services)
- Always-on devices with 24/7/365 availability and explosive marketplace growth
- Off-the-shelf products with low security standards
- Malware can easily change default passwords, preventing a user from logging in or other attackers taking control
- Devices are rarely monitored and poorly maintained, allowing hackers to easily shut down or enslave large numbers of IoT devices
- Low cost of entry for attackers as control of thousands of devices can occur for nearly zero cost (i.e., different than the high cost of accessing and controlling servers for more traditional DDoS attacks)[52].

3.6.3 Impact & Context

A botnet is created and used for malicious gain in the following way:

[52] https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/

1. A hacker purchases or builds a Trojan and/or exploit kit and uses it to start infecting users' computers, whose payload is a malicious application—the bot.
2. The bot on the infected PC logs into a particular command-and-control (C&C) server. (This allows the bot master to keep logs of how many bots are active and online.)
3. The bot master may then use the bots e.g. to gather keystrokes or use form grabbing to steal online credentials and may rent out the botnet as DDoS and/or spam as a service or sell the credentials online for a profit.

Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. Generally, the more vulnerabilities a bot can scan and propagate through, the more valuable it becomes to a botnet controller community.

Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment.

The most important part of a botnet is the so-called command-and-control infrastructure (C&C). This infrastructure consists of the bots and a control entity that can be either centralised or decentralised (distributed).
The centralised approach is comparable to the classic client-server network model.

Decentralised (peer-to-peer) C&C models, which are newer, often require the bots to act at least partially autonomously. The bots maintain connectivity to other bots and issue requests for new commands to the botnet. Because there is no single set of command servers that can serve as a single point of failure, and the botmaster can hide inside the network of bots when giving commands, this approach is harder to mitigate. Botnets are mainly used as a tool to perform other criminal or malevolent actions. A compromised computer or device is no longer under the legitimate user’s control, and sensitive data may be harvested by attackers. Botmasters have developed techniques that make their network of infected computers more resilient to takedown and also to evade detection by cyber security solutions.

Today it is getting easier for hackers to take over scores of internet of things (IoT) devices. All they have to do is purchase a botnet kit from the dark web and they are in business. The top three botnet kits — Andromeda, Gamarue and Wauchos — are estimated to be responsible for compromising more than a million devices a month. The Reaper botnet has infected more than 1M devices. It takes time to build, secure, and set up the command infrastructure for a botnet at a Reaper-like scale. A hacker would not likely invest that kind of effort without expecting a large return[53].
Mirai and Gafgyt have been tied to DDoS attacks against gaming servers and the botnet owner’s perceived rivals. Operators attempt to drive traffic to the gaming servers they control. According to ‘Krebs on Security’, a large, successful Minecraft server with more than a

[53] https://www.csoonline.com/article/3242866/security/our-top-7-cyber-security-predictions-for-2018.html

thousand players logging on each day can easily earn the server's owners more than $50,000 per month[54].
Botnet networks that fuel malware, spam, and cybercrime are expensive to maintain, but the rewards can top $20M a month according to Quartz Index. Despite the risks, returns are huge: Botnets running DDoS attacks and ad-spam easily generate thousands of dollars monthly. Bank fraud and click fraud can yield several million[55].
Radware's Threat Research has recently discovered a new botnet, dubbed DarkSky. DarkSky features several evasion mechanisms, a malware downloader and a variety of network- and application-layer DDoS attack vectors. This bot is now available for sale for less than $20 over the Darknet. Radware suspects the bot spreads via traditional means of infection such as exploit kits, spear phishing and spam emails[56].

An unusual botnet dubbed Mylobot has emerged, percolating up from the Dark Web – and displaying a never-before-seen level of complexity in terms of the sheer breadth of its various tools, especially evasion techniques. In terms of function, Mylobot can be used to download whatever payload its bot herders choose, whether that's cryptomining, ransomware, banking trojans, spyware or others. It could also be used for DDoS attacks. In the examined campaign, it was downloading the DorkBot backdoor. The current delivery method of the malware is unknown. "The main functionality of the botnet enables an attacker to take complete control of the user's system – it behaves as a gate to download additional payloads from the command-and-control servers," Nipravsky, a security researcher for Deep Instinct, said.

Interestingly, Mylobot also hunts for other malware on target machines, and disables anything it comes across. "The Dark Web plays a critical part in the spread of malware: Its rather simple accessibility of services and knowledge has made it easy for any attacker to gain much more abilities in minimum effort," explained Nipravsky. "By using the Dark Web, anyone today can access an online market and purchase a malware. An attacker can purchase access to exploit kits, buy traffic of tens of thousands of users to a web page, or even buy a full ransomware-as-a-service for his own use"[57].

Insikt Group assesses that a Mirai botnet variant, possibly linked to the IoTroop or Reaper botnet, was utilised in attacks on at least one company, and probably more, in the financial sector in late January 2018. This assessment is based on third-party metadata and existing open source intelligence. IoTroop is a powerful IoT botnet primarily comprised of compromised home routers, TVs, DVRs, and IP cameras exploiting vulnerabilities in products from major vendors including MikroTik, Ubiquity, and GoAhead. This is the first time we have observed an IoT botnet being used in a DDoS since Mirai, and it may be the first time IoTroop has been used to target victims since it was initially identified last year[58].

[54] CenturyLink 2018 Threat Report
http://www.centurylink.com/business/enterprise/blog/thinkgig/centurylink-2018-threat-report-meet-cybersecuritys-heroes-villains/

[55] https://qz.com/index/1282169/botnet-fraud-is-an-expensive-risk-but-its-worth-20-million-a-month-for-hackers-and-cybercriminals

[56] Radware, Cybersecurity Threat Alert – Darksky Botnet
https://security.radware.com/malware/darksky-botnet/

[57] https://threatpost.com/mylobot-botnet-emerges-with-rare-level-of-complexity/132967/

[58] Recorded Future, Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018
https://www.recordedfuture.com/mirai-botnet-iot/

According to Kaspersky Security Bulletin attacks via the underlying blockchain technologies on the financial systems in 2018 will be on the rise "Almost all of the world's large financial organisations are actively investing in systems based on blockchain technology. Any new technology has its advantages, but also a number of new risks. Financial systems based on blockchain do not exist autonomously, therefore vulnerabilities and errors in blockchain implementation can enable attackers to earn money and disrupt the work of a financial institution. For instance, in 2016-2017, a number of vulnerabilities and errors were discovered in smart contracts, on which a number of financial institution's services have been built"[59].

During a presentation at BSides Tel Aviv, security researcher Omer Zohar demonstrated proof-of-concept code for a fully functional command-and-control infrastructure built on top of the Ethereum network. Zohar was exploring the scope for potential misuse of blockchain technology in a bid to keep one step ahead of hackers and develop potential mitigation strategies.

The distributed ledger technology might be abused to create a decentralised and distributed infrastructure for the ultimate zombie network (botnet) C&C.

Secure communications, high availability, authentication and anonymity functions that a botnet operator might want are all handled by blockchain technology, thus blockchain-based command infrastructures would also be takeover and takedown resistant[60].

In 2017, according to "ENISA Threat Landscape Report 2017" the following notable statistics are worth mentioning:

- In the first quarter of 2017 a 69.2% increase of malware usage was revealed in comparison with the previous quarter. Malware tools like Ursnif, DELoader and Zeus Panda were used to leverage phishing emails and transform the targets into zombies – botnets members.
- Necurs, one of the most active botnets in 2017 has more than 1.5 million infected computers under its control.
- The Reaper IoT botnet infected a million networks and has been assessed as a serious threat to the whole internet.
- Regarding Reaper, some statistic were done about its activity. So, it was estimated that over 2 million of vulnerable devices are waiting to be infected only in one Command & Control server queue. Also, it was estimated that around 10 thousands of active bots are controlled daily by one Command & Control server.
- As of 27 November 2017, the world's worst botnet infected countries are: China, India, Russia Federation, Brazil, Vietnam, Argentina, Islamic Republic of Iran, Thailand, United States, Indonesia.
- The top four largest botnets to date are: 1 – BREDOLAB, 2 – MARIPOSA, 3 – CONFICKER, 4 – MARINA BOTNET.

[59] https://securelist.com/cybercriminals-vs-financial-institutions/83370/

[60] http://www.theregister.co.uk/2018/06/20/blockchain_bitcoin/

Notable Iot Botnets

Recently, a number of vigilante hackers have attempted to secure or lockout other bot herders from IoT devices via their own malware. One of the original examples of this was a botnet named Linus.Wifatch, but recently two new vigilante botnets have been discovered. In 2017, Radware's research team monitored thousands of attempts from Hajime, an alleged vigilante botnet, when it discovered BrickerBot.

Linux.Wifatch

A group called White Team released a piece of malware in 2014 known as Linux.Wifatch. Designed to infect routers to prevent them from being infected by other IoT botnets, Wifatch is a peer-to-peer botnet that stayed updated of evolving threats so it could attempt to mitigate them as well. It infects devices via Telnet by leveraging default credentials, closes the Telnet session and instructs the owner to login and change their Telnet password and update the firmware.

Hajime

Hajime is a sophisticated, flexible and future-proof IoT botnet. It is capable of updating itself and provides the ability to extend its member bots with 'richer' functionality efficiently and fast. The author behind Hajime is another suspected vigilante hacker attempting to secure IoT devices. This is a peer-to-peer botnet that has infected over 300,000 devices to date. Hajime targets devices via Telnet and gains access by brute-forcing default credentials. Hajime was released prior to Mirai but targets devices like, DVRs and CCTVs.

BrickerBot

Earlier this year, Radware identified a new botnet named BrickerBot. BrickerBot uses a network of globally-distributed devices that passively detect exploit attempts from devices infected with IoT bots such as Mirai. BrickerBot reacts to an exploit attempt by scanning the source of the exploit for a set number of ports in an attempt to secure the device. If it is unable to, BrickerBot launches a permanent denial-of-service (PDoS) attack that attempts to brick the infected device by leveraging 90-brick sequences via a Telnet session. As long as an IoT device does not become infected by malware, there should be no reason to fear BrickerBot.

Notable Botnets

According to the Inside Story on botnets of the "Managed Security Services Report"[61] (IBM) the following are the most notable botnets:

The Zeus Trojan

Zeus, also known as Zbot, is a Trojan horse malware kit that operates on several versions of Microsoft Windows. Its primary mission is to steal financial information using keystroke logging and HTTP form-grabbing techniques. Zeus is the type of malware that can execute remote commands on the machines it infects, and one of its operators has also been known to fetch additional malware from its C&C servers and install a ransomware package called CryptoLocker. This

[61] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03086USEN

botnet propagates the malware to new endpoints primarily via drive-by downloads and phishing tactics.

GameOver Zeus Botnet (GOZ)

This is a P2P botnet developed by the original author of the Zeus Trojan, using components of the earlier versions of Zeus with the added and highly resilient P2P communication protocol. Unlike its predecessor, this botnet relies on an encrypted peer-to-peer system for communication between the worker nodes and the C&C servers, reducing the potential for law enforcement takedowns. GameOver Zeus has been used primarily to commit banking fraud, and was also responsible for a distribution of CryptoLocker ransomware to thousands of unsuspecting users' endpoints that reportedly grossed cybercriminals more than USD 30 million within 100 days.

The Dridex Trojan

Dridex, also known as BUGAT, is a P2P-based botnet that contains a large variety of keylogging and data theft functions. Since its emergence in mid-2014, it has infected thousands of computers around the world. The main objective of the organised crime gang that operates Dridex is to steal and use the banking credentials for consumer, business and corporate bank accounts. Dridex has a two-phase infection mechanism. It typically spreads via spam email containing an attachment with a Microsoft Word vulnerability using poisoned macros, which in turn downloads and executes the Dridex loader. The loader fetches the actual payload from a remote server and then installs the botnet components on the victim's machine.

The Dyre Trojan

Like the previously noted botnets, the Dyre banking Trojan employs essentially the same elements of infection via malware spam tactics. Although Dyre emerged around mid-2014, the U.S Computer Emergency Response Team (CERT) first noted a Dyre campaign in October 2014. One of the more popular attack vectors Dyre employed was to target a vulnerable version of Adobe Reader with a weaponised PDF file. Once the exploitation succeeded, the victim machine would be instructed to download the Dyre banking malware.

Dyre was owned by a very prominent organised cybercrime group that targeted the online banking account credentials of consumers and businesses of all sizes and sent the information it harvested to malicious actors. Dyre also has the ability to perform man-in-the-middle attacks using a browser injection technique. It can steal security certificates and take browser snapshots to learn how users transfer money out of their bank accounts, and it can automate illicit transactions out of infected users' accounts.

Top notable attacks

According to "ENISA Threat Landscape Report 2017" the most notable attacks are the following:

- At the start of 2017 Twitter discovered that there were over 350.000 fake accounts which all were part of one botnet. More, other accounts which were part of smaller bot networks were found, bringing the total of fake accounts to over half a million.

- After three months of inactivity at the beginning of this year, Necurs reappeared in March and resumed its activity with mass mailing spam campaigns spreading in most cases ransomware.
- In July 2017 an unnamed 29-year-old man pleaded guilty in a German court to charges related to Deutsche Telekom's routers which became infected with a modified version of the Mirai malware.
- In late 2016 and early 2017 a massive DDoS attack was performed using Leet Botnet, which reached 650 Gbps (Gigabit per second).

3.6.4 Suggested Controls and Mitigation

According to the ENISA report “Botnets: Detection, Measurement, Disinfection and Defense”[62], the mitigation techniques to the botnet threats are divided into the following two sections: technical methods and social and regulatory approaches.

Technical countermeasures

The countermeasures presented in this section apply at a technical level.

- *Blacklisting*
  Blacklisting itself is not a direct countermeasure against botnets. Instead, it should be perceived as a supporting process which provides input for further technical means of resistance.

- *Sinkholing*
  Sinkholing is a technique that is used to redirect the identification of the malicious Command and Control (C&C) server to one that is controlled by an investigator for analysis. This way, the malicious traffic that comes from each client goes straight to the investigator’s one ready to be analysed.

- *Orchestration of controls at host and network level*[63]

- *Vulnerability management in combination with regular updates*
  The effort to keep software up-to-date to remove known vulnerabilities.

- *Distribution of fake/traceable credentials*
  The distribution of fake credentials is not only a purely technical countermeasure but also targets the botnet‘s profitability by attacking the underlying business model. A common botnet application is identity theft. Profit is created by stealing credentials or credit card records.

- *DNS-based countermeasures*
  Depending on the type of botnet, many malware samples use fixed domain names as identifiers for their underlying C&C infrastructure, which is contacted by compromised hosts. If a domain name like this can be found to

[62] https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

[63] https://www.shadowserver.org/wiki/pmwiki.php/Information/BotnetDetection

be related to malware, and it has been established that it is used for malicious purposes only, the domain should be shut down by the responsible registrar.

- *Direct takedown of command-and-control server*
  The mitigation technique known as direct takedown or decapitation aims at eliminating the instances of command-and-control servers with which bots are remotely controlled. In order to perform a takedown, a centralised botnet architecture, as often used in IRC- and HTTP-based botnets, is required.

- *Packet filtering on network and application level*
  It extends the idea of transparent monitoring and detecting to the actual application of further actions, if suspicious activities are recognised. A typical component that performs packet filtering at host level is a desktop firewall, and if the technique is applied at the network level, packet filtering is usually performed by a firewall. An intrusion detection system can be enhanced to automatically take actions, thus promoting the IDS to an intrusion-prevention system. Packet filtering may also be applied at ISP level.

- *Walled gardens*
  The concept of a “walled garden” has the goal of protecting an ISP‘s customers and other Internet users from further damage, by intercepting and isolating outgoing connections from a detected infected host. According to “Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks, Mody, N., O‘Riordan, M., Masiello, S, Zebek, J. M3AAWG”, the procedure can be divided into three stages: detection, notification and remediation. The general idea of a walled garden is to forbid almost all connection attempts by the isolated user, except those to a defined whitelist of malware mitigation services.

- *Peer-to-peer countermeasures*
  Every peer-to-peer based network has to handle information management to do with connectivity and routing. New peers have to be advertised within the network and the information about different peers has to be publicised in the network. Countermeasures aimed at peer-to-peer based botnets exploit this concept of peer-lists and their publication mechanisms (e.g. Sybil Attack).

- *Quarantine Infected Computers*
  The idea is that infected computers spreading malware or being part of a botnet are a risk to the greater community and thus need to be isolated. Detect infected systems and isolate them from the internet, so place them in a quarantine. Internet service providers would administer the quarantine, and can help to clean up the systems. Once cleaned the systems can re-join the greater Internet.

- *Infiltration and remote disinfection*
  Infiltration, in the context of botnets, describes the process of finding a way to impersonate the botherder and obtain control over the infected hosts. As almost all botnet families exhibit differences in their implementation and mode of operation, an infiltration can be considered as a tailored approach for each targeted botnet. The main goal is to spot weaknesses in the botnet’s

communication protocol, which may serve as attack vectors on which the actual infiltration can be constructed.

Regulatory and social countermeasures

These approaches rely less on technical measures but aim at improving the environment needed for botnet countermeasures. This includes end users who are affected by the impact of botnets and how to improve the coordination and courses of action in handling the botnet challenge from an international point of view. Such approaches are the following:

- Dedicated laws on cybercrime
- User awareness raising and special training
- Central incident help desk
- Enhance cooperation between stakeholders.

Since 2010 there have been several highly profiled takedowns of botnets through coordinated efforts, and this continues. In December 2015 law enforcement and Microsoft disrupted Dorkbot, a botnet which had infected more than 1 million computers the previous year. In December 2016, Europol[64] reported that they cooperated on the takedown of the Avalanche network. It has caused an estimated EUR 6 million in damages in concentrated cyberattacks on online banking systems in Germany alone. In addition, the monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the high number of malware families managed through the platform. The operation marked the largest-ever use of sinkholing to combat botnet infrastructures and is unprecedented in its scale, with over 800,000 domains seized, sinkholed or blocked. In April 2017 Kelihos/Waledac botnet, involved in stealing banking credentials, spamming, DDoS attacks and spreading malware, has also been disrupted by US law enforcement.

The good news is that efforts against botnets are improving. In December 2017, three people pleaded guilty to charges related to their creating and using the Mirai botnet to launch a DDoS attack on DNS service company Dyn. Also in December 2017, ESET and Microsoft announced that they had cooperated to take down 464 botnets and more than 1,200 command and control domains. Also encouraging, an individual believed to be associated with the botnets was arrested in Belarus.

International cooperation will be necessary to stop botnets. In spring 2017, the Belarus arrest along with the arrest of Peter Levashov, the hacker behind the Waledac and Kelihos spam botnets in Spain gave hope that hackers will have fewer safe havens next year[65].

[64] https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

[65] https://www.csoonline.com/article/3242866/security/our-top-7-cyber-security-predictions-for-2018.html

3.6.5 Final Considerations

According to Spamhaus Botnet Threat Report 2018 “There is no sign that the number of cyber threats in 2018 will decrease. The big increase of IoT threats in 2017 is very likely to continue in 2018. We are sure that securing and protecting IoT devices will be a core topic in 2018”.

With Gartner predicting a world filled with more than 20 billion IoT devices by 2020, we’re becoming more connected by the minute. All of these devices and sensors will improve and enhance many aspects of life, but they also present risks when the devices are infiltrated by hackers.

Many IoT devices are built without even a minimum of security controls, so they’re exposed and vulnerable from the outset. There’s also a lack of standards throughout devices, which prevents enforcing uniformity in security settings and establishing universal security parameters. Poor patch management is another area of concern, as many IoT device manufacturers require end users to update devices and obtain the latest patches.

To combat the challenges with IoT, companies should perform risks assessments to fully understand where they might be exposed and how they can remedy those risks. They need a log of every connected device in their network along with a way to automate patching and updating.

Corporate IT must consider the security needs of provisioning and authenticating IoT devices throughout the company. This includes accounting for the role and location of all of these devices, along with details on updates and patches. The actual data sent between the devices and the network must also be protected. Many companies rely on IoT-derived data to make impactful decisions, so the integrity and security of the data is supremely important. Considerations should include how the data is protected at rest and in transit, and if tools such as encryption should be used to render stolen IoT data unusable[66].

As the IoT botnet attack marketplace continues to grow, and the number of IoT devices continue to proliferate, so will the number of vendors adapting to the changes in their environment. This growth in competition will result in more IoT devices being targeted for profit. Financial gain is the main motivation behind the evolution, driving the growth of the attack marketplace and IoT botnets. The result? Botnets have been involved in nearly every major recent DDoS attack, resulting in service degradation, compromised data, lost revenue and tarnished brands for organisations globally. As the botnet landscape expands and more destructive threats become inevitable, it’s critical to understand these bot-based assaults and move beyond legacy security solutions[67].

[66] TechTarget/IoT Agenda

[67] https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/

3.7 Cloud Services and Big Data

3.7.1 Definitions

Cloud Services are resources provided over the Internet. These services are made available to users on demand via the Internet from cloud computing provider servers as opposed to being provided by a company's on-premises servers. Cloud computing, also known as on-demand computing, is a kind of Internet-based computing, where shared resources and information are provided to companies and end-users on-demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centres. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network.[68]

The most common cloud service resources are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

There are several types of deployment models for cloud services. Private cloud is cloud infrastructure operated uniquely for a single organisation, whether managed internally or by a third-party and hosted either internally or externally. A public cloud is an infrastructure performed over a network that is open for public use by cloud service providers. A hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models.

Big Data is a broad term for data sets (both structured and unstructured) that is so large or complex that traditional database techniques and data processing applications are inadequate. Challenges include analysis, capture, data curation, search, sharing, storage, transfer, visualisation, and information privacy. The term often refers directly to the use of predictive analytics or other particular advanced methods to extract value from data.[69]

3.7.2 Fraud Description

The mainstream of cloud computing seen as IaaS, PaaS and SaaS (Software as Service) technologies have enabled companies to obtain flexibility and scalability of services, reduction of costs and time to market. These have been the main drivers to move legacy and new banking applications to cloud computing services. As organisations continue to migrate on-premises services and applications to the cloud, it is reasonable to deduce that they will also suffer the same fraud threats and risk, with the addition of new ones. The latter being because of the delegation of software and hardware to a third party, the cloud provider. Despite the fact that the cloud provider customer might have some control over their services and applications, such as the authentication mechanisms, there are still inherent risks with the cloud service providers that can produce fraud scenarios. Weak code and software vulnerabilities in the cloud, outside the traditional perimeter of control, may produce different types of breaches and fraud. Some cloud scenarios such as SaaS may imply delegating the authentication and encryption to APIs controlled by the SaaS provider, which may increase the risk factor of possible data leakage. The same might happen if using PaaS when constructing native applications in

[68] https://en.wikipedia.org/wiki/Cloud_computing

[69] https://en.wikipedia.org/wiki/Big_data

the cloud. It is vital that private keys and sensitive data are always under control and not delegated to the cloud service provider or a third party.

3.7.3 Impact & Context

Taking core and non-core applications to the cloud can be challenging if the appropriate measures, controls and risk-based policies are not set correctly. The same old fraud scenarios may occur under cloud computing, and some of the most common scenarios where an impact on fraud in the coming years could potentially be seen are the following:

- The typical vulnerabilities that lead to intrusion via any layer surrounding the application in the cloud. A software application not properly patched 24x7 can be infected in the same way as it may occur in a PSP's data centre. As a consequence, there will be an increase in the risk of data breaches where the cyber criminals could potentially see greater value in stealing information from cloud-based applications.
- A Denial-of-Service will not go undetected by the cloud service provider that would probably proceed to shut the access to the active cloud service automatically. This type of attack could be used as a distraction to overload CERTs who could be busy in the resilience recovery while an undercover fraud scheme could be in progress.
- An insider from a company or the cloud provider could potentially access the PSP's application or the configuration surrounding it, gaining access to information and algorithms used or injecting malicious code or malware.
- Privacy related issues such as attacks to steal profiling data related to customer data analytics.
- Social engineering is another attack vector that could potentially increase with the cloud support provider service who might have weak customer authentication and verification processes.
- Phishing campaigns and botnets using the cloud service provider's infrastructure might become more common.
- A potential increase in the risk of using payment credentials stored in cloud service provider's infrastructure, being IaaS, PaaS or SaaS.
- Manipulation of big data analytics and algorithms if not adequately monitored.
- The unauthorised access to cloud computer resources could lead to execution of crypto mining software.

3.7.4 Suggested Controls and Mitigation

Cloud governance including a risk-based analysis approach, based on international standards such as NIST, ISO 2700x, COBIT or PCI-DSS as well as continuous monitoring of the implemented controls using recognised international audits such as SSAE 16, are first steps to mitigating or reducing the previous fraud risks. It is paramount to have a clear set of policies and cloud governance throughout the whole lifecycle of applications and services.

This lifecycle should include a risk analysis phase to determine the type of risks of each initiative. Some primary risks that need to be detected and scored are technological maturity, change impact in the operational and technical environment, functional maturity, technical complexity in the organisation, compliance with the internal and external regulations as well as with the security patterns, classification of the information, analysis scoring of possible fraud schemes, resilience strategy and risk of being hacked.

The risk analysis scoring should be used to prioritise the decision to start or not the security evaluation and the continuation of the cloud-based initiative. The security evaluation is the process of creating a detailed security report that explains the architecture, communications, data, authentication, authorisation, prevention, monitoring, incident reporting, compliance and active risks necessary to comply with the security regulations.

Of equal importance is the regular execution of a security audit to verify the cloud provider's conformity to the security requirements set not only prior to production deployment but through the whole lifecycle of the application, including any change to its environment.

The architecture, applications, process, systems and data in the cloud need to be desegregated from each other to avoid propagation of malware or breach attacks. Contingency planning and rehearsal via cyber exercises should be part of the ongoing risk review, including ethical hacking on the systems to test the confidentiality, integrity and availability.

The risk-based approach and governance of fraud and security should be thoroughly controlled throughout the whole value chain taking special care in delimiting it via appropriate contracts with the necessary SLAs and liabilities for all providers involved.

Data privacy and control as well as compliance with regulatory framework are the most critical challenges to achieve when moving to the cloud. PSPs must always have the control over their data, security included. For example, when encryption is used for data privacy, PSPs must have control over the key management and not the cloud provider. Compliance with security and privacy regulations such as the protection of sensitive or personal customer data related to payments should always be taken into practice. Also, where technically possible, the authentication mechanism should always be controlled by the company and not by the cloud provider. Also, the possibility to control the "on" and "off" switch to security mechanisms in case of emergency by the company's Computer Emergency Response Team is key.

Usage of new tools and applications for cloud computing and big data need to be analysed and assessed from the point of view of security, risk and governance, as some tools might not be sufficiently mature to use and could potentially cause data breaches and fraud. Therefore, a thorough analysis from the security and fraud perspective is needed before making any usage or buy decision.

Before use of a cloud service, a PSP must identify (data, applications, infrastructure) and evaluate the assets (criticality, classification) and define the appropriate security controls. Then they should choose an appropriate cloud deployment model and define whether and how the data can move in and out of the cloud. Finally, there should be a due-diligence process to evaluate the service provider regarding security, privacy, availability and their SLA. Common and international recognised certifications and audits should be considered as part of this due-diligence. Some organisations are currently requesting to service providers the usage of standards, best practices and controls such as the PCI DSS Cloud Computing Guidelines, NIST, ISO 27001, COBIT, SSAE 16 or the framework of the Cloud Security Alliance (SCA).

Lastly, it is important to consider that new technologies such as cloud computing require the skills of legal, privacy and security, and it is therefore an important need from public and private institutions to seek or train employees with these new skills to avoid worst case scenarios due to lack of knowledge or skills.

3.7.5 Final Considerations/Conclusions

Cloud computing and big data analytics are already mainstream, and some PSPs are commencing to move both non-core and core applications to cloud providers. Obviously this will result in a reduction of IT costs, complexity and time to market for those PSPs. However, necessary steps need to be taken to mitigate the risks under cloud computing as lack of the appropriate security controls and governance could easily lead to fraud. Besides traditional security best practices, care should also be taken in complying with regulations such as data privacy and security. Having a strict cloud governance control over the whole lifecycle of the applications running and data processed or stored by a cloud provider is vital. For this reason, applying DevSec, a variant of DevOps[70] for security, to automatize lifecycle operations and harden solutions uploaded into CSP or any outsource provider should be implemented into the IT culture. Moreover, particular emphasis should be put on achieving the control of the security mechanisms in the cloud services, contractual clauses that ensure the necessary security checks, fulfil the compliance obligations (e.g. data privacy, exit clause, right to audit) and share liabilities between both parties. Finally, international standards such as NIST, ISO 27001, SSAE 16 and COBIT should be carefully considered and applied on these new technologies, as well as internationally recognised frameworks such as the one developed by the CSA. Moreover, new standardisation and guidelines developments on cloud computing services[71] need to be monitored and applied as they become available.

3.8 Internet of Things (IoT)

3.8.1 Definition

The Internet of Things (IoT) is the network of physical objects ("things") embedded with software, sensors, computing elements and network connectivity, which enables these objects to be interconnected and send, receive and process data. It refers to a hyper-connected world where a continuously growing number of devices (“things”), used by consumers and enterprises, are connected and communicate with each other, mainly through the Internet. IoT has evolved due to the extensive use of the mobility and the convergence of wireless technologies, the micro-electromechanical systems and the Internet.

In this document only the usage of IoT in the context of payments is considered.

[70] https://en.wikipedia.org/wiki/DevOps

[71] see for instance:

https://www.dnb.nl/en/news/dnb-publications/archive/newsletters/nieuwsbrief-banken/nieuwsbrief-banken-augustus-2013/dnb295744.jsp

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.html

https://www.ssi.gouv.fr/actualite/secnumcloud-la-nouvelle-reference-pour-les-prestataires-dinformatique-en-nuage-de-confiance/

3.8.2 Fraud Description

Like traditional computers and networks, IoT devices pose at least similar risks, for example in transaction processing or in the device (IoT) hardening needed for Internet banking. Because IoT devices are connected to the Internet, they represent new targets for data exposure and attacks. They can be infected by a malware and be compromised by fraudsters or their communications could be intercepted (unauthorised access and use of the device, misuse and disclosure of personal information). But due to the nature and the different types of the IoT devices (different hardware, firmware and operating system), the risks and the type of attacks may differ from those of the traditional computing devices. Today, with a smart TV, which is connected to the Internet and has built-in capabilities and applications, a consumer could perform payments. The same exists for point of sales or other similar devices which support contactless technologies (NFC). Wearable objects are another example. All these IoT devices change the traditional means of payment (they actually expand the scope of use of these means) but it is more complex to enforce security upon them. For example, how easy is it to notify and apply a security update or hotfix to mitigate a critical vulnerability in a smart TV? On the other hand, many enterprises do not take seriously the security of an IoT device, as they do for the traditional computing devices. They do not even lock down the devices in order to be secure against typical attacks, because they do not realise that these new devices pose similar risks and are targets for attacks too. The lack of usage and incentive of common standards in security such as encryption in IoT devices or the continuous usage of factory default password that are never changed make them more attractive for attacks, and we are increasingly seeing new forms of extortions, botnets hacks, data theft and even physical harm. The use of new technologies which could potentially serve as a new framework to facilitate processing of transactions or coordination of IoT could increase fraud if not properly secured.

3.8.3 Impact & Context

Research shows that up to the year 2020 there will be about 4 billion connected people and more than 25 billion connected devices and intelligent systems (including more than 250 million vehicles), using more than 25 million apps. The risks described above will increase and the impacts too. Imagine the huge amount of data exchanged and stored onto these devices and how vulnerable these could be. Unauthorised access and use of the IoT devices, fraudulent transactions as well as data leakage, botnets and privacy incidents will increase if no countermeasures be taken. Both consumers and enterprises will face new types of attacks, depending on the types of the IoT devices. These devices will be hard to be controlled if an adequate security level is not designed from the beginning and maintained through their lifetime.

3.8.4 Suggested Controls and Mitigation

Before integrating the use of IoT services into the business process, whether this includes a new type of device, a new network communication channel or a new interconnected payment application, specific controls must be considered to mitigate the respective risks:

- Perform a security risk assessment for every new device and infrastructure being a part of the IoT for the organisation. Identify and evaluate the risks associated with a device, an application or a network connection and implement multiple levels of defence mechanisms.

- Adopt security and privacy by design: security for the devices, infrastructures, software and data must be adopted from the beginning and follow each phase of the project.
- Implement strong authentication and authorisation controls in every communication and exchange of data. Ensure the identity of the interconnected devices, sign and certify, where applicable, the associated applications.
- Monitor all service providers involved for security and privacy compliance.
- Device to device communication must be always secure (e.g. use of encryption, devices identification, change default factory user and passwords, etc).
- Minimise the amount and type of data exchanged, processed and stored. Secure the data storage of the devices adequately.
- Perform security audits before they go live. Identify vulnerabilities and take mitigation actions. Monitor the security status and periodically evaluate the security level.

3.8.5 Final Considerations/Conclusions

Enterprises across the world try to find new ways of doing business and IoT provides new opportunities. Since these “things” don’t look like traditional computers, they aren’t treated like computers. As a result, enterprises are often not taking adequate measures to ensure that they have an acceptable security level. The October 2016 DDOS attacks provoking a massive attack on Twitter, Spotify and Google due to a botnet partially created out of CCTV, routers, intelligent bulbs and other IoT is revealing that this type of malware is here to stay and is due to create new frauds related to IoT and payments or ransomware attacks on IoT such as heaters, air conditioning, door locks or intelligent refrigerators.

Internet of Things contains and expands, due to the different types of devices and ways of communication, the well-known risks of the mobility and the interconnection of traditional infrastructures, applications and services. So, it should be treated and evaluated like any other consumer-facing or internal business service. So far, not many of those IoT devices are used for performing payments or the use for payments is limited, but the number and the types of IoT devices (and the capabilities of them) are increasing rapidly (e.g. make a payment transaction from an interconnected car), so that the services offered will be extended more and more to cover the payment sector, increasing the risks for both consumers and enterprises.

3.9 Virtual currencies

3.9.1 Introduction

Virtual currencies, defined by the European Banking Authority (EBA) as “a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat currency, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically”[72] or as defined by the ECB as “a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific

[72] https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

virtual community"[73], are not new. From in-game digital coins to loyalty programs such as air miles, they have been present in our society since the 1990s. However, all virtual currencies until 2009 were centralised as there was always a third party validating transactions and controlling users' balances. Consequently, they were relatively easy to take down once it was established they facilitated criminal activity.

Over the last few years, popularity of virtual currencies has skyrocketed, due to the surge of decentralised digital currencies, like Bitcoin, the first to appear in 2009 and still the most important of them. Decentralisation means that one person can pay directly to another without using a third party as an intermediary, something that before was only possible using cash. It is for this reason that decentralised digital currencies are commonly considered "digital cash".

In Bitcoin-like schemes, trust is provided by a mix of technologies that include primarily cryptography, instead of being provided by a trusted third party. Therefore, these kinds of decentralised currencies are also referred to as cryptocurrencies.

This kind of global digital currency that allows for reliable, fast and irreversible online transactions, is not centrally controlled, has no built-in know-your-customer (KYC) mechanism, and is relatively difficult to trace. Therefore, they are a potential magnet for criminals. Indeed, its illicit use is increasingly happening as the criminals are gradually accepting it as a currency of choice for trade in the darknet and various extortion or fraudulent schemes. Lately new trends have been seen on users who are beginning to use virtual currencies to trade or for currency exchange due to the low commission benefits provided by some of them.

There are a large number of web pages dedicated to the trade and management of this new type of currency. Following the birth of Bitcoin, the first cryptocurrency, many more blockchain based technologies have emerged, some of them issuing tokens that act as currency, competing in the currency market, for example Dash, Ethereum, Litecoin, Monero, Ripple, Veritaseum or Zcash. In 2018, thousands of cryptocurrencies exist, tens of them with a market capitalisation of more that 100 million euros[74].

However, most types of cryptocurrencies, including Bitcoin, are not completely anonymous. Although the Bitcoin blockchain itself does not identify the parties involved in a transaction, suspects of using it in illicit activities can be traced by using a combination of open source research, commercial tools and information provided by the private sector, so there are solutions that can be put in place to avoid or at least diminish fraudulent transactions.

3.9.2 Types of Fraud

Presently different types of fraud patterns are arising. There are modus operandi where Bitcoin and other digital currencies are involved. Some fraud scenarios are described next.

Anonymity exploitation via crypto currency transactions

Although all crypto currency transactions are stored publicly and permanently on the network by means of blockchain technology, the identity of a user behind an address can remain unknown allowing the fraudsters to move and cash-out the stolen funds

[73] https://en.wikipedia.org/wiki/Virtual_currency

[74] Cryptocurrency market capitalisation is available at https://coinmarketcap.com/

anonymously. As such it is used as a vehicle for criminal activities such as money laundering, buying illicit goods, extortion[75]...

[75] https://www.europol.europa.eu/newsroom/news/two-criminal-groups-dismantled-for-laundering-eur-25-million-through-smurfing-and-cryptocurrencies

Attacks to large crypto currency exchange traders

2018[76] has seen an increase in crypto currency exchange traders suffering data breaches were customer accounts and assets have been stolen, massively compromised and as a consequence Bitcoin funds retrieved from those accounts. The increase of the market capitalisation of crypto currencies has increased the motivation for individuals performing attacks to the crypto currency exchange traders.

These frauds to the traders were a consequence of security vulnerabilities and the lack of risk mitigation countermeasures from the company. And as a Reuters report[77] shows there is a tendency that these types of hacks are going to continue to occur in the future. As explained by this report, "this rising risk for Bitcoin holders is compounded by the fact there is no depositor's insurance to absorb the loss, even though many exchanges act like virtual banks. Not only does that approach cast the cyber security risk in stark relief, but it also exposes the fact that Bitcoin investors have little choice but to do business with under-capitalised exchanges that may not have the capital buffer to absorb these losses the way a traditional and regulated bank or exchange would."

We could conclude that these traders are holding customer Cryptocurrency wallets in a centralised infrastructure in a similar way as banks with deposit accounts, and the issue arises when Cryptocurrency customers claim the stolen funds to the trading company realising the low probability to recover the Cryptocurrency mainly because the company probably will fail after the cyberattack.

Bitcoin Wallet compromise

The increase of interest showed by fraudsters in Cryptocurrency held by individuals is boosting the number of stolen credentials to gain access to Virtual Currency wallets.

Cryptocurrency wallets typology are diverse like desktop wallets, mobile wallets, online wallets, hardware wallets or paper wallets[78]. Taking into account the great variety of wallets there is as a consequence an equal increase in many different attack vectors depending on wallet type to steal this wallet credentials, one of the latest trends seen is stealing the mobile phone number[79].

Many of the attack vectors and corresponding countermeasures run parallel to fraud patterns and prevention measures in non-digital currencies. Online wallets for example

[76] https://www.ccn.com/731-million-stolen-from-crypto-exchanges-in-2018-can-hacks-be-prevented/

https://www.coindesk.com/token-platform-bancor-goes-offline-following-security-breach/

https://news.bitcoin.com/hacked-korean-bitcoin-exchange-yapizon-offers-ious/

https://www.cryptocoinsnews.com/classic-ether-wallet-falls-victim-to-a-social-engineering-hacker/

http://fortune.com/2017/07/18/ethereum-coindash-ico-hack/

http://thehackernews.com/2017/07/ethereum-cryptocurrency-hacking.html

https://www.coindesk.com/veritaseum-founder-claims-8-million-ico-token-stolen/

[77] http://www.reuters.com/article/us-bitcoin-cyber-analysis-idUSKCN11411T

[78] https://www.ccn.com/myetherwallet-warns-of-another-hack-urges-hola-users-to-move-funds/

[79] https://mobile.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html?smid=pl-share&referer

can look like online banking platforms in terms of credentials provisioning, authentication and use of two factor authentication. In July 2017, we became aware of the second largest heist in the history of virtual currencies that exploited a critical flaw in the Parity multi-signature wallet on the Ethereum network, draining massive wallets of over $31,000,000 of Eth, the coin on Ethereum blockchain, in a matter of minutes, confirming us that the same old attack vector can occur with new disruptive technologies.

Crypto currency mining:

Diverse attack scenarios raised up during the end of 2017 and beginning of 2018 in order to obtain crypto currency mining with unauthorised use of resources. Crypto Mining software has appeared included at diverse websites and servers in an unauthorised manner, as it has been spread as malware, including IoT Devices[80].

3.9.3 Impact and context

The impact of these types of attacks targeting virtual currencies is limited due to the trusted systems created by governments and central banks. The limited use of virtual currencies coupled with the fact that they remain unregulated in most jurisdictions suggest that nowadays they only pose low risk to most payment service providers.

3.9.4 Suggested controls and mitigations

There are some recommendations that can help prevent such types of fraud as the Ponzi schemes. The United States' Securities and Exchange Commission suggests several red flags[81] to detect their characteristics. There are also some Bitcoin wallet security best practices that help to protect these wallets, although the same old security principles to mitigate security risk still apply.[82]

The links to this document highlight the importance to establish controls and mitigation plans under the daily cybersecurity plan based on risk management. Particular care should also be taken with respect to regulation -is the virtual currency regulated or not? Extra care should be taken if the financial entity is trading or interchanging money with third parties such as Bitcoin exchange traders, where some type of cyber insurance, if possible, should be taken into account in order to become more resilient in worst case scenarios.

[80] http://www.wired.co.uk/article/browsealoud-ico-texthelp-cryptomining-how-cryptomining-work

https://www.zdnet.com/article/cryptocurrency-mining-malware-why-it-is-such-a-menace-and-where-its-going-next/
https://www.alienvault.com/blogs/labs-research/massminer-malware-targeting-web-servers?utm_source=feedblitz&utm_medium=FeedBlitzRss&utm_campaign=alienvaultotx
https://www.helpnetsecurity.com/2018/05/03/crypto-mining-botnets/

[81] https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf

[82] https://www.cryptocoinsnews.com/bitcoin-wallet-security-best-practices/

3.9.5 Conclusions and final considerations

Virtual Currencies are here to stay, ICOs have raised more than 6,178 Millions USD during the first semester of 2018, compared to the 969 Millions in the same period of 2017.[83]

As seen from the previous recap of the different fraud modus operandi where Bitcoin or other virtual currencies are involved, it is important to highlight that these patterns do not imply that there is a lack of security along the Bitcoin and the underlying blockchain technology. In fact, security measures are embedded in this technology with no single point of failure, providing not only confidentiality, but also authentication to all Bitcoin transactional activity.

Up to now the general preventive measures in financial entities appear to be sufficient, as risks are currently low and the impact of this fraud has been very limited to financial institutions.

3.10 Multi-vector attacks

Multi-vector attacks exploit common weaknesses in the security chain - such as poorly configured servers, gullible staff, vulnerable applications or lack of multiple levels of defence - by combining elements like social engineering, spear phishing, contaminated USB drives and voice phishing with malicious attachments carrying code that exploits known or unknown vulnerabilities on the target system.

Oftentimes, multi-vector attacks are designed to avoid traditional defences like anti-virus software, intrusion detection systems and other endpoint protection programs, which makes them elusive, difficult to detect and hard to defeat. Combined with the constantly evolving threat landscape and the fact that the speed, frequency, and severity of attacks have accelerated, it has become evident that financial institutions must keep investing in new state of the art security technologies (Advanced Threat Protection), ensuring that their cyber defence frameworks provide adequate response and defence-in-depth for identifying, stopping and recovering from multi-vector attacks.

Recent examples of multi-vector attacks include cyberattacks using the SWIFT-related banking infrastructure, ATM infections, remote banking systems and POS terminal networks[84], making changes in banks' databases to 'play' with card balances, as well as the so-called supply-chain attacks, i.e. attacks on software vendors supplying financial organisations.[85]

[83] https://www.icodata.io/stats/2018

[84] See for example:
https://www.tripwire.com/state-of-security/security-data-protection/hackers-indian-bank-attack/

[85] https://securelist.com/cybercriminals-vs-financial-institutions/83370/

4 Payment fraud

4.1 Card related fraud

4.1.1 Definition

Payment Card Fraud is a wide-ranging term relating to the theft and crime committed using or involving a payment card or payment card details. The purpose may be to obtain goods or services to resell for cash or to obtain funds directly from a related bank account, usually to pay for the criminal's lifestyle or to fund more serious criminal activity.

4.1.2 Card Fraud Scenarios

There are several card fraud scenarios. In principal, the fraudster's modus operandi is to obtain the physical payment card and PIN for use in a face to face, Point of Sale (POS) environment, or to obtain payment card data for use in an ecommerce or card not present (CNP) environment, such as Internet shopping, mail order, phone ordering, etc. The following are typical card frauds:

- Lost / Stolen Card – a card can be stolen by several methods such as so-called pick-pocketing, after the thief observes the PIN code being entered by the genuine cardholder at an ATM or in a store at a POS terminal. A thief can also steal a card and without knowing the PIN use the contactless (NFC) facility on the card to obtain goods or cash under the card issuer's contactless transaction ceiling or counter limit.
- Account Take Over / Fraudulent Application – refers to the situation when a cardholder inadvertently gives personal information or allows personal data to be obtained, such as home address, ID card number, PIN code details, etc. to a fraudster. The fraudster contacts the cardholder's bank or financial institution and, using the genuine cardholder's details, dupes the bank into believing they have changed address and lost payment cards, which are replaced by the bank and sent to the fraudster's newly advised address.

  These frauds often occur in combination with social engineering fraud and Phishing.
- Card not received – Where a criminal will steal a payment card from an individual's mail box so the rightful owner never receives it. This is only effective when the card is active. It should be noted most card issuers issue inactive cards which can only be activated by the genuine cardholder.
- Skimming – where a device is installed into an ATM or POS terminal by a criminal in order to capture data from the magnetic stripe on a cardholder's payment card. The criminal manipulates the ATM or POS terminal or attaches a skimming device to the card reader of the ATM or POS terminal; usually a PIN compromise device such as a micro-camera or PIN pad overlay is installed at the same time.
- Shimming – like skimming, is where the aim of the fraudster is to skim or 'shim' data from the EMV Chip on a payment card rather than from the magnetic stripe, using similar methods.
- Payment Card Data Interception – This type of fraud occurs when stolen payment card details are fraudulently used to purchase goods via the Internet, over the telephone or by mail order (CNP Fraud).

4.1.3 Current and New Payment Card Fraud Trends

Social engineering

In a number of instances, credentials recovered through social engineering have been used to make transfers to money mule accounts. Subsequently, using their own cards, those pick up big sums at casinos and jewel / watch shops in other European countries.

Lost and stolen Card Fraud

Although lost and stolen card fraud can be detected easily and quickly by the genuine cardholder in most cases, the trend continues to grow and losses remain high. The impact of lost and stolen card fraud is still significant for consumers and for banks and financial institutions across Europe. Fraudsters consistently look at better and easier ways to capture PINs, e.g. using social engineering or shoulder surfing, then they steal the payment card using various methods.

Contactless payment cards are increasingly being accepted in stores. A lost or stolen card can be used for purchases as long as the cardholder authorisation is not required for a contactless transaction, but only up to a certain number of times and to a limited value. It is expected there will be an increase in the theft of cards for this purpose, i.e. to purchase goods that can be resold for cash.

Cardholders are generally good at reporting their cards lost or stolen to their financial institution once they realise the card is missing however some wait a period of time before reporting. This can be an issue as cards need to be blocked as soon as possible to reduce the overall fraud losses.

Account take over / Fraudulent application. Card not received.

Fraudsters are using social engineering techniques such as infiltrating cardholders' homes, approaching bank staff or other methods, such as spear phishing, to obtain the data needed to take over an account or create a false application / request for a payment card or PIN.

Counterfeit Cards

- Copying magnetic-stripe track data at POS terminals and ATMs by skimming is still a pre-dominate type of fraud in Europe as not all payment terminals and ATMs are protected with anti-skimming measures. Fraudsters are more capable of bypassing existing anti-skimming methods by placing skimming devices in areas where the machines have no protection such as at the card reader of the terminal or ATM itself. While usage of such a cloned magnetic-stripe payment card is hardly possible in the European area due to cards being secured with EMV Chip technology, globally there is still a situation that in different countries where EMV has not yet been introduced. This remains a major concern for European card issuers. Fraud losses remain high for this fraud type including the significant cost to banks and financial institutions to replace ATMs, terminals, cards and PINs and to monitor their customers' accounts for fraudulent activity.

- Shimming is a simple way to counterfeit data from the (EMV) chip on a payment card and this has been experienced around the globe. Fraud can occur when card issuers have implemented the EMV specifications incompletely. Incidents in Europe have been seen but success is rare on the part of the fraudster due to the comprehensive implementation of EMV standards across Europe. However, in the

U.S. and Mexico, due to the lack of implementation of EMV standards by issuers, fraud losses continue to occur related to shimming.

Card Data Interception

- Card not present (CNP or remote purchase fraud) (it should be noted incidents of CNP fraud are decreasing due to the implementation of secure cardholder authentication measures)
  As the volume of payment card purchases made via the Internet continues to grow, so too does Card Not Present (CNP) fraud. The Internet is the main route to buy goods or services where the payment card is not physically present and stores must rely on the cardholder information indirectly. Payment card details are obtained by fraudsters in various ways by malware or data hacks. When independent, small merchants set up their own online stores, a lack of knowledge around fraud risks can mean preventative measures are overlooked, which can leave those merchants open to greater risk of data hacking resulting in fraud.
  Hacking of large merchants continues to occur even though stores use protective measures. Criminals regularly find weaknesses and vulnerabilities.

- In addition to intercepting data via the Internet, criminals are also intercepting data using contactless technology which is increasingly popular on payment cards.
  The magnetic-stripe on payment cards is losing its value for fraudsters with the increase of EMV compliance globally. Criminals continue to research new vulnerabilities and methods to compromise card data.

- In connection with the above, “Tour Operators Online” stands for very much stolen card data. International booking sites represent the most. Card data is stolen in transit and we see most manually entered transactions due to this in hotel environment (mcc 7011) and clean consumer goods (clothing). Most of these fraudulent purchases are made in Europe.

- Recently a new type of fraud for intercepting card data information has been seen what has been referred to as account testing attacks. The objective of this attack is for the criminal to acquire knowledge on the existence, status or other sensitive information related to accounts. As examples, in a testing attack a malicious actor may try to test if a card PAN exists, test CVVs or expiry dates related to a certain PAN, or try to inject any transaction with doctored fields to try to fool the authorisation system in accepting the transaction as valid. Account testing attacks can be of various types. For CNP channels the following are common types of attacks:
  - PAN sweeps
  - Expiry Date sweeps
  - CVV2 sweeps

  These attacks can be performed through the transaction authorisation systems or through the ACS enrolment verification systems. Account testing attacks can harvest millions of card credentials if no fraud detection system, with the capability to intercept transactions, is in place. Attacks have been detected where accounts are tested at great speeds (12 per second).

Testing the accounts can be performed on certain merchants that do not have mechanisms in place to detect these kinds of attacks and once the elements are all known, the attacker can perform the high value transactions on unsuspecting merchants.

Advanced Persistent Threat (APT)

APT attacks are targeted at specific stores or financial institutions, with the aim to compromise the network or payment system and gain payment card data (see section 3.3).

Although these attacks can occur on all payment systems there have been attacks against payment card issuers resulting in serious fraud losses. Payment cards with an almost infinite limit are issued by the fraudsters and intercepted, duplicated and distributed within their global fraud network. Attacks are organised and occur mainly during periods when fraud monitoring is at a low level, e.g. at night or during weekends. After penetrating a system, fraudsters can sometimes wait for months, 'sleeping' inside the system before completing their attack.

4.1.4 Suggested Controls and Mitigation

For Merchants:

- 3D Secure: authentication protocol based on a three-domain model (Acquirer, Issuer and Interoperability domain) to ensure authenticity of both peers through Internet transactions.
- Tokenisation: process of substituting sensitive data with non-sensitive equivalent called token.
- Fraud monitoring. Deploy a responsive, real-time fraud system with prevention capabilities. Ensure your fraud system identifies suspicious patterns of behaviour to stop fraud based on tailor-made scenarios and rules.
- Always use the latest recommended update and recommendations for the operational systems from service provider, card schemes, etc.
- Perform an annual risk assessment by your Risk and / or Fraud Departments to check if all mitigating measures are completely set and in control.

For Issuers:

- Geoblocking: To protect payment cards from being misused by skimming fraud, it is strongly recommended to protect payment cards within a geographical region of use.
- Blocking: To limit the usage of payment cards to specific channels or specific contexts.
- Strong Customer Authentication with every aspect of payment card and PIN replacement.
- 3D Secure: authentication protocol based on a three-domain model (Acquirer, Issuer and Interoperability domain) to ensure authenticity of both peers through Internet transactions.
- Card synchronisation in stand-in systems. Some stand-in systems have no knowledge of what cards exist and are active (they only know of the ranges of cards that they process) and therefore the capability to detect account testing attacks is greatly reduced so too is the capability to protect against brute force attacks.
- Non-sequential issuance of cards. Some issuers still issue cards in a sequential manner. Thus all cards in a certain range will be valid and with the same expiry date. In order to reduce the level of success for an attacker to determine valid PANs and also in order to help fraud detection systems, PANs should be issued in

a non-sequential fashion. By doing so, an attacker that sweeps through a range of PANs, will generate a high percentage of “Inexistent PAN” errors and ultimately be detected with greater ease.

- Mandatory use of CVV2: The CVV2 was introduced more than two decades ago in order to reduce the probability of success in performing a valid transaction, with only the PAN and expiry date. Unfortunately, the exemption for the mandatory use of the CVV2 at certain big merchants results in the fact that issuers deactivate the validation of CVV2, otherwise a significant percentage of their cardholders´ transactions would be rejected. The use of CVV2 for internet payments should be mandatory.
- Card limits: Promote customer awareness on the ability to reduce withdrawal limits or even limit to zero.
- Transaction information: Inform your cardholders about authorised transactions in real time (could be SMS or push messages) to enable quick customer feedback.
- Always use the latest recommended updates and recommendations for the operational systems from service providers, card schemes, regulators, etc.
- Fraud monitoring: Deploy a responsive, real-time fraud system with prevention capabilities. Ensure your fraud system identifies suspicious patterns of behaviour to stop fraud based on tailor-made scenarios and rules.
- Perform an annual risk assessment to check if all mitigating measures are completely set and in control.
- Besides the technical measures awareness-raising (customer education) is an essential point to prevent, more in particular, “low-tech” fraud.

For Cardholders

- Always keep your payment card in a safe place and protect your PIN. Report immediately to your card issuer, if the payment card goes missing.
- If a financial institution offers controls on limits for the payment card, ensure you set these at the limits typical for your daily usage.
- If your financial institution offers geoblocking, set the correct geographical region of use and adjust it on time for your convenience.

4.1.5 Final Considerations/Conclusions

Historical and current fraud types such as lost and stolen fraud, counterfeiting and card not present will continue to be the predominant drivers of payment card fraud. However technical developments can change this trend and therefore should be implemented and advice taken as much as possible from entities such as the EPC’s Card Fraud Prevention Forum.

Especially, new fraud techniques such as shimming or attacks on contactless cards should be monitored carefully and guidelines on preventing these issues implemented.

4.2 ATM Fraud

4.2.1 Definition

ATMs are vulnerable to several types of attacks which essentially come under the following headings:

- ATM fraud – an attack against the Payment Cards and PINs used at an ATM (e.g. skimming and shimming attacks);

- Malware/Logical attacks – an attack on the logical integrity of an ATM or the ATM Environment (logical attacks), e.g. via ATM malware which typically compromises the ATM software and operating system;
- Physical attacks at ATM – an attack on the physical integrity of the ATM.

Note: Physical attacks are out of scope for this document.

4.2.2 Fraud description

The following description of the modus operandi is based on the European Association of Secure Transactions (EAST) guidelines.

Attacks against customers - Cards and PIN

- Skimming - Skimming is the installation of an unauthorised device to capture data from the magnetic stripe of a payment card
- Shimming - Shimming is the interception ("passive") and / or manipulation ("active") of information flowing between an EMV card and the chip interface of a card reader. Target: to obtain the original payment card and PIN details

Card Trapping

Card Trapping is the unauthorised physical manipulation of an ATM, preventing the payment card being returned to the card owner. The criminal mounts a device over or within the ATM card entry slot prior to the customer using the machine and collects it directly afterwards; the PIN can be gathered via shoulder surfing, camera or PIN-pad overlay.

Transaction Reversal Fraud

Transaction Reversal Fraud is the unauthorised physical manipulation of an ATM cash withdrawal which makes it appear cash has not been dispensed thereby causing a reversal message to be generated. The criminal requires an active payment card, approved for ATM usage and with sufficient available funds; they carry out a financial transaction and then physically manipulate the cash presenting sequence, either with or without the use of an unauthorised device. The criminal has gained access to, and removed, the cash yet the ATM perceives that no cash was dispensed and passes a reversal message for the Issuer to complete. In these cases, fraud losses are absorbed by the ATM owner.

Attacks against the ATM (without Card involvement)

ATM Malware Attack - Cash-Out (Jackpotting) / Man in the Middle (MitM) / Software Skimming (SW-Skimming). With an ATM malware attack, the criminal can run unauthorised software, or authorised software in an unauthorised manner, at the ATM computer to perform an attack known as '*Black Box*' which is where the fraudster connects an unauthorised device to an ATM that sends dispense commands directly to the ATM cash dispenser effectively telling the machine to "Cash-Out".

4.2.3 Current and new ATM fraud trends

ATM Skimming

Skimming remains a major issue, resulting in high fraud losses. An increasing number of criminals are bypassing ATM anti-skimming equipment by placing skimmers where they know the anti-skimming equipment is not effective, e.g. the inside of a card reader.

As magnetic-stripe usage outside Europe continues, fraudsters will continue to skim card data and used the cloned cards in countries where Chip / EMV has not been implemented.

While an increasing number of countries in Europe are adopting geo-blocking as a form of fraud prevention (or geo control) on their cards portfolio, skimming will migrate from these countries.

Where skimmed card usage is prevented, there is often an upwards trend in cash and card trapping incidents. However, in all these cases the losses are limited as just one card or money from just one cash withdrawal can be stolen during each attempt.

Shimming

Attempts of shimming devices on ATMs and POS terminals have been seen across the globe. The criminal is targeting issuers and/or acquirers which have not implemented EMV protocol correctly.

Transaction Reversal Fraud (TRF)

Fraudsters are overcoming mitigating measures taken by ATM deployers to prevent TRF, especially at the more vulnerable legacy ATMs still in operation.

Malware and black box attacks (to be updated following H1 2018 EAST figures)

An ATM is, in principle, a money box which is operated by an internal computer. This computer has become increasingly under attack by criminals. In 2014 the European Association of Secure Transactions (EAST) began collecting statistics on ATM malware and logical attacks, when the first attacks in Western Europe were reported. In the European Payment Terminal Crime Report from EAST (European association of Secure transactions) covering first half of 2018 there were 61 such attacks reported against European ATMs. This is a 46% decrease from the 114 attacks reported during H1 2017. And all the reported ‘jackpotting’ attacks were ‘black box’ attacks. Related losses were down 83% (from €1.51 million to €0.25 million) reflecting the fact that many of these attacks are unsuccessful.

4.2.4 Suggested Controls and Mitigation

For Card Issuers

- Geoblocking: To protect cards from being misused by skimming fraud, it is strongly recommended to protect cards with a geographical region of use. This restriction is an effective protection against fraud through skimming.
- Blocking: To limit the usage of cards to specific channels or specific contexts.
- Card limits. Customer awareness on the ability to reduce withdrawal limits or even limit to zero.
- Always use the latest recommended update and recommendations for the operational systems from service provider, card schemes etc.
- Perform an annual risk assessment to check if all mitigating measures are completely set and in control.
- EMV Fall-back: Ensure that no fall-back to magnetic stripe transactions are authorised.

- Fraud monitoring: Deploy a responsive, real-time fraud system with prevention capabilities. Ensure your fraud system identifies suspicious patterns of behaviour to stop fraud based on tailor-made scenarios and rules.

For ATM Owners / Operators

- For details on malware countermeasures, consult the EAST Expert Group on ATM Fraud / Europol guidance document which provides recommendations on countermeasures regarding logical attacks on ATMs (published by Europol in June 2015.[86])
- Always use the latest recommended update and recommendations for the operational systems from service providers, regulators, card schemes, etc.
- Perform an annual risk assessment to check if all mitigating measures are completely set and in control.

For Cardholders

- Always keep your payment card in a safe place and protect your PIN. Report immediately to your card issuer, if the payment card goes missing.
- If a financial institution offers controls on limits for the payment card, ensure you set these at the limits typical for your daily usage.
- If your financial institution offers geoblocking, set the correct geographical region of use and adjust it on time for your convenience.

4.2.5 Final Considerations/Conclusions

Skimming and low-tech fraud remain the most common frauds at ATMs. The financial impact from these types of fraud is often absorbed by the card issuer of the compromised/stolen card. Thus, countermeasures should be taken by the card issuer.

For ATM owners/operators, high tech fraud, such as the use of malware or black box attacks, is a growing concern. The financial impact hits the ATM owner/deployer and not the cardholder or card issuer. Therefore, it is recommended to establish the guidelines provided in the related Europol Guide.

4.3 SEPA Credit Transfer (including instant) and Direct Debit fraud

The various types of attacks described in this document under sections 3 and 4 could lead to fraud for SEPA credit transfers and direct debit transactions.

During the last years, the criminals' use of impersonation and deception scams, as well as online attacks to compromise data, continued to be the primary factor behind fraud losses related to these types of payments. In all of these methods, criminals target personal and financial details which are used to facilitate fraud.

In an impersonation and deception scam, a criminal purports to be from a legitimate and trusted organisation, such as a bank, the police, a utility company or a government department. These scams typically involve the fraudster contacting a customer or a company employee (pretending to be the CEO), through a phone call, text message, email or social media.

[86] https://www.ncr.com/content/dam/ncrcom/content-type/brochures/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf

CEO fraud and business email compromise attacks continue to grow and evolve, targeting all size of businesses and personal transactions. Between December 2016 and May 2018, there was a 136% increase in identified global exposed losses, according to a release by the FBI in July 2018[87].

It has been recently noted that fraudsters have been targeting specific customer groups (e.g. elderly persons) to convince them to create a mobile authenticator under the fraudster's control (e.g. mobile e-identity) that is used later-on to initiate fraudulent payments

As mentioned in the 2018 report from UK Finance[88], intelligence suggests that criminals have recently increased their focus on contacting customers by phone, text message or email pretending to represent a trusted organisation such as a bank, the police, a utility company or a government department. Often the approach claims that there has been suspicious activity on an account, account details need to be updated or verified or a "refund" is due. The information gathered (such as passwords and passcodes, bank account details) are then used by the criminal to make an unauthorised payment. Criminals also use these fraudulent approaches to trick people into authorising a payment to them. Fraudsters use a range of tactics to commit this crime such as sending fake invoices, offering fraudulent investment opportunities and online auction scams.

One of the most important techniques now and for the future seems to be APT. It must be considered as a potential high risk not only for the payment infrastructure but for all network related ecosystems. With a minimal of involved criminals a maximum result can be established (see section 3.3).

Currently only some high-level indications of levels and types of fraud can be observed, related to SCT and SDD payments which indicate that fraud rates remain at a minimum level. The procedures for collecting data, as well as the related cooperation between authorities and payment service providers, will be enhanced in the near future with the implementation of harmonised fraud reporting requirements at EU level under PSD2 [3] and the dedicated EBA guidelines [2]. As a result more accurate figures should become available in the future.

In countries where instant payments have been implemented, no difference has been noted yet concerning fraud levels compared to "normal" credit transfers.

With regard to types of fraud, "issuance of a payment order by a fraudster" remains the main fraud type for all SEPA payment instruments. "Manipulation of the payer to issue a payment order" suffered the highest growth over the past years, while "modification of a payment order or issuance of a fraudulent payment order by the fraudster", based on information gathered through social engineering, phishing, or malware is scoring the highest priority amongst PSPs concerning combating fraud. This last category also encapsulates some current technical frauds such as malware and "man-in-the-browser" attacks.

[87] https://www.ic3.gov/media/2018/180712.aspx

[88] https://www.ukfinance.org.uk/fraud-the-facts-2018/

5 Conclusions

The organisation and sophistication of recent cyberattacks have shown a greater degree of professionalism of cybercriminals.

The main attack focus over the past year has shifted slightly away from malware to social engineering attacks, except for attacks against companies where malware appears to be the prevalent methodology. Social engineering attacks and phishing attempts are still increasing and they remain instrumental often in combination with malware. Whereas before consumers, retailers and SMEs have been the main focus, the last year more and more company executives, employees (through CEO fraud), financial institutions and payment infrastructures appear to become preferred targets.

Malware remains a major threat but more in particular ransomware has been on the rise during the past years. This type of attack appears to be more profitable to the attackers than the traditional banking Trojans. It is not possible to achieve full protection to not be hit by a malware attack. However, raising awareness campaigns with a few simple advices to the customers to mitigate malware attacks (software updates, anti-malware tools, do not click on links, etc.), are one of the best tools to mitigate the risks and impact. Similar awareness must be in place for the employees of the PSPs.

One of the most lucrative types of payment fraud now and for the future seems to be Advanced Persistent Threats (APTs). It must be considered as a potential high risk not only for the payment infrastructures but also for all network related ecosystems. With a minimal involvement of criminals a maximum result can be established. Therefore all users who are normally cautious when operating their company computers but often tend to be less careful when using personal mobile devices (BYOD) and apps (BYOA) will need to consider utilising new defense mechanisms in order to hide their data. Endpoint and network defenses, as well as using the latest anti-virus software and next-gen firewalls, are effective but may not be enough for companies to prevent them from being hacked. A mixed approach made of traditional tools, new advanced behaviour-based detection solutions with improved automated monitoring, correlation and analysis, and improved incident response capabilities can aid system security administrators in identifying these hard-to-detect intrusions. APTs have become a significant challenge for many cybersecurity professionals around the world and with evidence of more complex APTs in front of us as the threat landscape evolves, learning to detect – and stop - even the most advanced threats is paramount[89].

The number of (D)DoS attacks is still growing and they are still frequently targeting the financial sector and have impacts on the availability of their services to the customers.

There is a continuation of botnets and because of the high volume of infected consumer devices (e.g. PCs, mobile devices, etc.) severe threats remain. Besides an ever increasing level of professionalism among the attackers whereby addresses of infected

[89] http://resources.infosecinstitute.com/current-trends-apt-world/#gref

computers, routers or bots are sold or rented, the usage of IoT devices (such as CCTVs) for launching DDoS attacks continued to be noted during the past year. It is expected that the usage of these devices to launch attacks will further increase over the years to come.

Multi-vector attacks are becoming commonplace and have been targeting a number of financial institutions. Recent examples of multi-vector attacks include cyberattacks using the SWIFT-related banking infrastructure, ATM infections, adapting card risk parameters, remote banking systems and POS terminal networks.

Along with the “classic” threats mentioned above, new risks are arising from the use of innovative technologies. Mobility is part of both consumers' and enterprises' daily life and operation. Smart mobile devices have become a commodity in Europe enabling a wide variety of mobile apps, including payment apps. As a result, they are more and more becoming an attractive target for cybercriminals, along with the IoT devices. The number and types of IoT devices are continuously increasing, posing the risk of new types of attack.

The need for reducing operational costs and the huge and rapidly growing size of data lead to new business decisions for adopting cloud and big data analytics technologies. Data everywhere, 'data in flight', data produced and stored in billions of interconnected devices, and data in the cloud. Innovation, like IoT devices and mobile apps/wallets, and new technologies are bringing new opportunities to businesses but new risks too.

There is also a competitive market drive for user-friendliness and simplicity which leads to increased pressure on security resources and difficult trade-offs to be made by PSPs. The challenge will be to find the right balance between the user-friendliness and the security measures needed. As security becomes more regulated (NIS Directive [5], GDPR [6], PSD2 [6]), payments also face a new regulatory landscape in Europe, which on one hand increases the security barrier with respect to fraud (e.g. customer authentication) but at the same time also “opens up” the payment value chain which introduces new security challenges for all stakeholders involved.

Another phenomenon that is appearing in the market is “cybercrime-as-a-service”, causing huge challenges to companies. It appears to be a business model that is continuously growing as threats are evolving, which is also increasingly efficient. These services offer the possibility to persons that do not have the technical knowledge, to execute attacks. Examples of these services that are currently being offered include ransomware, phishing campaigns and malware attacks. They represent a big challenge for PSPs, because although the threats are the same as described in this document, a much larger number of people can now participate in a cyberattack, leading to a certain automation level. The recommendation for PSPs would be to be up to date in threats tactics and campaigns paying close attention to attacks that have occurred with other PSPs or companies.

Concerning card payment fraud, as long as the mag-stripe is needed for international transactions, skimming will remain an issue. Criminals are changing their approach to fraud. Not only by changing to more high tech frauds like APT, but also a part of the criminals is reverting to old school types of fraud such as lost and stolen. This has already become in some EU countries a higher cost driver than skimming. As e-commerce is still on the rise, CNP fraud remains a significant factor for fraud losses. The problem remains the implementation of strong customer authentication by (risky) merchants. The Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication under PSD2 [4], are a key factor for the reduction of this type of fraud.

For SEPA Credit Transfers and Direct Debit transactions, the criminals' use of impersonation and deception scams, as well as online attacks to compromise data, continued to be the primary factor behind fraud losses related to these types of payments. In all of these methods, criminals target personal and financial details which are used to facilitate fraudulent transactions.

An important aspect to mitigate the risks and reduce the fraud related to payments is the sharing of fraud intelligence and information on incidents amongst PSPs. However, often this is being limited by existing regulations related to data protection, even more so in the case of cross-border sharing. It is to be expected that the new EBA guidelines on fraud reporting [2] will support an improved information sharing and more accurate fraud figures.

Moreover, new mechanisms should be put in place to enable cybercriminal prosecution within the European Union and internationally.

The European Commission is reviewing and extending the legislation on combating fraud and counterfeiting of non-cash means of payment[90]. The 2001 Council Framework Decision on combating fraud and counterfeiting of non-cash means of payments no longer reflects today's reality, such as use of virtual currencies and mobile payments and was focused on card-fraud only.

The European Union is also discussing an e-evidence Regulation[91] to make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals and terrorists[92]. Although this Regulation will only cover the Member States there is still a need to increase the international scope. Furthermore, it is vital that the pressure increases on those countries that are not being diligent with cyber-criminal prosecution. Even though there is also a cyber diplomacy toolbox under discussion, this tool is initially targeting critical infrastructure issues such as large cyber-attacks and other cyber-space conflicts. It does not address the essential need to prosecute ongoing minor cyber-criminals' fraud acts that although not seen as a single big attack, are overall causing a huge amount of economic impact.[93]

[90] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0489:FIN

[91] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[92] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

[93] https://www.euractiv.com/section/cybersecurity/news/eu-plans-aid-to-prosecute-hackers-and-support-member-states/

Finally, PSPs must understand the emerging threats, the possible impacts and should keep investing in appropriate security and monitoring technologies as well as in customer awareness campaigns.

Annex I – SEPA Payment Instruments

The SEPA payment instruments are:

SEPA Credit Transfer (SCT)

The SCT scheme – like any other credit transfer scheme – allows to transfer money from account A to account B at the request of the holder of account A. The SCT scheme enables payment service providers to offer a credit transfer service throughout SEPA, whether for single or bulk payments. The scheme's standards facilitate payment initiation, processing and reconciliation based on straight-through-processing. The scope is limited to payments in euro within SEPA countries, regardless of the denomination of the underlying accounts. The PSPs executing the credit transfer would have to be scheme participants; i.e. both would have to formally adhere to the SCT scheme. There is no limit on the amount of a payment carried out under the scheme.

The SCT scheme rulebook and the accompanying Implementation Guidelines are the definitive sources of information regarding the rules and obligations of the scheme. In addition, a document entitled "Shortcut to the SEPA Credit Transfer Scheme" is available which provides basic information on the characteristics and benefits of the SCT scheme.

SEPA Instant Credit Transfer (SCT Inst)

The SCT Inst scheme is a new scheme which entered into effect in November 2017. It allows euro credit transfers – initially up to 15,000 euro – in less than ten seconds, 24/7/365, between accounts located in the 34 countries of the SEPA schemes geographical scope. In addition, PSPs willing to increase the maximum limit and transaction speed can bilaterally or multilaterally agree to do so. The SCT Inst scheme is optional.

SEPA Direct Debit (SDD)

The SDD schemes - like any other direct debit scheme - are based on the following concept: "I request money from someone else, with their pre-approval, and credit it to myself".

The Core and Business to Business (B2B) SDD schemes apply to transactions in euro. The debtor and creditor each would need to hold an account with a PSP located within SEPA. The PSPs executing the direct debit transaction would have to be scheme participants; that is, both would have to formally adhere to the SDD scheme. The scheme may be used for single (one-off) or recurrent direct debit collections; the amounts are not limited. The SDD B2B scheme is available only to businesses and is an optional scheme.

Cards ("SEPA for Cards" - SEPA Cards Standardisation Volume)

The SEPA Cards Standardisation Volume (see [8]) was initially created by the EPC and further developed by the Cards Stakeholders Group (CSG). This document defines a standard set of requirements to enable an interoperable and scalable card and terminal infrastructure across SEPA, based on open international card standards. The European Cards Stakeholders Group (ECSG) was created in 2016 and took over the mission of the CSG. This multi-stakeholder association is made up of organisations from five sectors of the card payment chain (retailers/wholesale, vendors, processors of card transactions, card schemes, and PSPs). The ECSG develops and maintains the Volume, and focuses on a cards standardisation programme that will create a better, safer, more cost efficient and functionally richer card services environment, whatever the card product or scheme may be. The latest version of the Volume (version 8.0) was published in March 2017.

Further information on the SEPA payment instruments may be obtained from the EPC website (www.epc-cep.eu).

Annex II – Summary Threats versus Controls and Mitigations

Threat	Suggested Controls & Mitigations
Denial of Service Section 3.5	o Dynamic DDoS security control framework o DDoS mitigation scrubbing service o Periodic tests of anti DDoS measures o Security intelligence feeds and incident response team o “Forensic ready” logging
o Flooding	
o Protocol	
o Application layer	
Social Engineering & Phishing Section 3.1	o Exchange of information between PSPs o Transaction filtering and monitoring o Awareness raising for consumers, SMEs and corporates o Blocking spoofed mails (DMARC) o Takedowns of phishing web sites
o Reverse Trojan horse	
o Voice Phishing (vishing)	
o Angler Phishing	
Malware Section 3.2	o Regular software update o Script and macro blockers, IPS / IDS functionality o Limited usage of admin rights o Firewalls and antivirus on consumer devices o Awareness about danger of opening attachments o Web traffic and e-mail content analysis
o Trojans	
o Ransomware	
o Remote Access Trojans	
Advanced Persistent Threats Section 3.3	o Behaviour analysis tools o Real time advanced security data analytics o Incorporation of security threat intelligence into infrastructure o Advanced IP scanner/ APT scanner o Red Team/Blue Team approach o Five styles of Advanced Threat Defense Framework
o Customised malware	
o Waterhole attack	
Mobile Device Related Section 3.4	o Regular software updates o Screen lock / mobile device lock o No jailbroken or rooted devices
o Fake Apps	
o Mobile malware	

o Spoofed SMS (smishing)	o Only call validated PSP numbers o PSPs never ask for credentials over the phone o App store monitoring o Installation of anti-virus software o App code protection and pen testing o Sensitive data encryption o No trust in third-party libraries o Controls to protect communication channels o User and device verification o User notification via more than one channel o PSP notifications by operator about SIM swaps or duplications
o Attacks on mobile apps (app & OS security, user awareness, abuse of privacy, enrollment processes, biometric authentication, duplicated SIMs)	
o SIM swapping	
Botnets Section 3.6	o Blacklisting o Sinkholing and blocking o Distribution of fake/traceable credentials o DNS-based countermeasures o Direct takedown of command-and-control server o Packet filtering on network and application level o Walled gardens o Peer-to-peer countermeasures o Infiltration and remote disinfection o Take downs by law enforcement o awareness raising and co-operation
o Captcha solving	
o Brute force	
o Data harvesting	
o Spreading of malware	
Cloud Services & Big Data (SaaS, PaaS, IaaS) Section 3.7	o Risk based approach o Self-control over authentication o Strong authentication and authorisation controls o Monitoring/audit/certification of service providers o Adequate training of employees
o Data exposure	
o Enhanced risks related to authentication / encryption	
Internet of Things (IoT) Section 3.8	o Security risk assessment for every new device and infrastructure o Adopt security and privacy by design
o Data exposure	

o New targets for # attacks (malware, botnets, etc.)	o Strong authentication and authorisation controls o Secure device to device communication o Deployment of devices with international recognised security certifications o Minimisation of amount and type of data exchanged
Virtual currencies Section 3.9	o Detect characteristics of fraudulent investment schemes o Wallet security best practices o Cyber insurance o Regulation of virtual currencies
o Anonymity exploitation	
o Attacks to exchange traders	
o Wallet compromise	
Multi-Vector Section 3.10	o Invest in Advanced Threat Protection (ATP) o Response and defense to identify, stop and recover
o Combination of multiple attack elements	
o Designed to avoid traditional defenses	

Table 5: Summary threats versus controls and mitigations

End of Document