European Payments Council

2019 Payment Threats and Fraud Trends Report

EPC302-19 /Version 1.0 / Date issued: 9 December 2019

Report

2019 Payment Threats and Fraud Trends

EPC302-19
Version 1.0
Date issued: 9 December 2019
November 2019

European Payments Council

European Payments Council AISBL,
Cours Saint-Michel 30 B-1040 Brussels
T +32 2 733 35 33
Enterprise N°0873.268.927
secretariat@epc-cep.eu

Abstract

This new edition of the threats trends report reflects the recent developments concerning security threats and fraud in the payments landscape over the past year.

Table of Contents

List of tables

List of Figures

Annex List

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 https://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) entice payment fraud and how to mitigate related 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 Transfer 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 and more frequently leading to authorised push payments fraud.
- With PSD2 and the dynamic linking of authentication codes to the payment transaction details for remote transactions, phishing of authentication codes will become useless but phishing of activation codes for mobile payment /authentication apps could be expected to become a new playing field for social engineering.
- 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 APTs. It must be considered as a potential high risk not only for payment infrastructures but also for all network related payment ecosystems.
- More and more, mobile devices are becoming an attractive target for cyber criminals, along with IoT devices.
- The number of (D)DoS attacks does no longer increase but they are still 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" is 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.

Notwithstanding these 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 remains to find the right balance between user-friendliness and the security measures needed.

As security becomes more regulated (PSD2 [6] and the RTS [9], GDPR , NIS Directive [7]), 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, criminals are changing their approach. 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, sometimes in combination with social engineering. 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. During the past year an increase in Authorised Push Payment fraud is to be noted.

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 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 the availability of more accurate fraud figures.

It is also worthwhile mentioning that the EPC is establishing a new group on fraud related to the SEPA payment instruments[1], namely the Payment Scheme Fraud Prevention Working Group. The aim is to contribute to operational payment fraud prevention by facilitating SEPA payment scheme fraud data collection and analysis, information sharing and prevention measures.

PSPs could also investigate new proactive methods to prevent fraud. As an example, the payee’s PSP having received a possibly fraudulent transfer may easier recognise subsequent attempts to pass on the money as mule activity, if the transfer is accompanied by a fraud marker, signalling that the payer’s PSP although not having clear evidence of fraud, finds the transfer suspicious. Another potential fraud mitigating measure is the implementation of a “Confirmation of payee” service as described in this report.

The European Commission has reviewed and extended the legislation on combating fraud and counterfeiting of non-cash means of payment (see [10]). But also new mechanisms should be put in place to enable cybercriminal prosecution not only within the European Union but also globally.

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] see Annex I.

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, the scope and the targeted audience of the document. Section 3 analyses threats which are encountered nowadays in payment contexts and are contributing to fraud. Section 4 elaborates on fraud related to payment instruments and how fraudsters can monetise their gains from attacks. Conclusions of this report may be found in Section 5. Annex I provides a brief overview of 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]	EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC	EBA
[4]	EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2	EBA
[5]	EBA-Op-2019-11: Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions	EBA
[6]	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
[7]	Network Information Security Directive (NIS Directive) 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	EC
[8]	General Data Protection Regulation (GDPR)	EC

	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	
[9]	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')	EC
[10]	Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA	EC
[11]	ECSG 001-17 – SEPA Cards Standardisation Volume	ECSG
[12]	EMV Payment Tokenisation Specification	EMVCo
[13]	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.
Authorised Push Payment scam (APP scam)	This is fraud caused by a criminal who tricks their victim into transferring money directly from their account to an account which the criminal controls, whereby the victim authorises the payment themselves.
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 [13]).
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, smartphones, 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.
Near Field Communication (NFC)	A contactless protocol for mobile devices specified by the NFC Forum for multi-market usage. NFC Forum specifications are based on ISO/IEC 18092 but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443.
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 Articles 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 [12].

Table 2 Definitions

1.4 Abbreviations

Throughout this document, the following abbreviations are used.

Abbreviation	Term
AI	Artificial Intelligence
APP	Authorised Push Payment
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
CSA	Cloud Security Alliance
CSDE	Council to Secure the Digital Economy
CSP	Cloud Service Provider
C&C	Command and Control
DoS	Denial of Service
DDoS	Distributed Denial of Service
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DOTS	DDoS Open Threat Signalling
DVR	Digital Video Recorder
EBA	European Banking Authority
EBF	European Banking Federation
EC	European Commission
ECSG	European Cards Stakeholders Group

ENISA	European Network and Information Security Agency
EPC	European Payments Council
EV	Extended Validation
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
Gbps	Gigabit per second
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS
IBAN	International Bank Account Number
IDS	Intrusion Defense System
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Preventions System
ISO	International Organization for Standardization
IT	Information Technology
KYC	Know Your Customer
MTAN	Mobile Transaction Authorisation Number
NFAT	Network Forensic Analysis Tool
NFC	Near Field Communication
NIS	Network Information Security
OTP	One-Time Password/Passcode
PAN	Primary Account Number
PC	Personal Computer
PII	Personally Identifiable Information[2]
PIN	Personal Identification Number
PLC	Programmable Logic Controllers
POI	Point of Interaction

[2] Defined as personal data under the GDPR (Article 4 in [8]).

POS	Point of Sale
PSD	Payment Services Directive
PSP	Payment Service Provider
RAM	Random-Access Memory
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
RTS	Regulatory Technical Standard
SCA	Strong Customer Authentication
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
SPF	Sender Policy Framework
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
U2F	Universal Second Factor
VPN	Virtual Private Network

Table 3 Abbreviations

2 General

2.1 About the EPC

The European Payments Council (EPC), as one representative of the European Payment Service Providers' (PSPs) sector, 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 and payment-related 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 payment and payment-related 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 based on 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 payment threats and fraud trends report.

2.3 Scope and objectives

The present document aims to provide an insight in the latest developments over 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 in 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 Service Providers
- 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

3.1 Introduction

In this section, various threats that may lead to fraud related to payments will be described. Note however that often attacks are caused by exploiting a combination of several threats. Multi-vector attacks are becoming commonplace and have been targeting a number of financial institutions (e.g. recent examples of multi-vector attacks include cyberattacks using the SWIFT-related banking infrastructure, ATM infections, remote banking systems and POS terminal networks[3], making changes in PSP' databases to "play" with account balances, as well as the so-called supply-chain attacks, i.e. attacks on vendors supplying financial organisations[4]).

3.2 Social Engineering

3.2.1 Definitions

Social engineering is a method of persuasion whereby through a variety of techniques the attacker manipulates people into carrying out actions leading to compromise or fraud. 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 directly attack their system or device.

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

The ultimate goal of a social engineering attempt used against bank customers or employees varies; it may be exploited to first gain access to data or systems via tricking users into exposing their credentials (phishing) or their systems (as covered in the malware Section 3.3); it may also be exploited to directly get hold of financial resources via manipulating users into initiating themselves payments to accounts under the attacker's control (authorised push payment fraud).

Social engineering attacks further range from mass email attempts that can be more or less easy to identify as an attempt to defraud a customer, to dedicated mails or voice calls that target a specific customer or employee (spear phishing).

3.2.2 Fraud Description

Below an insight is given on how social engineering may lead to fraud. More details on fraud caused by social engineering on specific payment instruments, may be found in Section 4.

Phishing: There are various phishing techniques (including credential/password/OTP phishing) whereby smishing and vishing are used to specifically refer to phishing via SMS or voice channels. The vast majority of phishing cases adopt one of the following approaches:

- An email or SMS pretends to come from a trustworthy organisation with a link that seems to lead to the login page of this organisation's website.
- A pop-up window or overlay on a PC or mobile device tricks users into exposing credentials, card data or other sensitive information towards a fake user interface.

A typical voice phishing case may run as follows. The fraudster calls a victim and claims they are a PSP employee (or policeman, or from a public authority) and that there is an emergency (putting psychological pressure on the victim). By claiming that there is a risk that a huge sum of the victim's money may get lost, the victim gets further scared. Fortunately, the "PSP employee" can

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

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

offer help. The victim just needs to authenticate with their credentials. This psychological mix of urgency, fear of losing money, and kind helpfulness may overcome the targeted person's unwillingness to expose credentials, and if not the "PSP employee" may ask a "senior fraud investigator" to call the potential victim, who might give in when the second "serious PSP employee" calls and confirms the story told by the first.

Having used phishing to get hold of the necessary credentials the fraudster has various ways to abuse them:

- Create a fraudulent payment in an on-line banking system or in a 3DSecure card transaction.
- Enrol a payment app, mobile bank app or general authenticator app, with which not just one, but several fraudulent transactions can be made.
- Change personal information in an authoritative registry e.g. change the surface mailing address for credentials or the bank account for tax returns (and then trigger a return by claiming a lower income or the like).
- Get control over the mailbox or social media accounts and send social engineering emails to potential victims, claiming to be in great distress and asking for the friends to send money (cfr. email from a friend).

The latter example is in fact a hybrid one since it starts as phishing, but eventually aims at social engineering for authorised push payment fraud.

Scam-based fraud: There are various ways to directly social engineer users into initiating themselves payments to accounts under an attacker's control (APP Fraud). "Email from a friend" as mentioned above is just one commonly cited example. 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 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.

For a description of commonly observed APP scams, the reader is referred to Section 4.4.

3.2.3 Impact & Context

Social engineering techniques have greatly increased over the last 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 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 3.2.4) 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.

[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/

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 (see Section 3.3).

Social engineering and phishing attack trends in 2019:

- According to a release by the FBI in September 2019[6]:
- Business Email Compromise attacks continue to grow and evolve, targeting small, medium, and large business and personal transactions. Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses.
- The scam has been reported in 177 countries, with monies transferred to at least 140 countries.
- Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, the FBI has seen an increase of fraudulent transfers sent to the United Kingdom, Mexico, and Turkey.
- The following statistics were reported in victim complaints between June 2016 and July 2019: more than 166,000 complaints have been made globally with an exposed loss of $26 billion.
- According to the Proofpoint Human Factor Report 2019[7]:
- Attackers are increasingly focused on obtaining credentials to feed further attacks and are improving the social engineering techniques with which they obtain them. Similarly, malware distribution is far more focused on establishing a silent foothold in organisations to commit fraud and steal data and credentials rather than simply smash-and-grab via ransomware attacks.
- Generic email harvesting accounted for almost 25% of all phishing schemes in 2018. In 2019, Microsoft Office 365 phishing has been the top scheme, but the focus remains credential harvesting.
- Kaspersky Lab identified the following trends in the first quarter of 2019[8]:
- In Q1, they observed a large surge in spam mailings aimed at users of the Automated Clearing House (ACH), a US-based e-payment system that processes vast quantities of consumer and small-business transactions. These mailings consisted of fake notifications about the status of transfers supposedly made by ordinary users or firms. Such messages contained both malicious attachments (archives, documents) and links to download files infected with malware. 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.
- Spammers continue to wring cryptocurrency payments out of users by means of “sextortion”.
- Fake customer support emails are one of the most popular types of online fraud. The number of such messages has grown quite significantly of late. Links to fake technical

[6] https://www.ic3.gov/media/2019/190910.aspx

[7] https://www.proofpoint.com/us/resources/threat-reports/human-factor

[8] https://securelist.com/spam-and-phishing-in-q1-2019/90795/

support sites (accompanied by rave reviews) can be seen both on dedicated forums and social networks.

- Banks are firmly established as top phishing targets. Scammers try to make their fake messages as believable as possible by substituting legitimate domains into the sender's address, copying the layout of official emails, devising plausible pretexts, etc. In Q1 2019, phishers exploited high-profile events to persuade victims of the legitimacy of the received message — for example, they inserted into the message body a phrase about the Christchurch terror attack. The attackers hoped that this, plus the name of a New Zealand bank as the sender, would add credibility to the message. The email itself stated that the bank had introduced some new security features that required an update of the account details to use.

3.2.4 Suggested Controls and Mitigation

The sender of **phishing** emails will typically like to spoof the domain name of a PSP or other trustworthy entity. Such organisations may try to prevent this by implementing following countermeasures:

- Sender Policy Framework (SPF), which is an email-validation system designed to detect email spoofing.
- Domain Keys Identified Mail (DKIM)9, 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.
- Domain-based Message Authentication, Reporting and Conformance (DMARC)[10] 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.

For SMS and voice there are no general countermeasures, but agreements e.g. by groups of PSPs with groups of telecom operators may help in achieving some level of protection here as well.

Awareness campaigns are still very important countermeasures against phishing. "Never give away your password and OTPs" to someone who calls. No matter who the caller claims to be – or how urgent the caller says it is." The warning against phishing is simple, but to get the message through and enable customers to comply in stressed situations is not simple. 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-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).

The customer's possibility to determine whether an email or website is genuine should be supported by service providers by ensuring that

- Login screens only occur in https sessions using certificates with Extended Validation.

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

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

- Websites consistently use the same easy-to-recognise domain names / URLs.
- Websites support HSTS.
- Emails to customers never contain links to login screens asking for passwords etc. or other sensitive information.

An inherent countermeasure against phishing is to provide the user/customer with an authenticator, which does not expose any information to the user. Hence, the user cannot expose any credentials, but social engineering may still be used to trick the user in unintentionally authorizing third-party access.

Private companies – working in close cooperation with telecom operators - offer takedown of phishing websites as a service. Such 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 compromised authenticator.

If credentials have been phished successfully and the attacker tries to abuse them to make a fraudulent transaction, there may still be hurdles to overcome. The service provider may detect that user device, IP-address, user behaviour on the website, financial transaction, time or other context information is 'suspicious' and therefore decide to put the transaction on hold, until customer has reconfirmed the transaction via a secure out-of-band channel, reconfirmation app or call-back.

Since September 2019, PSD2 [6] and the RTS [9] require that authentication codes used by the payer to authorise a remote transaction are dynamically linked to the transaction amount and payee. As such "authentication codes" can no more be abused by a "phisher" to authenticate another payment transaction. But phishing will remain an important fraudster tool, especially if it is possible to phish data that can subsequently be used to enrol a payment app or to authenticate in a voice call with the PSP.

Scams aiming for APPs are very different and require more elaborate warnings. Specific customer segments may be more exposed to some types of scams than others. For instance corporate customers are more exposed to invoice scams and CEO-fraud and the awareness campaigns must be tailored accordingly. In the private segment e.g., the elderly customers seem to be more exposed. It could be considered to have a special awareness campaign towards certain vulnerable groups. But since it may be difficult to reach the target groups effectively, it is recommended also to run more general campaigns that include a suggestion to discuss the risks with friends and family members who may be vulnerable. PSPs may further consider introducing payment limits or geo-blocking features as common with card payments. The restrictions could by default depend on customer profile, but still be configurable for the individual.

Same as with phishing, the service provider's "central monitoring" may find a transaction "suspicious", put it on hold and request customer reconfirmation via a secure out-of-band channel. Whenever a payment service user is prompted to approve or confirm a payment, the transaction data - especially amount and payee - must be clearly displayed on the user's device, supporting the user in better identifying certain APP scams. Certain countries like the Netherlands or the UK have established or are establishing "Confirmation of Payee" services. When a payer wants to make a payment, they may enter on their device (e.g. mobile phone) not just the account number, but also the name of the beneficiary. The payer's PSP than first validates the match between the account number and the beneficiary's name with the beneficiary's PSP or a common service acting for that PSP. If there is no match, the payer is informed and may decide not to

proceed with the payment. Certain types of fraud - especially invoice fraud - can specifically be countered by such a service.

3.2.5 Final Considerations/Conclusions

The strengthening of authentication methods due to PSD2 (requiring SCA with dynamic linking) (see [6] and [9]) and the general move towards mobile authenticators no more exposing any codes to the users will make it more difficult for fraudsters to run pure phishing attacks. However, the change may not happen overnight, which is why countermeasures should be maintained.

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 or limit attack impacts through introducing payment restrictions. However, social engineering remains an important attack factor which is further increasing – notably in relation to APP fraud - targeting not only individual customers but also CEOs / presidents of large companies. It is often used as an enabler for other types of attacks and is applied in the mobile world as well. Therefore appropriate education about social engineering remains a crucial factor to combat both phishing and APP scams.

3.3 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, to steal data, to bypass access controls, and to cause harm to host computers, customer devices and their applications or data.

3.3.1 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 users, serving them with pop-up ads when connected to the Internet. Based on the same approach, attackers are installing malware (Banking Trojan) targeting the victim while using e- or m-banking services. Banking Trojans are capable of hijacking the browser and tampering financial transactions or stealing user credentials during the use of e- or m-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 (APTs)

Another important category of malicious software is the one that is being abstractly described as Advance Persistent Threat. The reader is referred to Section 3.4 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 APTs (see Section 3.4) to bypass strong authentication and get access to important data.

Fileless malware (also known as non-malware)

Fileless malware is a malicious code that does not need a file or script in order to operate. It takes advantage of existing vulnerabilities on the machine, especially of Powershell and Windows Management Instrumentation (WMI). It exists exclusively in a computer's RAM and uses system tools to inject malicious code into trusted processes, such as javaw.exe or iexplorer.exe.

Fileless malware is more difficult to prevent, detect and remove, as it does not leave a file for an antivirus software to detect. Hackers can steal data or install other forms of malware to give it persistence, or hide it in some other trusted processes or even in the Windows Registry. This way, it can set up scripts that run when the system restarts to continue the attack.

Fileless malware:

- Has no code or signature to detect. It does not have a particular behaviour, so heuristics cannot detect it either.
- Uses processes that are native to the operating system in order to carry out the attack.
- Lives in a computer's RAM.

3.3.2 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 webpages. As making payments through mobile applications grows in popularity, there is also an increase in 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 3.2).

The most important and persistent banking malware is Emotet. It started as a Banking Trojan used to extract financial data, but it quickly evolved as a global threat to its victims, and it can also act as a door opener on a computer which prepares it for further infections. It was first detected in 2014 and it still remains one of the most important malware nowadays. Emotet is polymorphic, which means it can change itself every time it is downloaded, evading signature-based detection. The infection may arrive either via malicious script, macro-enabled document files, or malicious link or it can be spread from one infected computer to another through its worm-like capabilities. Emotet is also capable of copying numerous passwords stored on the computer, or it can be used to send spam. All these functions are built as different modules that can be started on any computer by the Command & Control (C&C) server, which detects which modules (functions) should be activated depending on the data found during the infection.

Finally, ATM malware threats are still affecting and evolve. More details are provided in Section 4.3.

3.3.3 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[11] ransomware malware strain gained infamy by crippling entire networks, across more than 150 countries, with hundreds of thousands of Windows computers infected.

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.

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

According to the Proofpoint Q1 2019 Threat Report[12]. There is clearly a shift, in 2018 and in the first months of 2019, of the type of attack that Emotet is involved in, shifting from a Banking Trojan to a botnet. This has to be considered in order to better understand all the increases in this area, as Emotet remains one of the most important attacks in the industry, namely 27% of all detected attacks.

Considering the type of vector involved in the attacks; in email attacks, URLs outnumbered attachments by roughly 5 to 1 for Q1 2019 and banking Trojans decreased to 21% of malicious payloads in email. In this type of attacks, Emotet has increased up to over 60% of the attacks. The word "Payment" jumped to the top subject line in email fraud attacks, up 6 percentage points from Q4 2018. Regarding web-based attacks, Coinhive samples have spiked from Q4 2018 to Q1 2019, but have drastically dropped since it closed in March 2019. Finally, it is worth noting that domain fraud has increased over three times, offering SSL and SSL certificate as legitimate domains and thus giving a false sense of security.

For 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 it 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- or m-banking (mobile and web), credit card credentials are of similarly 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.

3.3.4 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 do 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.

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.

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

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"[13].

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[14], 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.

3.3.5 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

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

[14] 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.

new security technologies, such as the Advanced Threat Protection ones, for combating state-of-the-art and 0-day malware attacks, including ransomware.

3.4 Advanced Persistent Threats (APTs)

3.4.1 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[15].

The term APT originated in the U.S. Department of Defense late in the first decade of the 21st century to describe cyberespionage efforts by China against American national security interests.[16]

APTs, according to Symantec's detailed report on the subject[17], 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 for 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, fraudulent financial scams with large amounts of money, 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 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, defense 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 and financial institutions managing their

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

[16] https://www.britannica.com/topic/advanced-persistent-threat

[17] 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 above.

clients' valuable assets 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.

3.4.2 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?[18]

Stage 1: Target selection

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.

The aim of the APT attack is to gain access to sensitive information and data. Targets are selected based on data required or data of choice. The sensitivity of the data and its economical worth is taking into account. A large number of organisations possess data that would be of very high financial and economic value.

Stage 2: Information gathering

The attacker after narrowing down the target organisation collects information about the target of choice. The information extracted at this point is very vital for the success of the attack. At this point the weakest link is taken into account, which has been proven to be the human factor. Many organisations adopt high security standards however, with a human present in the functioning of the system poses vulnerability in that organisation.

The process used in gathering the information is referred to as 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.

Stage 3: Gaining access

The information-gathering phase points the attacker to possible areas for intrusion. This phase is where the attacker gains access to the organisation. At this point a malware, usually a zero-day, is used to penetrate the organisation's network. This phase deals with using the information gathered from the reconnaissance phase to penetrate through the target organisation's defenses mostly through utilising malware deliveries. Besides gaining access through the deployment of a zero-day, there also exist alternative ways of gaining unauthorised access. The method used in gaining access depends greatly on the outcome of the reconnaissance phase.

[18] See international Journal of Information Security Science, Evaluating Advanced Persistent Threats Mitigation Effects: A Review, Article – February 2019, Oluwasegun Adelaiye, Aminat Ajibola, Silas Faki

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.

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.

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.

Stage 4: Exploitation

Exploitation is the stage after a malicious application has been used to gain access usually through a zero-day malware. It establishes a connection with a C&C server, which bypasses security by utilizing secure ports such as port 443, using legitimate tools and services to reduce suspicion and possible detection. Furthermore, it provides full exploitation of the organisation's network as commands can be issued from a remote location to the target organisation's information systems.

The C&C server is responsible for upgrading and updating the malware for better performance as well as issuing commands to compromised systems. Fast-flux DNS is a technique also adopted by a C&C server to aid in avoiding detection. This method prevents existing defense systems from detecting any unusual traffic to or from a single destination.

Stage 5: Operation

When a connection is established and secured with the C&C server, the earlier deployed malware tries to spread to other machines within the network firstly by scanning for vulnerable systems. The attacker through the C&C server uses this method to gain access to a system with highly valuable information.

This stage involves some internal reconnaissance to aid in locating confidential data being sought after. At this point the detection of an intrusion in the system becomes very difficult. The malware at this point continuously mutates and changes its location, which aids the malware in easily evading detection.

The attacker also evades detection by using off-the-shelf products, exploiting existing features in operating systems and ultimately stealing access credentials and escalating privileges of highly confidential systems.

Stage 6: Data discovery and collection

Lateral movement of the malicious content around the organisation creates a channel to transmit data out of the organisation. At this point data of high value is located and collected to a single or fewer locations for easy exfiltration of the data out of the organisation and to a remote location.

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.

A more detailed description of this stage's characteristics follows:

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.

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. C&C servers may covertly seize control of target systems and even destroy them depending on the APT's game plan.

Stage 7: Data Exfiltration

The ultimate purpose of an APT is to gain access to valuable highly confidential information. This stage marks the end of the attack process and is the point where the attacker gets or changes/creates (i.e. SWIFT attack) the desired information. The data is usually transferred using secured channels majorly SSL/TLS to evade detection and to hide the transmission process.

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

The losses at this point include data loss leading to loss of finances, customer data, access rights, intellectual property, trade secrets, intelligence information and other sensitive and vital information.[19]

Data transmission - Following C&C 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 manoeuvres.

Recognising an APT[20]

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.

Increase in elevated logons 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 logons occurs 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.

---

[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 above.

[20] 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 above.

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 exfiltrated data leak will be missed.

Of course, to detect a possible APT, the IT 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 a company.

Focused spear-phishing campaigns
One of the best indicators of an APT attack, it would be focused spear-phishing email campaigns against a company's employees using document files (e.g., Adobe Acrobat PDFs, Microsoft Office Word, Microsoft Office Excel XLS, or Microsoft Office PowerPoint PPTs) 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.

3.4.3 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, targeting financial institutions. Although parties like Europol and Interpol have done proper jobs with arresting gang members, criminal organisations such as Cobalt and Carbanak have been very active in 2018 attacking financial institutions. Cobalt, spreading SpicyOmelette malware in campaigns targeting financial institutions worldwide have been connected to the theft of millions of dollars and is believed to have caused over €1bn in damages. Carbanak alone is claimed to have managed to steal at least $1bn from banks worldwide. Modus operandi from these gangs varies by doing field research on the financial institutions to spear phishing on staff members with email 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 ATMs of financial institutions or changing the balance of cards to unlimited.

The FireEye Threat Intelligence Research Team in its "M-Trends 2019" Special Report[21] promoted two North Korean attack groups (APT37 also known as "Reaper" and APT38) to APT status.

APT37 has likely been active since 2012 and targets public and private sectors. Although it primarily targeted organisations in South Korea, starting in 2017, APT37 expanded the scope and sophistication of its operations in 2018, including leveraging zero-day vulnerabilities and wiper malware. Moreover, it expanded its targeting beyond the Korean peninsula into Japan, Vietnam and the Middle East. This expansion also revealed a wider range of targeted industry verticals including chemicals, electronics, manufacturing, aerospace, automotive and health care entities.

APT38 is a financially motivated group linked to North Korean cyber espionage operators, renowned for its attempt to steal hundreds of millions of dollars from financial institutions through the brazen use of destructive malware. APT38 executes sophisticated bank heists that typically feature long planning, extended periods of access to victim environments preceding any attempts to steal money, fluency across mixed operating systems, the use of custom developed tools and constant effort to thwart investigations capped with a willingness to destroy compromised machines. APT38 has compromised more than 16 organisations in at least 13 different countries, sometimes simultaneously, since at least 2014. Victimised organisations tend to be in developing economic regions. Although APT38 focuses almost exclusively on the financial sector, its bank heists are reminiscent of sophisticated espionage campaigns. APT38 continues to conduct phishing activity against Bitcoin and other cryptocurrency-related financial services.

Another APT group "Lazarus" is linked to the Redbanc cyberattack. The attack involved PowerRatankba, a malware toolkit with ties to the APT group. "It represents the latest known example of Lazarus-affiliated tools being deployed within financially motivated activity targeted toward financial institutions in Latin America", FlashPoint researchers said in a blog post[22]. The intrusion reportedly occurred when the malware was delivered via a trusted Redbanc IT professional who clicked a link to apply for a job opening found through social media. The

[21] See https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

[22] See https://www.flashpoint-intel.com/blog/disclosure-chilean-redbanc-intrusion-lazarus-ties/

applicant was ultimately and unwittingly tricked into executing the payload, researchers said. "Lazarus attacks appear to reportedly rely on social media and trusted relationships, which may elevate their abilities to execute and install their payloads," the post said. "As such, security awareness training—especially that which pertains to social media and social engineering—is also recommended."

The APT group OilRig, also known as APT34, which has been in operation since at least 2016, remains a significant threat to governments and businesses. And while not as sophisticated as some other APT groups, researchers at Palo Alto Network's Unit 42 report[23] that "OilRig has been prolific, stealing about 13,000 credentials over the last three years, spreading out from the Middle East to other parts of the globe, and deploying a number of malicious tools, including over 100 web shells for creating backdoors and communicating with compromised systems across 27 countries, 97 organisations and 18 industries".

Researchers from ESET in 2018 released a report[24] analysing an APT group called GreyEnergy which they consider the successor of BlackEnergy. These researchers' analysis of the previously undocumented malware shows it has been used in targeted attacks against energy companies and other critical infrastructure organisations in Central and Eastern Europe. Whereas BlackEnergy is known for the disruptive 2015 attack on the Ukrainian power grid that cut power for roughly 225,000 people, GreyEnergy has to date preferred reconnaissance and espionage, according to ESET. The group has taken screenshots of its possible targets, stolen credentials, and exfiltrated files. GreyEnergy uses two main infection vectors. One is compromising public-facing web servers connected to an internal network and the other is spear phishing emails with malicious attachments. Once initial network mapping has been accomplished, the attackers then deploy the main malware and, often, several internal C&C proxies within the victims' networks to redirect requests from infected nodes inside the network to an external C&C server on the internet. The malware has been built as a modular framework that can adjust to different target infrastructures. Each module, including the main GreyEnergy module and accepts text commands with various parameters. The authors have created several attack modules almost completely devoted to reconnaissance and information collection.

GootKit is a notable APT[25] example for its evasiveness and the stealthy way it steals confidential data and sends it back to the operators of its 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.

3.4.4 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 defenses (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 defense-in-depth strategy and architecture, to protect enterprises from attacks of this complexity. The traditional

[23] See https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/

[24] See https://www.eset.com/int/greyenergy-exposed/

[25] See e.g. https://www.sentinelone.com/blog/gootkit-banking-trojan-deep-dive-anti-analysis-features/

defense-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 defiance 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 during 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 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 utilising 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 recognise signs that something appears out of place. IT security managers need to look for patterns of events characteristic of APT methodologies. There are many proposed methods for mitigating APT, a few common methods and the statistics classifying the methods employed by 25 researchers are highlighted in the following table:

No.	Mitigation Techniques	Percent
1	Traffic/ Data analysis	30%
2	Pattern Recognition	21%
3	Anomaly Detection	16%
4	Awareness	7%
5	Whitelists	5%
6	Cryptography	5%
7	Multi-layer security	5%
8	Blacklists	3%

9	Deception	2%
10	SIEM	2%
11	Intrusion Detection System (IDS)	2%
12	Risk assessment	2%

Table 4 Overview mitigation techniques used against APT attacks

User and Entity Behaviour Analytics (UEBA) is a new approach in uncovering APTs. UEBA is increasingly employing artificial intelligence (AI), to monitor and to analyse how users interact with an organisation's IT systems and to detect when these users engage in anomalous behaviour, often a sign that their accounts were hacked and an attacker has infiltrated the network.

Tools such as a SIEM 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.

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 exfiltrate valuable data, security researchers gather valuable information about the methods they use, including insights into an attacker's kill chain, and adjust their network defenses accordingly.

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 defenses 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 given operational environment and validate security defenses 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.

[26] https://www.ossec.net/

To support the cybersecurity professionals in their fight against Advanced Targeted Attacks, known as ATAs, Gartner has developed the Five Styles of Advanced Threat Defense Framework[27], 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 Analyzer 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 ATAs defense.

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.

3.4.5 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 criminals involved, 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 utilizing 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 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 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

[27] https://www.gartner.com/en/documents/2576720/five-styles-of-advanced-threat-defense

of us as the threat landscape evolves, learning to detect – and stop - even the most advanced threats is paramount.

3.5 Mobile device related attacks

The digital revolution is causing businesses to operate and endeavour outside the safety of corporate perimeters into the open internet where they can provide more frequent and more meaningful services to customers, partners and employees. Unfortunately, this also makes them a target for a new breed of attackers that align internet-scale threats with their digital attack surface. A significant portion of this attack surface is the mobile channel. Client assets outside the firewall protection, discovered by hackers in mobile devices are at risk, as they research their next threat campaigns.

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.

In 2018, mobile apps were downloaded onto user devices over 205 billion times.[28] Data by Marketing Land[29] indicates that 57% of total digital media time is spent on smartphones and tablets. More often than not, our daily lives depend on apps for instant messaging, online banking, business functions, and mobile account management. According to Juniper Research, the number of people using mobile banking apps is approaching two billion—around 40% of the world's adult population.[30] According to Wandera "Mobile Threat Landscape 2019" the number of mobile phone users in the world was predicted to pass the 4.7 billion mark by 2019, so it comes as no surprise that mobile is now the focal point of attacks.[31]

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 technology, peer-to-peer payment apps and others[32].

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.

According to PT Security "Mobile-Application-Vulnerabilities-and-Threats-2019"[33]:

[28] https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

[29] https://marketingland.com/report-50-digital-media-time-now-spent-within-five-mobile-apps-222543

[30] https://www.juniperresearch.com/press/press-releases/digital-banking-users-to-reach-2-billion

[31] https://www.wandera.com/mobile-security/mobile-threat-landscape/

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

[33] https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

- High-risk vulnerabilities were found in 38% of mobile applications for iOS and in 43% of Android applications.
- Most security issues are found on both platforms. Insecure data storage is the most common issue, found in 76% of mobile applications. Passwords, financial information, personal data, and correspondence are at risk.
- Hackers seldom need physical access to a smartphone to steal data: 89% of vulnerabilities can be exploited using malware.
- Most cases are caused by weaknesses in security mechanisms (74% and 57% for iOS and Android apps, respectively, and 42% for server-side components). Because such vulnerabilities creep in during the design stage, fixing them requires significant changes to code.
- Risks do not necessarily result from any one particular vulnerability on the client or server side. In many cases, they are the product of several seemingly small deficiencies in various parts of the mobile application.
- Many cyberattacks rely on user inattention. Escalated privileges or side-loaded software can pave the way for a damaging attack.

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[34]);
- To make person to person (P2P)[35] 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;

[34] 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)).

[35] 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.

- 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 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;
- Weaknesses in the implementation of biometrics as customer verification;
- Smishing SMS messages to people purporting to be from a trusted source (e.g. a PSP) 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 (including mobile applications and mobile wallets) and SIM swap-based attacks.

3.5.1 Attacks Targeting the Mobile Device

3.5.1.1 Impact & Context

Mobile security is at the top of every company's worry list these days — and for good reason: 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 average cost of a corporate data breach stands at $3.86 million, according to a 2018 report by the Ponemon Institute. That's 6.4% more than the estimated cost just one year earlier.[36]

In the first semester of 2019[37] researchers at Check Point Software Technologies discovered that mobile malware dubbed Agent Smith has infected about 25 million devices, mainly in India and other Asian countries. Other counties have also been affected, including the UK, Australia and the US. The malware exploits known Android vulnerabilities and automatically replaces installed apps – such as WhatsApp – with malicious versions without users' knowledge or interaction. It then shows fraudulent ads to device owners, earning money for the cyber criminals behind the malware campaign. The researchers have advised mobile users to uninstall any apps they suspect may be malicious.[38]

The "Data Breach Industry Forecast 2019" report by Experian[39] predicts that "A major wireless carrier will be attacked with a simultaneous effect on both iPhones and Android, stealing personal information from millions of consumers and possibly disabling all wireless communications in the United States".

A CBC news investigation[40] even showed how easy it was for hackers to gain access to a phone through the wireless carrier. The attack penetrated Signalling System No. 7 (SS7), a layering system that allows for phone, data, and billing connections. The investigation was able to track an individual phone's location and access the contents just by having the phone number. This incident shows that the wireless environment is vulnerable.

[36] https://www.csoonline.com/article/3241727/7-mobile-security-threats-you-should-take-seriously-in-2019.html

[37] https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/

[38] https://www.computerweekly.com/news/252466494/Agent-Smith-mobile-malware-hits-millions-of-devices

[39] https://www.experian.com/assets/data-breach/white-papers/2019-experian-data-breach-industry-forecast.pdf

[40] https://www.cbc.ca/news/politics/dube-cellphone-hack-cse-1.4628491

Google has enjoyed a long history of providing software that is aimed at protecting customers online. Google's program for eradicating online threats involves the use of both manual and automatic scanners to trawl the internet to locate websites involved in phishing or malware activities.

Wandera's threat research team has discovered a disparity between the protections available within Google's desktop browser versus its mobile browser.

Google Safe Browsing provides a service to check URLs against Google's lists of unsafe web resources. According to Google, the service is updated constantly and functions as a warning system within browsers to alert users when they navigate to URLs that may contain malicious content.

Over a period of eight months, Wandera's threat research team repeatedly found that URLs, that were being flagged as 'deceptive sites' when opened through the Google Chrome desktop browser, were not identified as malicious on the Chrome mobile app. The technologies used in endpoint security solutions are often limited by the functionality of the endpoint operating system. In the case of mobile, the OS vendors limit the amount of memory and system resources thus restricting the threat intelligence that can be applied to network-based threats.

Additionally, endpoint-based security solutions are dependent on pre-packaged threat intelligence that is by definition static and therefore limited in efficacy.[41]

On smartphones, Android has the largest market share worldwide; about 85% compared to iOS's 15%. Because of that, Android is the #1 smartphone target for hackers and criminals.

A research, carried out by Pulse Secure, found that 97% of malicious mobile malware targets the Android operating system[42]. Malware targeting Android devices dominates mobile malware. The research drew on data collected from more than 2.5 million mobile applications. While Android suffered an attack from hackers, iOS users came off relatively unharmed. However, the report's authors warned that iOS threats were growing, despite only four attacks targeting jailbroken versions of Apple's mobile operating system.

On the iOS front, iOS app developers are taking shortcuts on security. Despite developers having a mandate from Apple to build end-to-end encryption into their apps, a high number of apps do not. Apple even offers a feature that helps developers comply with data privacy requirements, and Wandera's research data of June 2019 shows that this is not being used properly. To understand how app developers are using (or not using) encryption, Wandera's security researchers analysed over 30,000 of the iOS apps most commonly used by employees and found that more than two-thirds of apps do not use this feature to encrypt data[43].

A vulnerability recently discovered in Facebook's popular messaging service, WhatsApp, in both the Android and iOS operating systems, allows attackers to install spyware on a device simply by making a WhatsApp call. The spyware, known as Pegasus, was created by the NSO Group[44] and it gives attackers access to a substantial amount of data on an infected device, as well as control of the camera and microphone. Beyond updating the app to remedy this issue, how can businesses brace themselves for the next big mobile vulnerability?

---

[41] https://www.wandera.com/mobile-security/google-safe-browsing/

[42] https://www.pulsesecure.net/download/pages/2819/

[43] https://www.wandera.com/mobile-security/ios-app-developer-security-shortcuts/

[44] See https://www.nsogroup.com/

The recent WhatsApp vulnerability is alarmingly simple on the surface: it allows an attacker to install spyware on a device by making a WhatsApp call, and the victim does not even need to answer the call. Once installed, this spyware can:

- Turn on a phone's camera and microphone
- Scan emails and messages
- Collect a user's GPS location data

According to Wandera's VP of Engineering, Mike Campin, this new type of attack is deeply worrying, given WhatsApp's global popularity among more than 1.5 billion users.[45]

"While WhatsApp is not typically used as an official corporate messaging application, it is used widely internationally on employees' personal devices as well as on corporate-issued devices," Campin said. "And once exploited via this new attack, the attacker has complete control and visibility of all data on the phone."

Fixes were rolled out in the form of app updates through the Apple App Store and Google Play store, the story received ample press coverage, and Wandera informed its clients of the vulnerability along with steps to remedy it.

However, an analysis by Wandera's threat research team showed that numerous devices across our global customer portfolio were still running vulnerable versions of WhatsApp several weeks after the vulnerability was discovered.

While this vulnerability has attracted much attention recently, it is only the latest reminder that IT teams and users alike need to stay vigilant when it comes to mobile threats.

New mobile vulnerabilities come to light so frequently that security teams cannot wait for developers to fix each issue. By the time a vulnerability is discovered and remedied, hackers have often had a substantial window to carry out attacks and exfiltrate corporate data.

RiskIQ discovered that after three consecutive quarters of decline in 2018, Q1 in 2019 showed a nearly 15% increase in blacklisted apps over Q4 of 2018. In Q1 of 2019 the blacklisted apps rose 14.5% from 37,592 to 43,049, accounting for nearly 2% of all apps.[46]

The more realistic mobile security hazards, lie in the following easily overlooked areas, all of which are only expected to become more pressing in the future according to CSO[47]:

Data Leakage

Most mobile applications contain at least some programming flaws that make them susceptible to leaking data containing personal information. Mobile applications distributed in Apple's App Store and Google Play Store are more likely to have at least one hidden bug that can compromise privacy than they are of containing a security vulnerability, according to a recent study.[48]

Mobile software penetration testing provider *NowSecure* determined in that recent study that 90% of applications in the U.S., portions of those marketplaces could potentially leak one or more pieces of personal information.

---

[45] https://www.wandera.com/mobile-security/whatsapp-spyware-whats-next/

[46] https://www.riskiq.com/research/q1-2019-mobile-threat-landscape-report/

[47] https://www.csoonline.com/article/3241727/7-mobile-security-threats-you-should-take-seriously-in-2019.html?page=2

[48] https://www.nowsecure.com/blog/2019/06/06/test-of-250-popular-android-mobile-apps-reveal-that-70-leak-sensitive-personal-data/?utm_source=press&utm_medium=referral

A test of 250 popular Android mobile apps revealed that 70% leak sensitive personal data.[49] The analysis found that personal data can leak within the confines of the device itself, to another application or in a file over a network that a hacker can intercept. *NowSecure* conducted the privacy assessment in the second quarter of 2019, after it added the ability to scan for potential GDPR violations to its mobile app testing engine. The spectre of leaking personally identifiable information (PII) could put an organisation at risk of violating GDPR, though it does not mean such a violation will or has occurred.[50]

Social engineering

Despite the ease with which one would think social engineering cons could be avoided, they remain astonishingly effective. A staggering 91% of cyber-crime starts with email, according to a 2018 report[51]. The firm refers to such incidents as "malware-less attacks," since they rely on tactics like impersonation to trick people into clicking dangerous links or providing sensitive info. Phishing, specifically, grew by 65% over the course of 2017, the company says, and mobile users are at the greatest risk of falling for it because of the way many mobile email clients display only a sender's name — making it especially easy to spoof messages and trick a person into thinking an email is from someone they know or trust.

In fact, users are three times more likely to respond to a phishing attack on a mobile device than a desktop, according to an IBM study[52]— in part simply because a phone is where people are most likely to first see a message. While only 4% of users actually click on phishing-related links, according to Verizon's 2018 Data Breach Investigations Report[53], those users tend to be repeat offenders: The company notes that the more times someone has clicked on a phishing campaign link, the more likely they are to do it again in the future. Verizon has previously reported that 15% of users who are successfully phished will be phished at least one more time *within the same year*.

Robinson, an information security and anti-phishing strategist, notes that the line between work and personal computing is also continuing to blur[54]. 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 does not seem at all unusual on the surface, even if it may in fact be malicious.

Wi-Fi interference

A mobile device is only as secure as the network through which it transmits 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 research by enterprise security firm Wandera[55], corporate mobile devices use WiFi almost three times as much as they use cellular data. Nearly a quarter of devices have connected

[49] https://www.nowsecure.com/blog/2019/06/06/test-of-250-popular-android-mobile-apps-reveal-that-70-leak-sensitive-personal-data/?utm_source=press&utm_medium=referral

[50] https://sdtimes.com/mobile/chances-of-data-leaks-are-high-in-mobile-apps/

[51] https://www.fireeye.com/offers/rpt-email-threat-report.html

[52] https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-wp-us.pdf

[53] https://enterprise.verizon.com/resources/reports/2018/DBIR_2018_Report.pdf

[54] https://www.computerworld.co.nz/article/631214/5-mobile-security-threats-should-take-seriously-2018/

[55] https://www.thethreatreport.com/5-mobile-security-threats-to-be-taken-seriously-in-2019/

to open and potentially insecure WiFi networks, and 4% of devices have encountered a man-in-the-middle attack — in which someone maliciously intercepts communication between two parties — in 2019. McAfee[56], meanwhile, says network spoofing has increased "dramatically" and yet less than half of people bother to secure their connection while traveling and are relying on public networks.

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 embarrassingly ineffective at keeping their products up to date — both with operating system (OS) updates and with the smaller monthly security patches between them — as well as with IoT devices, many of which are not even designed to get updates in the first place.

Increased likelihood of attack aside, an extensive use of mobile platforms elevates the overall cost of a data breach, according to Ponemon[57], and an abundance of work-connected IoT products only causes that figure to climb further. The Internet of Things is "an open door," according to cybersecurity firm Raytheon[58], whose sponsored research is showing that 82% of IT professionals predicted that unsecured IoT devices would cause a data breach — likely "catastrophic" — within their organisation.

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 chaotic, it falls upon a company to create their own security net around them.

Cryptojacking attacks

A relatively new addition to the list of relevant mobile threats, cryptojacking is a type of attack where someone uses a device to mine for cryptocurrency without the owner's knowledge. The cryptomining process uses the company's devices for someone else's gain. It leans heavily on the company's technology to do it — which means affected phones will probably experience poor battery life and could even suffer from damage due to overheating components.

While cryptojacking originated on the desktop, it saw a surge on mobile from late 2017 through the early part of 2018. Unwanted cryptocurrency mining made up a third of all attacks in the first half of 2018, according to a Skybox Security analysis[59], with a 70% increase in prominence during that time compared to the previous half-year period. And mobile-specific cryptojacking attacks absolutely exploded between October and November of 2017, when the number of mobile devices affected saw a 287% surge, according to a Wandera report[60].

Since then, cryptocurrency attacks have decreased slightly, especially in the mobile domain — a move aided largely by the banning of cryptocurrency mining apps from both Apple's iOS App Store and the Android-associated Google Play Store in June and July 2018, respectively. Still, security

[56] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf

[57] https://databreachcalculator.mybluemix.net/

[58] https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf

[59] https://lp.skyboxsecurity.com/WICD-2018-07-Report-VT-Trends-MY_03Asset.html

[60] https://www.wandera.com/mobile-security/cryptojacking/cryptojacking-mobile-threat/

firms note that attacks continue to see some level of success via mobile websites (or even just rogue ads on mobile websites) and through apps downloaded from unofficial third-party markets.

Poor password hygiene

Users are still not securing their accounts properly — and when they are carrying phones that contain both company accounts *and* personal sign-ons, this can be particularly problematic.

A recent survey by Google and Harris Poll[61] found just over half of Americans, based on the survey's sample, reuse passwords across multiple accounts. Equally concerning, nearly a third are not using two-factor authentication (or do not even *know* if they are using it — which might be a little worse). And only a quarter of people are actively using a password manager, which suggests the vast majority of users probably do not have particularly strong passwords in most places, since they are presumably generating and remembering them on their own.

Things only get worse from there: According to a 2018 LasPass analysis[62], a full half of professionals use the same passwords for both work and personal accounts. And if *that* isn't enough, an average employee shares about six passwords with a co-worker over the course of his or her employment, the analysis found.

In 2017, Verizon found[63] that weak or stolen passwords were to blame for more than 80% of hacking-related breaches in businesses. From a mobile device in particular — where workers want to sign in quickly to various apps, sites, and services — the risk to the organisation's data increases if even just one person is carelessly typing in the same password they use for a company account into a prompt on a random retail site, chat app, or message forum. Now combine *that* risk with the aforementioned risk of Wi-Fi interference, multiply it by the total number of employees in the workplace, and think about the layers of likely exposure points that are rapidly adding up.

Physical device breaches

A lost or unattended device can be a major security risk, especially if it does not have a strong PIN or password and full data encryption.

In a 2016 Ponemon study[64], 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 did not use encryption. Also 68% of respondents indicated they sometimes shared passwords across personal and work accounts accessed via their mobile devices.

The message is simple: Leaving the responsibility in users' hands is a risk. Appropriate policies should be prepared and enforced.[65]

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.

---

[61] http://services.google.com/fh/files/blogs/google_security_infographic.pdf

[62] https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/IAM_LastPass_SOTP_ebook.pdf

[63] https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/

[64] https://www.ponemon.org/local/upload/file/How%20much%20is%20the%20data%20on%20your%20mobile%20device%20worth%20Final%2010.pdf

[65] https://www.csoonline.com/article/3241727/7-mobile-security-threats-you-should-take-seriously-in-2019.html?page=2

According to 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[66].

The key finding of the "2019 Mobile Threat Landscape Report: A Comprehensive Review of Mobile Malware Trends" by CrowdStike[67] provides an overview of the key types of mobile malware observed in 2019, along with their typical deployment mechanisms. They read as follows:

- The targeting of mobile platforms is increasingly being adopted by a range of criminal and targeted intrusion adversaries.
- Malware targeting mobile banking is likely to remain prolific, supported by an active underground industry of developers operating mobile "malware-as-a-service" subscription models to complement their desktop offerings.
- Targeted adversary groups continue to develop mobile malware variants, typically as ports of established malware families. Development capability has proliferated to less-skilled groups due to the accessibility of proof-of-concept mobile malware variants.
- Mobile malware running on the Android operating system is the most prevalent at this time, driven by the ease of installing new applications from third-party sources.
- The current maturity level of mobile security solutions lags behind that of traditional platforms, leading to longer potential attacker dwell times on compromised mobile devices.

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 exist 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, in the hope that the

[66] McAfee Mobile Threat Report Q1, 2018 - https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf

[67] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

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.

A popular method for forcing users into installing malicious applications is by sending them links to APK files[68] hosted on attacker-controlled websites, normally achieved through either SMS or email spam messages sent to large groups of targets.

Users should be wary of messages being delivered by SMS or email that prompt them to install applications from untrusted sources, because this mechanism is often used by attackers to trick their targets into installing mobile malware.

Fake enrolment to mobile authentication/payment app

Whereas the secure and correctly enrolled mobile authentication/payment app may be hard to attack, the enrolment procedure itself may be weaker and therefore become the preferred target for the fraudster in the future. The enrolment may require information that can be phished or vished or depend upon approvals by the victim, who may be persuaded to "approve" by some sort of scam. If so, the fraudster may be able to impersonate a legitimate user during the enrolment procedure and get in control of a mobile authentication/payment app that could result not just into one, but many fraudulent transactions.

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.

- Poor application and OS 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:

[68] Android Package (APK) is the package file format used by the Android operating system for distribution and installation of mobile apps and middleware. Victims might be prompted to click an SMS link to a spoofed banking site designed to look trustworthy and convince the victim to "update your banking app". The update would then install the malicious app (code), thereby allowing the attacker to gain access and collect credentials.

- 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 3.2 – Phishing), 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 (this even could include a forced consent since the app would not run without this permission). 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 security 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.
- Biometric authentication:
  - Numerous studies and frauds have shown that biometric authentication in payments without a second factor can be weak and result in fraud, especially if the fraudster can physically access 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 3.5.2) 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 can be cloned, 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.

3.5.1.2 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 jailbreak or root your 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.

Mobile payment service providers should:

- Create awareness campaigns to educate consumers on how to avoid the previous explained fraud scenarios;
- Monitor app stores and Internet for fake applications;
- Implement anti-tampering and integrity controls in app;
- Reject app installation on jail-broken or rooted devices;
- Protect app code with code signing and 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 (such as certificate pinning) to ensure an app will only communicate with a trusted party;
- Implement app as personalised and prevent transfer of personalised app to another device;
- Implement device owner/user verification as well as mobile device verification;
- Use always two-factor authentication, which should be implemented in a user-friendly way;
- Establish secure mobile payment app enrolment procedures, which cannot be circumvented by vishing and/or other social engineering scams.

3.5.2 SIM swapping

3.5.2.1 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 providing flexibility to consumers for 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.

SIM swap fraud happens when fraudsters transfer a customer's mobile number to a fraudster's SIM. Fraudsters then takeover customer accounts and carry out fraud.

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 the customer's 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.

SIM swap fraud detection identifies suspicious SIM swaps. It ranks the risk of a SIM swap based on location, device type and customer behaviour. Different risk levels trigger different corrective actions. Actions like blocking transactions, locking accounts, or sending customer communications.

3.5.2.2 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.

Although it is very difficult to obtain accurate figures on fraud committed in part through the use of exploiting weaknesses in the SIM swapping process, according to Yahoo finance in May 2019, the U.S. Department of Justice charged nine "SIM swapping" attackers for stealing 2.5 million $.[69]

As stated in the 15-count indictment unsealed, five Americans and an Irishman related to "The Community" hacking group are charged with conspiracy to commit wire fraud, as well as aggravated identity theft. On successful SIM swapping, "The Community" attackers used their victims' phone numbers to reset passwords and gain access to their online accounts—including email, cloud storage, and cryptocurrency exchange accounts and wallets—using verification codes and two-factor authentication codes received on those numbers.

In total, the defendants executed seven SIM swapping attacks to steal the victims' funds from their cryptocurrency exchange wallets, transferring approximately 2.5 million $ worth of cryptocurrency to wallets controlled by the hacking group.

Meanwhile, in January 2019, a 21-year old American was accused of stealing almost 24 million $ in crypto via SIM swapping. And in February 2019, a New York resident was indicted in what constituted the jurisdiction's first SIM-swapping prosecution.[70]

3.5.2.3 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;
- Keep personal details that would be useful to a fraudster, i.e. phone number, date of birth etc. off social media sites;

[69] https://thehackernews.com/2019/05/sim-swapping-hacking.html

[70] https://finance.yahoo.com/news/us-doj-charges-group-individuals

- Ask your mobile payment service provider to give you details of every financial transaction through two channels - for instance, SMS as well as email alerts.

In addition, a mobile payment service provider can negotiate with the mobile operators that they are 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[71], 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.

3.5.3 Final Considerations/Conclusions

Consumers spend increasingly more time on Internet and mobile every day and the smartphone constitutes an immediate reliable channel between the PSP and their 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 the payment industry 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 PSP. 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[72].

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).

---

[71] 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

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

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 has 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.

3.6 Denial of Service

3.6.1 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, trends in DDoS are remarkably stable. The sizes of the largest attacks have grown by approximately 6% on an annual basis, with occasional outliers like the Mirai botnet. By the end of 2018, a number of booters have been taken down.

3.6.2 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. Patches are sometimes available without consumers being aware of them.

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 firewalls. 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.

3.6.3 Impact & Context

In 2018 there has been a number of very large-scale attacks on non-PSPs. In March 2018 a memcached[73] amplification attack broke a new DDoS record at 1.7 Tb/s. As far as the available reports indicate, this is the largest attack to date.

When people think of DDoS attacks, they focus on the outliers, the massive Terabit attacks that generate headlines. But the smaller, more focused attacks can do just as much damage. More importantly, these smaller attacks are actually more common than their larger-scaled counterparts. The attacks mentioned above were possible, because of the fact that many IoT devices were infected. Akamai reported[74] that between January 2017 and January 2018, DDoS attack density grew 39.8%, from 560 Mbps to 783 Mbps. But looking at 2018 as a whole, things were completely different. Over 2018 a 97.7% growth rate in attack size was seen, with a median in January of .56 Gbps ballooning to 1.548 Gbps by December.

Also in 2018 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 as of 2016.

PSPs have seen an increase in more complex types of attacks, like combined attacks (flooding and application-layer attacks using HTTPS) which 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).

3.6.4 Suggested Controls and Mitigation

PSPs should preferably set up a (DDoS) security control framework. In general terms they should be able to identify, protect, detect, respond, recover, assess and adjust possible DDoS attacks. The table below gives a high level description of these controls[75].

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

[74] https://blogs.akamai.com/2019/01/a-look-back-at-the-ddos-trends-of-2018.html

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

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 5 High-level dynamic DDoS security control framework

The Internet Engineering Task Force (IETF) established a new working group called DDoS Open Threat Signalling (DOTS). The aim of DOTS is to develop a standard 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.

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 still being discussed in the Netherlands at this moment. The aim is to recognise DDoS structures by their fingerprints and thus mitigating attacks. Furthermore some PSPs reported the DDoS attacks that have been carried out on them to 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.

3.6.5 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 as of 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 by showing that they are very well capable to execute these attacks.

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.

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 PSPs, universities, internet service providers, internet exchanges, responsible governmental cyber authorities, and the national 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.

In April of 2018 Europol coordinated the takedown of webstresser.org, arresting the administrators behind the DDoS marketplace, which was responsible for more than 4 million attacks by the time the website was forced offline. Webstresser.org was responsible for attacks against financial services, governments, and gamers. Once DDoS traffic returned to expected levels, the banking, finance, and education industries were popular targets, along with the gaming industry, which was the top target throughout the year.

3.7 Botnets

3.7.1 Definition

A botnet is a collection of internet connected devices compromised by an attacker who orchestrates through a Command and Control (C&C), without the knowledge of the victim.

Botnets act as a force multiplier for malicious activity. Commonly used for DDoS attacks, attackers also make use of the botnets' collective power to scale attacks such as spamming, credential compromise or cryptocurrency mining. The word "botnet" is a combination of the words "robot" and "network".

3.7.2 Fraud Description

Botnets have two main objectives:

- Herding more devices into the botnet and;
- Performing malicious activity.

The malicious activity performed by a botnet can be of a wide variety, namely:

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.

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.

Credential harvesting

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.

Man-in-the browser malware to intercept online banking credentials is one of the attack vectors that can achieve a large-scale attack through the use of a botnet.

Account testing fraud

Cybercriminals can scan a range of IP addresses to find a specific port, and then bombard the service - FTP, Telnet, RDP or others - with rapid-fire authentication credentials from a list they have developed or bought in the underground.

In the electronic payments sector this can be used to test credit card numbers or online banking accounts.

Cryptocurrency mining

Cryptocurrency mining benefits from intensive computing power. Botnets are a preferred means to mine crypto-currency drawing on the victim's system computing power and electricity.

Many other malicious activity may be performed benefitting from the large scale offered by botnets, such as:

- Click and pay-per-install fraud;
- Manipulation of online polls;
- Denial of inventory;
- CAPCHA solving;
- Hosting illegal downloads.

3.7.3 Impact & Context

A few evolutions have occurred to botnets in the last years, in respect to their C&C strategy, to the types of infected devices, to the malicious activity and to the commercial model of botnets.

C&C strategy - Centralised to decentralised

The most important part of a botnet is the so-called C&C infrastructure from where the attacker can control the botnet giving instructions to the bots and receiving collected data from them.

The first botnets would have a centralised approach comparable to the classic client-server network model.

Newer botnets use a decentralised, i.e. peer-to-peer, model in order to try and evade detection and to be more resilient in face of takedown attempts.

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.

Types of infected devices – Computers to IoT

The compromised systems in traditional botnets were almost exclusively computers, recent botnets compromise IoT devices such as cameras, routers, DVRs, wearables and other embedded technologies. IoT botnets tend to be larger in scale due to a set of characteristics of the compromised systems:

- IoT devices are usually designed with lowering costs as a major driver and security interests tend to be neglected. As a result these embedded devices are easily exploited (e.g., default credentials, exposed services).
- These devices are in many cases not subject to patching or firmware upgrades leaving large numbers of devices subject to exploitation of already published vulnerabilities.
- Many of these devices are permanently online and available 24x365, resulting in a larger exposure surface from the beginning of an exploit.
- Devices are rarely monitored, preventing timely detection.

Botnet malicious activity – Crypto-currency mining

Botnets are the basis for certain types of attacks such as DDoS and spam mailing; and are a way to enlarge the scale of other attack types.

One use of botnets that fits perfectly the objective of the attackers is by using the bots for crypto-currency mining. The vast computing capacity managed through the botnet's compromised devices and the tremendous usage of electricity power, both supported unknowingly by the victims, are beneficial for financial gains through crypto-currency mining. The fact that no apparent harm is sensed by the victim makes detection less probable and turns the botnet even more profitable.

Commercial model of botnets – Botnet kits

For some years, botnets have been offered as a commodity either through selling subparts of the botnet or by leasing botnets. More recently botnet kits have been behind some major botnets. The top three botnet kits — Andromeda, Gamarue and Wauchos — are estimated to be responsible for having compromised more than a million devices a month.

3.7.4 Suggested Controls and Mitigation

The CSDE (Council to Secure the Digital Economy) has published the "International anti-botnet guide – 2018"[76] that highlights practices to combat botnet threats. This report details a wide range of mechanisms and processes that mitigate the effects of attacks conducted through botnets. It divides the measures applicable to "Infrastructure", "Software development" and "Devices and device systems" and further details measures for "Home and small business systems installation" and for "Enterprises".

The ENISA report "Botnets: Detection, Measurement, Disinfection and Defense"[77] continues to be a reference for mitigation techniques for botnet threats, covering both technical methods and social and regulatory approaches.

Technical countermeasures

- Blacklisting
- Sinkholing
- Orchestration of controls at host and network level
- Vulnerability management in combination with regular updates
- Distribution of fake/traceable credentials
- DNS-based countermeasures
- Direct takedown of C&C server
- Packet filtering on network and application level
- Walled gardens
- Peer-to-peer countermeasures
- Quarantine Infected Computers
- Infiltration and remote disinfection.

Regulatory and social countermeasures

- Dedicated laws on cybercrime
- User awareness raising and special training
- Central incident help desk

[76] https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf

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

- Enhance cooperation between stakeholders.

3.7.5 Final Considerations/Conclusions

As a result of the evolutions that botnets made, they have been very successful in 2019, and will probably continue so in the following years. The growth of the IoT ecosystem and with no end in sight for the relaxed security they inherently have, will be a fruitful area for exploit.

The availability of low-cost botnet kits on the darkweb and the commercialisation of botnets on darkweb market places will make botnets prosper. The beneficial fit of crypto mining to the botnet features will probably make this kind of usage continue to grow.

In respect to payment threats the use of botnets for DDoS will continue to be a relevant threat but keeping in mind that financial gain for the attackers is mainly obtained through extortion or similar techniques. It seems that botnet DDoS may achieve more advantageous gains extorting other time dependent activities (e.g. events) or through other extortion-based attacks (e.g. ransomware).

Account verification attacks and payment credential compromise, at the European level, will be mitigated by the adoption of Strong Customer Authentication as required under PSD2 [6]. Compromising knowledge factors on a compromised system has historically been a reasonably achievable task for malware. Compromising two factors of different natures and usage of dynamic linking will elevate the bar for the attacker to be successful.

It is foreseeable that botnets will tend to be potentiated for other malicious activity not directly related to payments, given the recently increased measures through PSD2 compliance.

3.8 Cloud Services and Big Data

3.8.1 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.[78]

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,

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

and information privacy. The term often refers directly to the use of predictive analytics or other particular advanced methods to extract value from data.[79]

3.8.2 Fraud Description

The mainstream of cloud computing seen as IaaS, PaaS and SaaS 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 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.

3.8.3 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 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.

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

- 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.
- Unauthorised access to cloud computer resources could lead to execution of crypto mining software.
- An unauthorised access to cloud computer resources could lead to sensitive data leakage.

3.8.4 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 previously mentioned 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 whether or not to start 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 segregated 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 using 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 (CSA).

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.

3.8.5 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 applicable regulations on 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[80] for security, to automate lifecycle operations and harden solutions uploaded into a Cloud Service Provider (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 Cloud Security Alliance or the Cybersecurity Act of the European Union which will increase trust via ENISA´s mandate and the harmonisation of certifications, including the cloud service certification which hopefully will also bring new enhancements such as the continuous monitoring on certifications which could be of great benefit for CSPs and end users, increasing trust, security and free flow of data and therefore fostering the digital economy. Moreover, new standardisation and guidelines developments on cloud computing services[81] need to be monitored and applied as they become available.

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

[81] 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

3.9 Internet of Things (IoT)

3.9.1 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.

3.9.2 Fraud Description

Like traditional computers and networks, IoT devices pose at least similar risks, for example in payment transaction processing or in Internet banking. Because IoT devices are connected to the Internet, they represent new targets for data exposure and attacks. They can be infected by 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 the security of an IoT device as serious as they do for 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 passwords that are never changed make them more attractive for attacks, and we are increasingly seeing new forms of extortions, botnet 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.

3.9.3 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 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.

3.9.4 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 always be secured (e.g. use of encryption, device 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.

3.9.5 Final Considerations/Conclusions

Enterprises across the world try to find new ways of doing business and IoT provides new opportunities. Since these “things” do not look like traditional computers, they are not 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. Hence, 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). As a consequence, the services offered will be extended more and more to cover the payment sector, increasing the risks for both consumers and enterprises.

3.10 Virtual currencies

3.10.1 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"[82] 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 virtual community"[83], 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 Ethereum (ETH), Ripple (XRP), Bitcoin Cash (BCH), or Litecoin (LTC). In 2019, thousands of cryptocurrencies exist, tens of them with a market capitalisation of more than 100 million euros[84].

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.

3.10.2 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, and moreover, services have appeared, called *Bitcoin mixers* with the aim of providing obfuscation

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

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

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

of the flow of the funds in exchange for a fee, allowing the fraudsters to move and cash-out the stolen funds anonymously. As such it is used as a vehicle for criminal activities such as money laundering, buying illicit goods, extortion, etc.[85]

Attacks to large crypto currency exchange traders

Crypto currency exchange traders keep suffering data breaches were customer accounts and assets have been stolen, massively compromised and as a consequence Bitcoin funds retrieved from those accounts[86]. 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[87] 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."

In conclusion, these traders are holding customer cryptocurrency wallets in a centralised infrastructure in a similar way as ASPSPs 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, hardware or paper wallets. 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 these wallet credentials or to exploit an existing vulnerability.

Many of the attack vectors and corresponding countermeasures run parallel to fraud patterns and prevention measures in non-digital currencies. Online wallets for example can look like online banking platforms in terms of credentials provisioning, authentication and use of two factor authentication. In July 2017, one of the largest heists in the history of virtual currencies was noted 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 that the same old attack vector can occur with new disruptive technologies.

Crypto currency mining

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

[86] https://www.pymnts.com/cryptocurrency/2019/major-crypto-hacks/

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

Diverse attack scenarios that raised up since end 2017 continued in 2019, in order to obtain cryptocurrency mining with unauthorised use of resources. Crypto mining software has appeared on diverse websites and servers in an unauthorised manner, as it has been spread as malware, including on IoT devices[88].

Scams

The anonymity that virtual currencies can provide, made diverse types of scams appear. Ponzi schemes, fraudulent initial coin offerings (ICOs) or inexistent virtual currency offers are some examples of these. As an example, in 2019, an investigation by The Washington Post uncovered a dozen of accounts, pages, and groups across Facebook and Instagram which misleadingly claim to be official hubs for Libra, the cryptocurrency proposed by Facebook[89] .

3.10.3 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 PSPs.

3.10.4 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[90] 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.[91]

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.

3.10.5 Final Considerations/Conclusions

Virtual currencies are here to stay. The market capitalisation of virtual currencies by the end of the first semester of 2019 has increased a 33.5% compared to the same period in 2018 according to Coinmarketcap[92].

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,

---

[88] 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/

[89] https://www.theverge.com/2019/7/23/20706772/facebook-libra-scams-pages-groups-accounts-pre-sale-cryptocurency-fraud

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

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

[92] https://coinmarketcap.com/charts/

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.

4 Payment fraud

4.1 Introduction

The various threats described in the previous section can basically lead to two categories of fraud, namely so called "Authorised payment fraud" and "Unauthorised payment fraud". *Authorised payment fraud* refers to authorised transactions in which the genuine payer initiates and approves a payment to an account under the control of a criminal. *Unauthorised payment fraud* refers to an unauthorised fraudulent transaction whereby the genuine payer does not provide authorisation for the payment to proceed and the transaction is carried out by a criminal.

The sections below describe fraud related to specific payment instruments.

4.2 Card related fraud

4.2.1 Definition

Payment Card Fraud is a wide-ranging term relating to the theft and crimes 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 payment account, usually to pay for the criminal's lifestyle or to fund more serious criminal activity.

4.2.2 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. Lately, omni-channel fraud e.g. using stolen card information in wearables and mobile devices in a POS environment has been noticed. The following are typical card frauds:

- Lost / Stolen Card – a card can be stolen by several methods such as 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 (shoulder surfing). 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. This could also be used in a social engineering context, tricking mostly elderly people to hand over card and PIN to what they believe is for a trustworthy cause.
- Account Take Over scenario 1 / Fraudulent Application – refers to the situation where 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 issuer or financial institution and, using the genuine cardholder's details, dupes the issuer into believing they have changed address and lost payment cards, which are replaced by the issuer and sent to the fraudster's newly advised address.
- This fraud often occurs in combination with social engineering fraud and phishing.
- Account Take Over scenario 2 / A cardholder enrols to a payment page on a merchant's web-site who has a secure storage solution (PCI compliant) of card data on file. The loading of card data on file occurs with or without 3DS. The access for making payments on the merchant site is through a simple cardholder ID and password, chosen by the cardholder. A fraudster can easily find out about these credentials and subsequently make payments using the cardholder's secured card-data-on-file.

- Card not received – Where a criminal will steal a payment card from an individual's mail box or in the mail delivery process, 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. The card data is then loaded into blank magnetic stripe cards and used to withdraw funds or make purchases.
- 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. Criminals can exploit this when issuers have implemented the EMV protocol incorrectly. Not common in Europe.
- 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).

4.2.3 Current and New Payment Card Fraud Trends

Social engineering

With more SCA solutions in place all over Europe, this fraud modus operandi is increasing, and expected to increase even more as the related requirements of the PSD2 and the RTS legislation get implemented. Basically, the fraudster goes after the weak link in a SCA payment chain, which often is the human. You could normally split this modus in two main tracks:

- *Identity theft or phishing.* The fraudster steals or tricks the victim to disclose their card/personal credentials/online banking verification methods and thereafter make the transaction, often to money mule accounts. For example, mules have used their own cards cashing out big at casinos and jewel/watch stores in Europe. Here we also have seen a recent problem with Global Wallets for Contactless or eCommerce payments. They use EMV data and are considered secure. But if the Card issuer does not have strong enough enrolment and card credential provisioning solutions, this service can become a vessel for Social Engineering fraudsters who download wallets into their own mobile devices and can perform fraudulent SCA-transactions. In many of these types of fraud the entry point towards the victim consists of different forms of phishing/vishing/smishing obtaining the online banking credentials and the exit of money is with card payments.
- *Authorised card transaction scams.* In this case the fraudster persuades the card holder to perform the transactions themselves, either by impersonating to be someone/something else or by selling fake services or goods. This fraud can be very devastating for the victim since they are not always refunded in view of unclear definitions of fraud and related liability. There is also often a personal shame in being scammed like this, hence the hidden number of victims can be big. Examples of authorised transactions fraud where card payments is used include investment fraud, romance fraud, smishing leading to fake websites, fake purchases of goods turning into unwanted subscriptions, fake advertising for renting apartments etc.

Lost and stolen card fraud

Although lost and stolen card fraud can be noticed 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 PSPs and financial institutions across Europe. Fraudsters consistently look at better and easier ways to capture PINs, e.g. using social engineering or shoulder surfing, and then they steal the payment card using various methods. Often targeting elderly. This fraud is due to its nature of chip and PIN, often hard to detect for issuers, even with sophisticated monitoring technology.

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 lost or stolen cards 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. The increased usage of blocking/temporarily blocking cards through bank apps, is also beneficial in this respect.

Account take over / Fraudulent cardholder application.

Fraudsters are using social engineering techniques such as infiltrating cardholders' homes, approaching PSP staff or other methods, such as spear phishing, to obtain the data needed to take over an account or create a false cardholder 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-dominant 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 this is still possible in countries where EMV has not yet been fully introduced. This remains a concern for European card issuers. Fraud losses remain high for this fraud type including the significant cost to PSPs and financial institutions to replace ATMs, terminals, cards and PINs and to monitor their customers' accounts for fraudulent activity.

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 which 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. For example, 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 is in place, with the capability to intercept transactions. 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 high value transactions on unsuspecting merchants.

Advanced Persistent Threat (APT)

APT attacks are targeted at specific stores, financial institutions or other sites holding valuable card- or customer information in their databases, with the aim to compromise the network or payment system and gain payment card data (see Section 3.4).

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.

First party fraud (overdrafting credit limits)

Non-credit worthy people trying to get payment cards and banking accounts with the only purpose to overdraft the accounts / credits without any intention to pay back. The only interest is to overdraft to get cash. Usually a weak KYC procedure and too flexible card products provided to the customer with generous credit limits are causing first party fraud.

Friendly / Family fraud

Increased "fraud" where for example a parent's card is loaded in a Merchant Wallet as used "card on file" in different entertainment gaming sites -or apps. It is not clear when a new purchase or top up of coins / points etc takes place, not for a child who is playing nor the parent. Too late is the parent (cardholder) aware on that payments have been made to the card / account to amounts a lot higher than one may have thought when the card was added / "installed". There is also an increasing problem with cardholders doing CNP purchases themselves, knowingly or unknowingly (could be under the influence of alcohol/drugs/addiction) and then dispute the transactions with their issuer.

Merchant refund fraud

When the fraudster with different methods apprehends an in-store card terminal and uses it to make refund purchases with stolen cards, predominately pre-paid. To make sure the merchant has sufficient funds on their account, the fraudster often first make purchases using stolen cards. They then cash out in ATMs immediately afterwards. The fraudster has knowledge about terminal functionality, and can in some cases also have inside help at the targeted merchant.

4.2.4 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. Always patch systems when needed.
- Perform an annual risk assessment by your Risk and / or Fraud Departments to check if all mitigating measures are completely set and in control.
- Educate store employees how to identify and how to act when they suspect fraudulent behaviour in POS-environment. Make sure to have well working routines to alert and how to protect the cash register and card terminals.
- Store and process customer data according to PCI DSS standards.

For Card 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 (SCA) 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: Allow for easy access customer customisation of ATM withdrawal limits, daily spend, e-com environment and contactless functionality, possibility for temporary block in mobile bank app etc. Promote customer awareness on this.
- 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: Use a several layered approach from authentication to authorisation, which includes automatic customer interaction. Deploy a responsive, self-learning, real-time fraud system with prevention capabilities and risk scoring. Ensure your fraud system identifies suspicious patterns of behaviour to stop fraud based on both generic and 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.
- Work together, non-competitively, with other players and law enforcement agencies within your market to establish good communication lines and information sharing forums. Use these forums for mutual information sharing and raise awareness to customers.

- Make sure your Fraud and Chargeback team works close together and with resources and tools available to identify the growing problem of friendly fraud.
- Within your local market, engage in working with others to develop standardised digital identification methods for safer e-com purchases and online access to bank account information.
- Make sure no credit limits can be over drafted in any offline environment with your issued cards. Don't issue a credit card if the customer is not credit worthy.
- Make sure no offline limits can be reset by card holder actions to commit friendly fraud.
- Global Wallets – Employ an enrolment solution with Strong Customer Authentication to heavily reduce the risk of 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.
- Do not give away your personal information or codes to your identification method if you don't initiate the event yourself.
- If a financial institution offers controls on limits and e-com and contactless functionality for the payment card, ensure you set these at the settings 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.
- Always check with your card issuer if you receive suspicious information or requests via SMS/mail/telephone to initiate a log-in procedure or approve a transfer. The issuer never requests the cardholder to do that.
- If you choose to store your card credentials "on file" at an e-commerce merchant, make sure that you understand what type of payments that can be made, and who is able to initiate a payment with your card.

4.2.5 Final Considerations/Conclusions

Historical and current fraud types such as lost and stolen card 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 countermeasures should continue to be implemented and advice taken as much as possible.

Especially, new fraud techniques such as shimming, attacks on contactless cards and attacks on global wallets for mobile devices should be monitored carefully and guidelines on preventing these issues implemented.

Stolen identity, phishing and in addition, various kinds of social engineering scams utilising authorised card transactions as a payment method, are the most growing modus operandi for fraudsters. The increase of authorised card transactions scams will most likely be an increasing problem due to the following three factors:

- Regulations like SCA and more advanced fraud prevention tools in use by the PSPs push the criminals away from unauthorised CNP fraud that has dominated fraud numbers for years, and instead going after the human which is the weakest link in the payment chain;
- Some countries have started to change the liability towards the issuer of the payment instrument, instead of the cardholder which gives more visibility to the PSPs;

- PSPs have likely under reported this type of fraud/scams and there has also been a lack of standardisation from FSAs and other regulatory bodies which is now slowly changing.

4.3 ATM Fraud

4.3.1 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.

4.3.2 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. Possible where the EMV protocol is not correctly implemented.

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.

Cash trapping

It's the unauthorized physical manipulation of an ATM, preventing the cash being disbursed to the card holder. Criminals immediately collect the cash afterwards.

Transaction Reversal Fraud (TRF)

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".

4.3.3 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 use the cloned cards in countries where Chip / EMV have not been widely 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.

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

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 the European Payment Terminal Crime Report from EAST (European Association of Secure Transactions) covering 2018 there were 157 such attacks reported against European ATMs. This is an 18% decrease from the 192 attacks reported during 2017. Related losses were down 70% reflecting the fact that many of these attacks are unsuccessful.

4.3.4 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: Allow for easy access customer customisation of ATM withdrawal limits, daily spend, and contactless functionality, possibility for temporary block in mobile bank app etc. Promote customer awareness on this.
- 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: Use a several layered approach from authentication to authorisation, which includes automatic customer interaction. Deploy a responsive, self-learning, real-time fraud system with prevention capabilities and risk scoring. Ensure your fraud system identifies suspicious patterns of behaviour to stop fraud based on both generic and 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.[93])
- 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 or ATM-usage 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.
- Don't give away your personal information, card or codes to your identification method if you don't initiate the event yourself.

4.3.5 Final Considerations/Conclusions

Skimming and low-tech fraud remain the most common frauds at ATMs. The financial impact from these types of fraud is absorbed by both the card issuer of the compromised/stolen card or the merchant/ATM deployer, depending on liability. Thus, countermeasures should be taken by every player in the chain.

For ATM owners/operators, high tech fraud, such as the use of malware or black box attacks, is still a 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.

4.4 SCT and SDD related fraud

The various types of attacks described in this document under Section 3 could lead to fraud for SEPA Credit Transfers (SCTs), including instant SCTs and SEPA Direct Debit (SDD) 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 or convince the genuine account holder to authorise a transaction to an account controlled by the criminal.

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

In an impersonation and deception scam, a criminal purports to be from a legitimate and trusted organisation, such as a PSP, 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 (see Section 3.2).

CEO fraud and business email compromise attacks continue to grow and evolve, targeting all size of businesses and personal transactions (see Section 3.2.3).

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.

Authorised Push Payment (APP) related fraud, in which the victim – being subject to a scam - actually makes the payment themselves, is showing a steep increase and for PSPs they are much harder to detect. At the root of any APP scam is a "convincing" lie with which the fraudster somehow manages to deceive the victim.

In the "Fraud-the-Facts 2019" report[94] from UK Finance, the following types of APP scams can be found:

- *Purchase scam*: the victim pays in advance for goods or services that are never received. These scams usually involve the victim using an online platform such as an auction website or social media.
- *Investment scam*: a criminal convinces the victims to move their money to a fictitious fund or to pay for a fake investment. The criminal will usually promise a high return in order to entice victims into making the transfer. These scams include investments in items such as gold, property, carbon credits, cryptocurrencies, land banks and wine.
- *Romance scam*: the victim is convinced to make a payment to a person they have met online through social media or dating websites, and with whom they believe they are in a relationship. Fraudsters will use fake profiles to target their victims in an attempt to start a relationship which they will try to develop over a long period of time. Once they have established their victim's trust, the criminal will then claim to be experiencing a problem, such as an issue with a visa, health issues or flight tickets and ask for money to help.
- *Advance fee scam*: a criminal convinces their victim to pay a fee which they claim would result in the release of a much larger payment or high-value goods. These scams include claims from the criminals that the victim has won an overseas lottery, that gold or jewellery is being held at customs or that an inheritance is due. The fraudster tells the victims that a fee must be paid to release the funds or goods, however, when the payment is made, the promised goods or money never materialises. These scams often begin with an email or a letter sent by the criminal to the victim. A special version of this scam occurs, when a victim realises that they have been subject to a fraud, and is contacted by a "solicitor" offering to help get the money back for a small fee.
- *Invoice or mandate scam*: the victim attempts to pay an invoice to a legitimate payee, but the criminal intervenes to convince the victim to redirect the payment to an account they control. It includes criminals targeting consumers posing as conveyancing solicitors, builders and other tradespeople, or targeting businesses posing as a supplier, and claiming that the bank account details have changed. This type of fraud often involves the criminal either intercepting emails or compromising an email account.

[94] https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019

- *CEO fraud*: is where the criminal manages to impersonate the CEO of the victim's organisation to convince the victim to make an urgent payment to the scammer's account. This type of fraud mostly affects businesses.
- *Impersonation of police / PSP staff*: in this scam, the criminals contact the victim purporting to be from either the police or the victim's PSP and convinces the victim to make a payment to an account they control.
- *Other impersonations:* a criminal claims to represent an organisation such as a utility company, communications service provider or government department. Common scams include claims that the victim must settle a fictitious fine, pay overdue tax or return an erroneous refund. Sometimes the criminal requests remote access to the victim's computer as part of the scam, claiming that they need to help "fix" a problem.

These scams may be perpetrated using only persuasion, but the fraudster sometimes may include other elements from the fraudster toolbox like vishing and abuse of credentials or malware on the victim's device.

Another important technique 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 limited number of criminals involved, a maximum result can be established (see Section 3.4).

According to the 2019 report from UK Finance[95], intelligence suggests that criminals continue to focus on contacting customers by phone, text message or email pretending to represent a trusted organisation such as a PSP, 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 APPs[96]. This fraud activity is not limited to just the traditional banking firms, TPPs (Third Party Payment Service Providers) are now also reporting it. Actually, APP fraud is the fastest growing fraud in the UK and the related loss is even larger than fraud losses related to "unauthorised fraud".

The procedures for collecting fraud data across SEPA, as well as the related cooperation between authorities and PSPs, will be enhanced with the implementation of harmonised fraud reporting requirements at EU level under PSD2 [6] and the dedicated EBA guidelines [2]. As a result, SEPA wide figures should become available in the near future from the ECB.

4.5 How fraudsters monetise their illegal gains

The fraudster, who has succeeded to establish a fraudulent payment transaction (whether authorised or unauthorised), knows of course that investigators soon will follow the trace and that the amount may be frozen or returned. The fraudster needs to immediately initiate a cash withdrawal, a purchase (that leaves no traces), a transfer by a money ordering service or a transfer to another bank account from which again a withdrawal, purchase or transfer must be done.

Fraudsters need mules

To stay in the shadows the fraudster hires 'money mules' and uses their bank accounts to receive the fraudulent transfers and the mules then -according to the fraudster's instructions- bring the

[95] https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019

[96] https://www.psr.org.uk/psr-publications/news-announcements/PSR-welcomes-industry-code-to-protect-against-app-scams

spoils to the fraudster in a way it cannot be tracked. The mule is either willingly or unwillingly, knowingly or unknowingly covering the tracks of the fraudster. All mules will eventually be subject to investigations and most likely reported to police. If there are any funds left on a mule's account after paying the fraudster, the mule will probably be forced to return the amount that was stolen from the original victim. Hence, it seems that a mule is bound to lose, and the question raises how anyone is persuaded to be a mule[97].

How are mules recruited or are mule accounts being established?

Mules fall in three (not completely distinct) categories:

1. Those, who are tricked into performing as a mule – not really understanding what they are doing. Even if they find the whole scheme a bit strange, they close their eyes to the possibility that they take part in a criminal act - sometimes influenced by the prospect of earning some easy money.
2. Those who know what they are doing and have (secretly) ensured themselves a good slice of the pie, have prepared statements that make it difficult to prosecute and calmly face consequences such as their client relationship being terminated by their PSP. Of course, on such a mule account there will be no money left that could be returned to the victim.
3. Those, who are actually not involved at all, except that their credentials have been misused or a bank account has been set up in their name by the fraudster somehow deceiving the PSP's on-boarding procedure.

How do mule schemes work?

When a fraudster has established the necessary mule(s), they will orchestrate the combination of conducting one or more fraudulent transactions and using the mules to get money out of sight. The actual flow may depend on the size of the amount(s) and needed level of complexity to escape investigators. Especially cross-border transfers and more in particular instant payments make it more difficult and complex.

A few examples of possible flows involved in money mules are provided below.

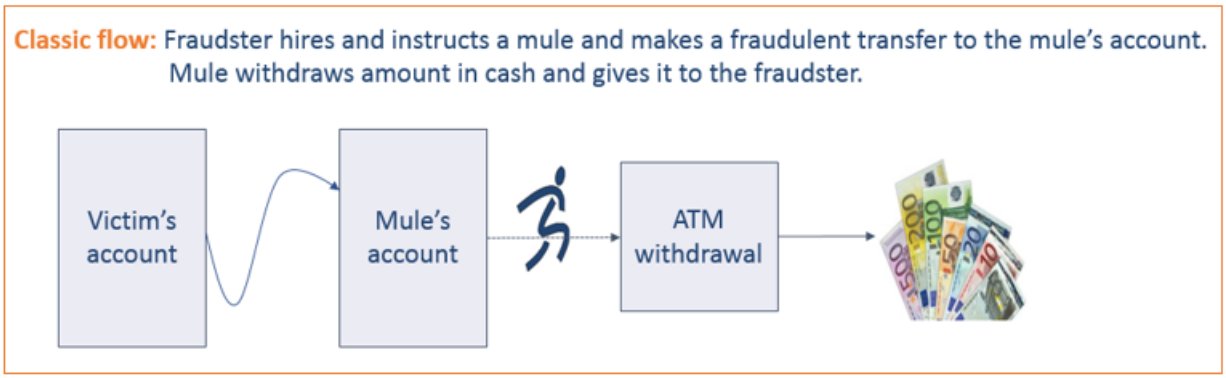

Figure 1: Classic money mule flow

[97] See a comprehensive description of "The money mule trap" at FINTRAIL

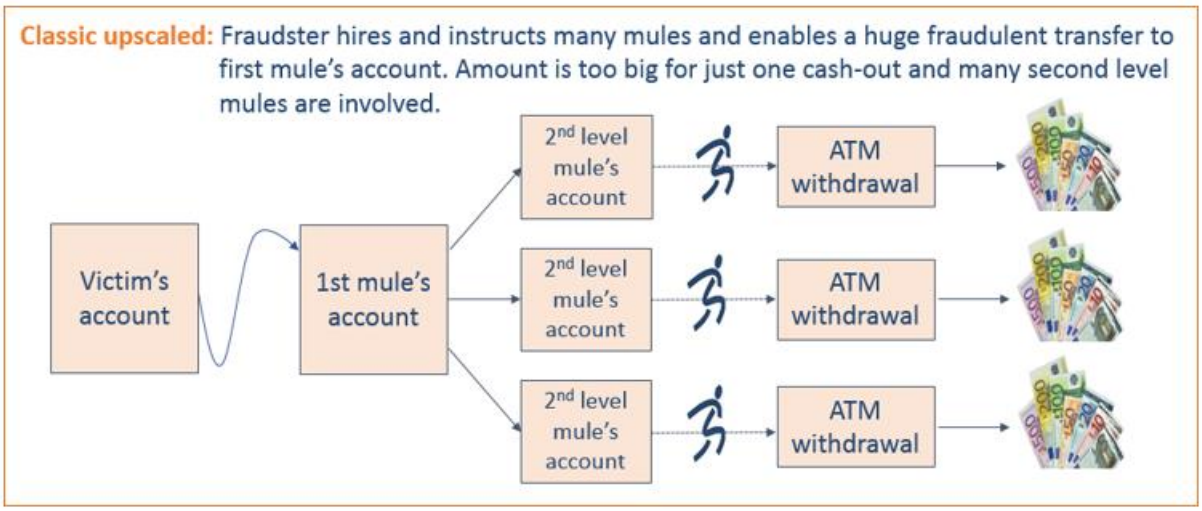

Figure 2: Classic upscaled money mule flow

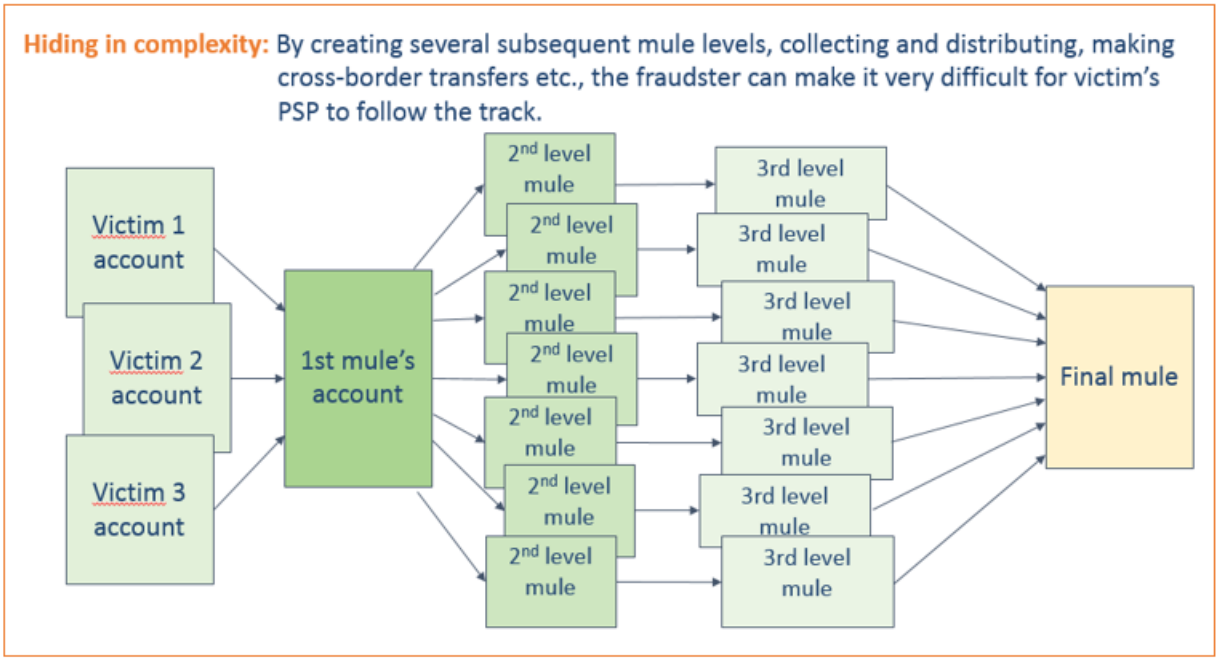

Figure 3 Complex money mule flow

Complexity certainly does make it harder for investigators, but it also increases quite dramatically the fraudsters tasks and risks. Most cases are therefore still not very complex and do not involve more than one or two levels of mules. But it is to be expected that the trend will go in the direction of using more complex mule or money laundering schemes – probably often offered "as a service".

A critical step is when the amount finally leaves the banking systems through some kind of transaction that covers the track sufficiently for the criminals. In the flows above the mule withdraws cash. However other modi operandi may be employed such as shown in the following examples:

- The mule buys bitcoins (or another hard-to-investigate cryptocurrency) and gives them to the fraudster;

- The mule purchases a valuable (easy-to-sell) asset which is (anonymously) taken over by the fraudster.

Countermeasures

Awareness

It is not generally understood that when a person receives some money (e.g. via a mobile P2P or banking app) – withdraws the same amount from an ATM and passes on the cash to some friendly person they just met, they might have in reality helped to cover up a crime.

Awareness is especially necessary towards youngsters, who due to natural lack of experience, low income, willingness to-help-out and sometimes some "peer pressure", seem more prone to become mules. PSPs should be careful to give easy-to-understand warnings against "becoming a mule" when they provide access to on-line banking services or issue cards. Awareness must also target other identified "vulnerable" groups (such as low-income persons, addicts, etc.) tempted by seemingly easy money and unaware of law and consequences[98].

Mule recruitment often comes in waves and the payment industry should cooperate to detect and warn against email and/or social media-based mule recruitment campaigns.

Registration of 'professional' mules

For those mules, who know what they are doing and do it for the gains they can achieve, awareness is not relevant. Instead PSPs should cooperate to achieve that the same person cannot act as colluding mule again and again by shifting to a new PSP. It should be possible to register in a common database if a person repeatedly has acted as a mule. This should not necessarily hinder this person to open a payment account, but it should enable monitoring to detect possible new mule activity by this person at a very early stage.

Monitor, detect and stop mule-like behaviour at PSP and ASPSP.

Instant payments obviously make it easier for mules and harder for fraud investigators. PSPs should consider having mechanisms in place that react and put transactions on hold, until further investigated, if transaction pattern on an account indicates "mule activity"" – e.g., if larger amounts arrive from new (unknown) sources followed by attempts to cash out or pass on these amounts via other ways.

Sharing of mule accounts

When a payer's PSP knows or strongly suspects that a payment (or attempted payment) is fraudulent, and the beneficiary account therefore is a mule account, it should be possible to share this information (suspicion) with peers in real-time to avoid the account is used for other fraudulent payments. It is important that the sharing is fast, since possible attempts to abuse the account may very well happen just after the first attempt that leads to detection/suspicion.

Detecting complex mule and money laundering schemes

For a single PSP it may end up being very difficult to "follow the track", if there are many mule-levels. However, if PSPs cooperate[99] and pool their payment data (in a secure and law-compliant way), it may be possible to use strong analysis tools and much more efficiently detect mule accounts and money laundering rings. Whereas the first mule level has a short lifetime, subsequent mule-levels may re-use accounts over a longer period, if they can stay undetected.

[98] See "The money mule trap" at FINTRAIL

[99] See New anti-money laundering technology sees UK fraud rings frozen

Analysis on pooled data can put a significant pressure on money mule schemes. To be effective in the long run such cooperation must be cross-border and will become more important in view of instant payments, which soon will become the new normal.

In that respect it is worth mentioning the initiative conducted by Europol, Eurojust and the EBF referred to as "the European Money Mule Action"[100] that involves more than 300 PSPs and private parties and has proven to be successful over the past years.

[100] https://www.europol.europa.eu/newsroom/news/over-1500-money-mules-identified-in-worldwide-money-laundering-sting

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, phishing and vishing attempts are still increasing and they remain instrumental often in combination with malware. Whereas in the past consumers, retailers and SMEs had 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. However, exact figures are lacking because scam-based fraud is not adequately reported for various reasons.

With PSD2 and the dynamic linking of authentication codes to the payment transaction details, phishing of authentication codes will become useless but phishing of activation codes for mobile payment /authentication apps should be expected to become a new playing field for social engineering (see Section 3.2).

Malware remains a major threat but more particularly ransomware has become the top cyber threat faced by European cybercrime investigators according to the recently published IOCTA report by Europol[101]. 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 customers to mitigate malware attacks (software updates, anti-malware tools, do not click on links, etc.), is one of the best tools to mitigate the risks and their 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 large customers, including merchants. Endpoint and network defences, as well as using the latest anti-virus software and next-gen firewalls, are not enough to prevent hacking. 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[102].

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

[101] https://www.europol.europa.eu/iocta-report

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

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 commonplace in Europe enabling a wide variety of mobile apps, including payment apps (see Section 3.5). As a result, they are more and more becoming an attractive target for cybercriminals and fraudsters, along with 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 amount 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, data in the cloud and 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 (PSD2 [6] and the RTS [9], NIS Directive [7], GDPR [8]), payments also face a new regulatory landscape in Europe, which on one hand increases the security barrier with respect to fraud (e.g. strong 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"103, causing huge challenges. 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, DDoS 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 mag-stripe is still largely usable in some countries, counterfeit fraud will remain an issue, and also gets further refined in its technique, potentially with the goal of successful and effective shimming or contactless skimming. Meanwhile in the POS space, low-tech fraud like lost and stolen, sometimes combined with forms of social engineering, is also going strong, and now represents a high fraud cost for card issuers in some EU countries. Unauthorised CNP fraud remains a huge problem and fraud cost driver. Due to criminals engaging in high tech activities like APTs and other breaches where card credentials are stored, there is no shortage of stolen credentials for sale at online marketplaces. However, with high-end preventive methods and regulations like PSD2 [6] and the RTS [9] with its requirement for SCA, criminals are changing their approach towards instead utilising various phishing and social engineering techniques to perform fully authenticated CNP transactions, either themselves or scam the victims to unknowingly perform them. It is also key that security of new products, e.g. mobile wallets, is being designed with that in mind. That being said, to combat fraud, it is of utmost importance, that all PSPs and merchants use the extended grace period granted by the EBA during 2020 (see [5]) to fully comply with the SCA regulatory requirements.

[103] See for instance https://www.bankinfosecurity.com/cybercrime-as-a-service-economy-stronger-than-ever-a-9396

For SEPA Credit Transfer and Direct Debit transactions, the criminals' use of impersonation and deception scams, as well as online attacks to compromise data, continued to be an important factor behind fraud losses related to these types of payments. In all these methods, criminals target personal and financial details which are used to facilitate fraudulent transactions. More in particular during the past year an increase was noted in Authorised Push Payment fraud (see Section 4.4).

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 rules and 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 the availability of more accurate fraud figures.

It is also worthwhile mentioning that the EPC is establishing a new group on fraud prevention related to the EPC-managed SEPA payment schemes[104], namely the Payment Scheme Fraud Prevention Working Group. The aim is to contribute to operational payment fraud prevention by facilitating SEPA payment scheme fraud data collection and analysis, information sharing and prevention measures.

PSPs could also investigate new proactive methods to prevent fraud. As an example, the payee's PSP having received a possibly fraudulent transfer may more easily recognise subsequent attempts to pass on the money as mule activity, if the transfer is accompanied by a fraud marker[105], signalling that the payer's PSP although not having clear evidence of fraud, finds the transfer suspicious. Another potential fraud mitigating measure is the implementation of a "Confirmation of Payee" service as described in Section 3.2.4.

The European Commission has reviewed and extended the legislation on combating fraud and counterfeiting of non-cash means of payment (see [10]). The – now replaced - 2001 Council Framework Decision on combating fraud and counterfeiting of non-cash means of payments no longer reflected today's reality, such as use of virtual currencies and mobile payments and was focused on card-fraud only. In addition, new mechanisms should be put in place to enable cybercriminal prosecution not only within the European Union but also globally.

The European Union is already discussing an e-evidence Regulation[106] 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[107].

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 while society should cater for early education on security and social engineering risks.

[104] See ANNEX I.

[105] As proposed by the ASPSPs in the Netherlands.

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

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

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 euros (100,000 euros as of 1 July 2020) – in less than ten seconds, 24/7/365, between accounts located in the 36 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 [11]) 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
Social Engineering Section 3.2	Exchange of information between PSPs Transaction filtering and monitoring Awareness raising for consumers, SMEs and corporates Blocking spoofed mails (DMARC) Takedown of phishing web sites
Reverse Trojan horse	
Voice Phishing (vishing)	
Angler Phishing	
Malware Section 3.3	Regular software updates Script and macro blockers, IPS / IDS functionality Limited usage of admin rights Firewalls and antivirus on consumer devices Awareness about danger of opening attachments Web traffic and email content analysis
Trojans	
Ransomware	
Remote Access Trojans	
Advanced Persistent Threats Section 3.4	Behaviour analysis tools Real time advanced security data analytics Incorporation of security threat intelligence into infrastructure Advanced IP scanner/ APT scanner Red Team/Blue Team approach Five styles of Advanced Threat Defense Framework
Customised malware	
Waterhole attack	
Mobile Device Related Section 3.5	Regular software updates Screen lock / mobile device lock No jailbroken or rooted devices Only call validated PSP numbers PSPs never ask for credentials over the phone App store monitoring Installation of anti-virus software App code protection and pen testing Sensitive data encryption No trust in third-party libraries Controls to protect communication channels User and device verification User notification via more than one channel PSP notifications by operator about SIM swaps or duplications
Fake Apps	
Mobile malware	
Spoofed SMS (smishing)	
Attacks on mobile apps (app & OS security, user awareness, abuse of privacy, enrolment processes, biometric authentication, duplicated SIMs)	
SIM swapping	

Denial of Service Section 3.6	Dynamic DDoS security control framework DDoS mitigation scrubbing service Periodic tests of anti DDoS measures Security intelligence feeds and incident response team "Forensic ready" logging
Flooding	
Protocol	
Application layer	
Botnets Section 3.6	Blacklisting Sinkholing and blocking Distribution of fake/traceable credentials DNS-based countermeasures Direct takedown of C&C server Packet filtering on network and application level Walled gardens Peer-to-peer countermeasures Infiltration and remote disinfection Take downs by law enforcement Awareness raising and co-operation
Captcha solving	
Brute force	
Data harvesting	
Spreading of malware	
Cloud Services & Big Data (SaaS, PaaS, IaaS) Section 3.8	Risk based approach Self-control over authentication Strong authentication and authorisation controls Monitoring/audit/certification of service providers Adequate training of employees
Data exposure	
Enhanced risks related to authentication / encryption	
Internet of Things (IoT) Section 3.9	Security risk assessment for every new device and infrastructure Adopt security and privacy by design Strong authentication and authorisation controls Secure device to device communication Deployment of devices with international recognised security certifications Minimisation of amount and type of data exchanged
Data exposure	
New targets for # attacks (malware, botnets, etc.)	
Virtual currencies Section 3.10	Detect characteristics of fraudulent investment schemes Wallet security best practices Cyber insurance Regulation of virtual currencies
Anonymity exploitation	
Attacks to exchange traders	
Wallet compromise	

Table 6 Summary threats versus controls and mitigations