2016 PAYMENT THREATS TRENDS REPORT

1 Introduction

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

The document is structured into two sections. The first section analyses threats which are encountered nowadays in payment contexts and are causing fraud. Hereby the following topics are covered:

- Denial of Service;
- Social Engineering and Phishing;
- Malware;
- Mobile Related Attacks;
- Botnets;
- Card related fraud;
- ATM Attacks;
- Multi-vector attacks.

The next section aims to include early warnings on threats related to emerging technologies which could lead to potential fraud in payment contexts. Hereby the following topics are covered:

- Cloud Services and Big Data;
- Internet of Things;
- Virtual currencies.

2 Main threats today

2.1 Denial of Service

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

Conseil Européen des Paiements AISBL– Cours Saint-Michel 30 – B 1040 Brussels
Tel: +32 2 733 35 33 - Fax: +32 2 736 49 88
Enterprise N° 0873.268.927 www.epc-cep.eu - secretariat@epc-cep.eu

attack directly affects the availability of a network system (server, system, platform etc).

Fraud Description

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

The ease for criminals, "script kiddies", etc. to prepare and execute a DoS attack is increasing. It is relatively easy and not expensive to "buy" attack capabilities on the internet. Two categories of perpetrators may be distinguished: "old school hackers" or "hacktivists" who just want to have a name or defend an ideology and the "hackers that essentially pursue financial gain". The latter ones use all means, human or technical failure, available to create blackmail or massive fraud. Moreover, DoS attacks are also used to conceal other attacks and distract the defenders.

DoS attacks are in general Distributed Denial of Services (DDoS) attacks. These attacks combine a large number of systems in the same time frame, making it more difficult to distinguish attack streams from genuine streams. In other words, a large numbers of compromised systems attack a single target.

Distinction can be made between three basic types of (D)DoS attacks as follows.

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

A special form of a flooding attack is the so called DNS amplification attack. In an 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 DNS 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. The IT components (routers, webservers, etc.) that are relevant when it comes to data traffic processing receive packets for processing that lead to unexpected results. As a consequence a large number of communication sessions are opened without being

properly closed in due time. This leads to buffer overflows in ICT components; as a result they can no longer accept any new sessions.

The application-layer attack

An application-layer attack takes advantage of an error in the implementation of a protocol. For instance, what may happen is that a software error in a particular IP packet causes a webserver to crash. This means that from that moment on, this webserver is no longer available for other traffic. In many cases, an application-layer attack is relatively easy to rectify, namely through the implementation of a patch that rectifies the software error. However, this patch does have to be provided by the supplier of the software component concerned.

Impact & Context

In 2016 a number of European payment service providers (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 e-mail. The only correct practice is to not "give-in". Also PSPs in Europe have seen larger attacks, at least up to 100 GBS. The current scrubbing services are (assuming sufficient capacity has been bought by the PSP) able to handle this size of attacks. Recently there have been a number of very large scale attacks on non-PSPs. The one on Krebsonsecurity was a long lasting attack of appr. 650 GBS. The cloud-hosting party Akamai Technologies has dumped the website from its servers after the site came under this "record" cyberattack. France-based hosting provider OVH was the victim to the record-breaking Distributed Denial of Service (DDoS) attacks that reached over one terabit per second (1 Tbps).

A third attack reported beginning of October 2016 was an attack on a DNS provider. Twitter, SoundCloud, Spotify, Shopify, and other websites have been inaccessible to many users throughout a day. The outages are the result of several distributed denial of service (DDoS) attacks on the DNS provider Dyn.

The attacks mentioned above were possible, because of the fact that many IoT devices were infected and attacked Krebsonsecurity, OVH and Dyn. Troubling to security experts was that the attackers relied on Mirai, an easy-to-use program that allows even unskilled hackers to take over online devices and use them to launch DDoS attacks[1]. 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.

The Akamai state of the internet Q3 2016 report[2] shows a 71% increase in total DDoS attacks, a 77% increase in infrastructure layer attacks (layers 3 & 4), a 138% increase in attacks > 100 Gbps (19 vs. 8) compared to Q3 2015. China ranked as the top source

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

[2] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf

country for DDoS attacks while US, UK, France and Brazil round out the remaining top five source countries.

It is clear that (D)DoS attacks are not a PSP specific issue, but it is also a threat to the financial sector.

Suggested Controls and Mitigation

PSPs are expected to have mitigating measures in place against (D)DoS attacks. 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. Such a service can be provided locally, at the premises of the PSP, or at a third party provider infrastructure, or at both.

Since protocol attacks comply with the standard for the protocol in question, it is more difficult to counteract such attacks, because the countermeasure must not prevent the correct implementation of the protocol.

PSPs can also implement mitigating measures against application level attacks including for instance application-level security products, application level key completion indicators; 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. 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. CERTs are internationally known for developing practices and technologies to protect, detect, and respond to attacks, accidents and failures on networked systems. This should be coupled with an Incident Response Team (IRT) at each entity involved in fraud detection, without regard for the activity sector, which could close the malicious software or infected server.

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.

Final Considerations / Conclusions

(D)DoS attacks have been an increasing risk, 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. Measures to mitigate the basic kind of (D)DoS attack should 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.

In the past, attackers seemed to aim at little or no financial gain through these attacks. However, recently more activity is to be noticed whereby hackers are using (D)DoS as a means for blackmailing. 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 or even to spear phishing attacks. It is probable that these attacks will continue in the near future and that financial sector or payments sector organisations remain potential targets.

One may not ignore that the probability of these attacks continuing in the near future is high (e.g., in view of the increased usage of IoT devices) and that financial and payments sector organisations remain potential targets.

2.2 Social Engineering and Phishing

Definition

Social engineering is a non-technical method of intrusion used by hackers which relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is the psychological manipulation of people into performing actions or divulging confidential information.

Phishing is the attempt to acquire sensitive information such as usernames, passwords, card or account details and physical cards including the PIN codes, for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Typically these attacks target the authentication methods used by the customer in on-line banking sessions and remote payments or the behaviour of the customers once logged-in into their on-line banking system.

Fraud Description

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

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

Common social engineering attacks include the following:

- *E-mail from a friend.* If a criminal manages to hack or socially engineer one person's e-mail 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 e-mail account under their control, they send e-mails to all the person's contacts

or leave messages on all their friends' social pages, and possibly on the pages of the person's friends' friends. These messages typically contain a link the persons trust and click causing an infection of their device with malware so the criminal can take over their machine and collect information or contain a download– pictures, music, movie, document, etc., that has malicious software embedded. In addition, these messages may create a compelling story or pretext: e.g., urgently ask for help or ask to donate to their charitable fundraiser, or some other cause. They may also be more targeted and concentrated and take over an active dialogue with the PSP.

- A special case of "E-mail from a friend" is *CEO fraud* where an attacker sends an e-mail that appears to come from the CEO, or some other powerful executive in the organisation, using social engineering to coerce employees to transfer money to a given beneficiary. The attackers spoof the e-mail of the CEO, CFO or other high-level executive by either compromising their real e-mail account or creating an account that looks almost identical to the real one. The use of the CEO's name is key to these attacks, it lends an air of authenticity and authority to the scams. Employees tend to take requests from the CEO seriously[3].
- *Recovery agent fraud.* Happens *when* former fraud victims are told the money they have previously lost can be recovered. Targeting former fraud victims, the fraudster poses as a legitimate organisation, claiming they can apprehend the fraudster and recover any monies lost - for a fee. Criminals use social engineering tactics either by phone or email, posing as a lawyer, a law enforcement officer or an official working for a government agency in another country. If the fraud victim responds to their offer of help, they will ask him or her for various fees, such as release and administration fees. If fraud victims pay these fees, they will keep coming back with another fee that has to be paid, before the money can be returned[4].
- *Phishing attempts.* Typically, a phisher sends an e-mail, instant message, comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution. These messages usually have a scenario or story:
    - The message may explain there is a problem that requires the receiver to "verify" information by clicking on the displayed link (which may look very legitimate) and providing information in their form. An example of SMS phishing may notify "Your online banking account is locked. You need to unlock it at the link provided", once you click on the link take you to a fake bank website that asks you to enter your personal information. The fake site looks identical to the bank's real homepage. However, when you attempt to log in to your account, the site asks for information that the real site never would. It may ask, for example, your account number, password or card PIN. These types of phishing scams often include a warning of what will happen if you fail to act soon, because criminals know that if they can get the individual to act before they think, they more likely will fall for their phish.

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

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

- The message may notify that you're a "winner". Maybe the e-mail claims to be from a lottery, or a dead relative, or the millionth person to click on their site, tax refund, etc. In order to give you your "winnings" you have to provide personal or bank information. These are the 'greed phishes', leading to emptied bank account or identity theft.
- The message may ask for help…. Preying on kindness and generosity, these phishes ask for aid or support for whatever disaster, political campaign, or charity is hot at that moment.
- Response to a question the receiver never had. Criminals may pretend to be responding to a "request for help" from a company while also offering more help. They pick companies that millions of people use like a software company or PSP. If the individual does not use the product or service, they will ignore the e-mail, phone call, or message, but if they do happen to use the service, there is a good chance they will respond because they probably do want help with a problem.
- The message may offer a "more secure" or "functionality enhanced" card, requesting the customer to send their outdated card to a certain physical address and requesting in addition that the customer also sends their PIN to a given e-mail address.

In recent years the perpetrators of attacks on customer authentication mechanisms have also been refining their methods. Where before, most attacks were directed towards all customers, they are now increasingly aimed at specific individuals identified as potentially worthwhile targets. Those phishing attempts directed at specific individuals or companies have been termed *spear phishing* and have proven to be more successful. Attackers may gather personal information about their target to increase their probability of success.

- Other type of phishing used by scammers is "Network spoofing". It is when hackers set up fake access points in high-traffic public locations such as coffee shops, libraries and airports. Then, cybercriminals give the access points common names, like "Free Airport Wi-Fi" or "Coffeehouse", which encourage users to connect. In some cases, attackers require users to create an "account" to access these free services, complete with a password. Many users employ the same email and password combination for multiple services, allowing the hackers to compromise their email, e-commerce, and other secure information.

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

- Attacks using malware to try to persuade the customer to carry out a "security update" or type in a number of TANs because of an alleged "security incident".
- So-called "reverse Trojan horse" attacks working as follows: the customer's device is infected with a Trojan horse which falsifies the customer's online bank statement so that it appears as if a large sum of money has been transferred by e.g., the tax authorities to the customer's account. The customer then receives an e-mail, allegedly from the local tax office, asking him or her to return the amount credited "in error", while the customer is in fact "reimbursing" the money to a fake account.
- Vishing (the word is a combination of "voice" and phishing) - exploits the public's trust in landline telephone services, which have traditionally terminated in

physical locations known to the telephone company, and associated with a bill-payer. Typically, the phishing link sends the victim to a fake helpdesk that attempts to scam the user into surrendering private information that will be used for identity theft.

- The angler phishing attack involves hackers creating fake Twitter accounts, posing as customer support staff, to trick customers into handing over their personal details. The scam entails hackers monitoring bank customers' interactions with their banks on Twitter. They then hijack conversations users attempt to have with genuine support staff of banks, and redirect the customers to a fake support page.

Impact & Context

Social engineering and phishing are very often employed as a first step to launch other specific attacks. Whereas a couple of years ago it was embarrassing that one could find malware on a customer's device (PC, mobile phone, etc…), this is no longer true with perpetrators using more clever social engineering.

Phishing plays a key role in carrying out targeted digital attacks. Some users are not able to recognise phishing e-mails. Means to make authentic e-mail recognisable as such are only used in practice to a very limited extent. This ensures that phishing continues to be a low-threshold and effective method for attackers.

Phishing is also sometimes used together with distribution of malware, malware which is for example being activated when the victims are directed to a specific infected website.

Social engineering and phishing attack trends in 2016:

- According to Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA)[5]:
    - Phishing has developed into one of the most widespread attack vectors. The quality of phishing messages and websites is also increasing. Professional looking phishing websites continue to be generated by easy-to-obtain phishing kits that require little technical skill to be installed and customised on a remote server.
    - An increase of phishing aimed at high value targets has been registered by law enforcement and the private sector alike. CEO fraud, a refined variant of spear phishing, has become a key threat.
- According to Kaspersky Lab - Spam and phishing report in Q2 2016[6]:
    - The focus of phishing attacks shifted slightly from the 'Global Internet portals' to the 'Financial organisations' category. The overriding trend of the quarter is that of fraud and making quick money from victims using direct methods such as Trojan cryptors that force unprotected users to pay a ransom, or phishing attacks that target financial organizations, rather than long drawn-out scams.

[5] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

[6] https://securelist.com/analysis/quarterly-spam-reports/75764/spam-and-phishing-in-q2-2016/

- Fraudsters try to place phishing pages on domains with good reputations to bypass security software filters. This significantly reduces the probability of them being blocked and means potential victims are more trusting.
- Hot topics: The themes of the Olympics in Brazil and presidential election in the US were exploited by phishers to make users visit fake pages with the aim of acquiring their confidential information or simply to get their money.
- Fraudster continue to focus most of their attention on the most popular brands (Microsoft, Facebook and Yahoo!) enhancing their chances of a successful phishing attack.

- In 2016 Proofpoint[7] has already seen a 150% increase in social media phishing attacks when compared to the same period in the previous year. In particular, they've seen an increase in a dangerous new variation called angler phishing. "This method of phishing is highly effective because your customers are already expecting a response from your brand. Unfortunately, angler phishing is part of a broader trend in social media fraud" said Proofpoint researchers.

Suggested Controls and Mitigation

A continuous exchange of intelligence information about attacks and countermeasures among the IT experts of PSPs is considered to be almost the only possible defense against these types of attacks.

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

However, a very important aspect to counter the social engineering attacks is continued awareness raising campaigns. PSPs need to have a proper customer education system in place, not only addressing individual clients but also including SMEs and large corporates, explaining the risks in layman words. In some countries coordinated campaigns are being set up where the financial industry cooperates with public or semi-public agencies. In addition, it is as important for companies and organisations (including PSPs) to also adequately educate and create awareness amongst their own staff (e.g., related to CEO fraud).

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

Among the technical measures that can mitigate phishing, the following may be considered as best practices[8]. Sender Policy Framework (SPF), which is an email-validation system designed to detect email spoofing. It is the first step in securing the mail channel. The next protection is to use DomainKeys Identified Mail (DKIM)[9], which

[7] https://www.proofpoint.com/us/proofpoint-stops-social-media-customer-service-phishing-industry-first-protection

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

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

is an email authentication method designed to detect email spoofing by providing receiving mail exchangers to check that the incoming mail from a domain is authorised to be sent by that domain's administrators. And then the final step to be implemented is Domain-based Message Authentication, Reporting and Conformance (DMARC)[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.

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

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

Final Considerations / Conclusions

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

2.3 Malware

This section will dive into the world of malware. There are many categories of malware, but common to all of them is that the software has no or very little benefit for the legitimate user. In reality, malware tries to control the infected user device and to steal valuable information or resources from it.

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 vira, worms, remote access tools, rootkits, Trojan horses, 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.

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

Trojan horse

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

Spyware, Adware & Banking Trojans

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

Ransomware

Ransomware is the growing kid in the malware family[11] with high risk for the target systems. Its primary goal is 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. Especially during 2016 a significant increase of ransomware attacks has been observed[12]. A surprising fact is that this kind of attacks seems to be more profitable to the attackers than the traditional banking Trojans.

Advanced Persistent Threats

Another important category of malicious software is the one that is being abstractly described as Advance Persistent Threat. Although usually this kind of threat serves one of the aforementioned kind of malicious software, it 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 0-day attacks since no normal signatures exist from the antivirus / antimalware tools. An example of such attack is the incidents against SWIFT infrastructure of several banks that led to unauthorised execution of transactions worth millions of Dollars. A combination of high skill techniques, state of the art malware, and lack of or inadequate technical and procedural protection measures contributed in one of the biggest security breaches in financial institutions.

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

[11] ENISA Threat Landscape report 2016 (https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2016-report-cyber-threats-becoming-top-priority/)

[12] see https://blog.barkly.com/ransomware-statistics-2016

commonly used by Advanced Persistent Threats to bypass strong authentication and get access to important data.

Fraud Description

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

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

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

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.

For the private user the most terrible loss will probably be the loss of personal data, e.g. access credentials, photos of loved ones. This is the typical problem of ransomware; during this year we have seen many attacks with ransomware affecting ordinary citizens. For SME and companies in general, the attacks can be similarly devastating, intellectual properties could be lost, access to customer databases, order status or even accounts overview might be lost forever. The mitigation to reduce damage here is at least to have backups. Ransomware is a very profitable business for attackers. During the first three months of 2016 $209 million have been collected by criminals, with FBI predicting that ransomware will be a $1 billion crime by the end of 2016[13]. The "Kaspersky Security Bulletin 2016 - The ransomware revolution" shows that in 2016 ransomware grew in sophistication and diversity, targeting both individuals and businesses (62 new ransomware families made their appearance)[14].

[13] http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

[14] https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/

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. A great example for 2016 is a malware called GozNym, stolen 4 USD millions until April 2016.

For the private users spyware and adware are a large threat towards the 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 looks for the individual behaviour, in fact that is their goal to group the individual by their own definitions, it is therefore not a direct threat towards corporate users. The general advice would however be to utilise specialised software to remove and protect against adware, as they also could use resources on the computer.

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

Suggested Controls and Mitigation

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

Script blockers is 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.

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[15], 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), 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 proved 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.

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 the advices are crucial and why they should be followed. Therefore PSPs should keep investing in customer awareness campaigns. On the other hand, PSPs should continue to invest in new security technologies, such as the Advanced Threat Protection ones, for combating state-of-the-art and 0-day malware attacks, including ransomware.

2.4 Mobile Related Attacks

The use of mobile devices for both online banking and the purchase of goods and services (both online and in person) has increased dramatically over the last couple of years. With this increase in usage there has been a corresponding increase in the threats affecting payments, this section is designed to provide an insight into these threats.

A mobile app(lication) is a computer program designed to run on mobile devices such as smartphones and tablet computers. Most such devices are sold with several apps included as pre-installed software, such as a web browser, e-mail client, calendar,

[15] 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.

mapping program, and an app for buying music or other media or more apps. A mobile payment usually involves a dedicated mobile app.

During the last decade, the evolution in mobile devices resulted in the deployment of more innovative mobile payments methods. Users of mobile devices can use mobile wallets, payments applications based on NFC technology, peer-to-peer payment apps and others[16].

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.

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[17]);
- To make person to person (P2P)[18] 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
    - To obtain SMS based authentication for online banking taking place on a separate channel;

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

[17] 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)).

[18] 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 e-mail 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 exploit new contactless payment methods in which a traditional payment mechanism i.e. a credit card is stored on a mobile device for contactless transactions;
- To obtain SMS based verification and/or validation messages e.g., payment verification, set up of new payee, digital wallet provisioning;

- 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.

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

2.4.1 Attacks Targeting the Mobile Device

Impact & Context

In 2015 a Mobile Payments Security Study conducted by ISACA[19] mentioned that "the global mobile payment market, will be worth an estimated US $2.8 trillion by 2020, according to Future Market Insights. As the use of mobile payment picks up speed, the associated risks grow as well."

More than 900 ISACA cybersecurity member experts participated in the study reaching the following conclusions:

- Only 23% believe that mobile payments are secure in keeping personal information safe.
- Nearly half (47%) say mobile payments are not secure and 30% are unsure.
- 87% expect to see an increase in mobile payment data breaches over the next 12 months, yet 42% of respondents have used this payment method in 2015.

The Trend Micro 2016 Security Predictions report, "The Fine Line"[20] predicts that "despite the slow adoption rate, the introduction of next generation mobile payment systems will inspire a renewed interest for threat actors to carry out real-world testing to steal information from new payment processing technologies like EMV credit cards, contactless RFID credit cards, and mobile wallets. In 2016, the improved security brought by these modes of payment will be challenged by online criminals." Therefore the protection against mobile payment attacks is considered to be an important security challenge that companies will face in the years to come.

The market offer for mobile payment applications is growing fast, but this tendency attracts cybercriminals and opens up new potential attack vectors. Bluebox Labs examined payment apps, concluding that "Today's most popular mobile payment apps leave consumer dollars and enterprise revenue exposed."[21] It found that many apps

[19] http://www.isaca.org/pages/mobile-payment-security-study.aspx

[20] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-fine-line.pdf

[21] BlueBox Security: http://www.marketwired.com/press-release/bluebox-security-reveals-todays-most-popular-mobile-payment-apps-leave-consumer-dollars-2076501.htm

have experienced security breaches compromising consumer data or allowing man-in-the-middle attacks.

Fake Banking Apps

During the last 24 months there have been a number of instances where fake copies of banking mobile apps have been released in an attempt to try and get users to install the application and then use the app to attempt to connect to their PSP. In most instances these apps are found on 'grey market' sites rather than official app stores such as iTunes or Google Play, but there have been isolated instances where a fake banking app has been uploaded to an official market place (Google Play). A recent example is FANDA SDK[22], a new variant of Android malware that poses as a fake banking app to trick users into compliance, after which it locks users out of their smartphones and sets about emptying their accounts, while victims scramble to access their phones again. It has been around since December 2015.

Mobile Malware

Malware targeting mobile devices continues to proliferate. The 2016 Kaspersky Security Bulletin[23] reports that "the main mobile threats in 2016 were advertising Trojans able to obtain "root" or superuser rights on an infected Android device – a level of access that allowed them to do pretty much whatever they wanted." This includes hiding in the system folder, thereby making themselves almost impossible to delete, and silently installing and launching different apps that aggressively display advertising. They can even buy new apps from Google Play. Moreover, 22 of the 30 most popular Trojans in 2016 are advertising Trojans – twice as many as in 2015. Many such Trojans were distributed through the Google Play Store: some of them were installed more than 100,000 times, and one – an infected Pokemon GO Guide app was installed more than 500,000 times.

Spoofed SMS Messages

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 the matter is urgent. 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.

This attack is very successful as most users believe that a SMS is more secure than an email, users are aware of the fact that spam and phishing mails exists but so far the awareness of a similar and even worse problem existing on SMS is not something that the public is aware of. A 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.

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

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

[23] https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary

will be displayed together with previous, legitimate messages from the PSP, increasing the likelihood that the message will be considered genuine.

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

Phishing Attacks

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

Other types of attacks on mobile applications

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

- Poor application and Operating System security:
    - Poor consumer data protection on device (visibility of authentication information, transaction history, personally identifiable information (PII) 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 mobiles.
    - Vulnerabilities not patched quickly enough in Applications and OS.
- Lack of user awareness:
    - Smartphone users are often not aware about practicing adequate security habits (i.e. no device access control, easy to hack passwords or lack of them, connections to unsecure WiFi and/or Bluetooth always activated, download of malicious applications, phishing (see also section 2.2 – Phishing Attacks), social engineering, device OS tampering (jailbroken, rooted), credentials storage, etc...).
- Abuse of Privacy:
    - A great variety of applications can access private and personal information with the permission of the user. In this case the application may not be malicious but the customers are granting access to the application developer's company without being aware that very sensitive information is being shared or who will eventually have access to this information (as an example, games asking access to the agenda, location, photos, etc...).
    - Mobile phones are mixing personal and corporate usage.

- Mobiles are gathering more and more information from the customer, which aggregated could help to carry out sophisticated attacks.

- Enrollment process:
  - Fraudsters are taking the advantage of the high volume of new enrollments occurring nowadays. Certain global payment apps have been exploited in that respect during the past years.
- Biometric authentification:
  - Numerous studies and frauds have shown that biometric authentification in payments without a second factor can be weak and result in frauds, especially if the fraudster can access physically the smartphone.
- Duplicated SIMs:
  - There is an increasing trend from fraudsters to duplicate SIMs so as to commit fraud.

Suggested Controls and Mitigation

There are a number of measures that users can implement to mitigate the threats of Mobile Fraud, these include:

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

- Implement device owner/user verification.
- Implement mobile device verification.
- Use two-factor authentication when the risk is high.

Final Considerations / Conclusions

Mobile and its applications are becoming the most used way to connect customers with their PSP to the detriment of the browser. From a security perspective this is a crucial change, whilst before customers had to "go to their PSP" through the browser, currently customers download applications on their smartphones from their PSPs or even dedicated stores "go to their PSP" (in analogy to "fat" clients on PCs).

Both for browser access and mobile apps, PSPs will need to define security policies and maintain appropriate infrastructures. The suggested controls to mitigate fraud should be used under an ongoing risk management governance.

2.4.2 SIM swapping

Definition and fraud description

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

Fraudsters obtain and utilise a customer's replacement SIM card to acquire security messages and one-time passwords (OTP) sent to the customer by the PSP. Using the OTP, criminals are able to change, add beneficiaries and transfer money out of the customer's account using their personal information that they would have obtained through phishing. During a normal online banking session, a PSP (using out-of band SMS or voice authentication) will send the customer an 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.

Impact and Context

Legitimate SIM swaps are increasing due to the movement to smaller SIM cards (micro and nano cards), which is providing malicious attackers with legitimate activities to cover their actions under. However, it is very difficult to obtain accurate figures on fraud committed in part through the use of exploiting weaknesses in the SIM swapping process. In the UK alone in quarter four of 2015 there have been a number of mainstream newspaper articles on the subject, highlighting numerous instances where people have had financial losses as a result of these activities.

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;
- Ask your PSP to give you details of every financial transaction through two channels - for instance, SMS as well as e-mail alerts;
- A PSP can negotiate with the mobile operators that the PSP is informed about the SIM swaps. This can help in monitoring the usage of the account.

Previous cybercrime reports have recommended that a movement away from MTAN authentication to hardware token authentication be advised, 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.

Final Considerations / Conclusions

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. Attackers will utilise all methods available, including social engineering attempts on the end user, malware on the 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 investigation and implementation of innovation and with robust security solutions from providers of mobile banking solutions.

According to CERT UK, the attacks on mobile devices in the UK alone quadrupled in 2015 and the trend seems to continue as Q1 2016 already had registered 50% of the numbers of 2015. This all points to the fact that mobile devices are increasingly

targeted for different types of attacks, however the awareness of these attacks and the dangers associated with mobile devices are not always well-explained to the end users. Most users trust that their phone is secure or have the common misunderstanding that they have nothing of value on their phone. Imagine the wealth of information on a smartphone there is.

2.5 Botnets

Definition

A botnet (also known as a zombie army) is a collection of compromised computers or other internet connected devices, each of which is known as a "bot". The compromised device will be equipped with code that commands it to become part of a botnet. The "botmaster" or "bot herder" controls these compromised computers.

Fraud Description

The following is to a large part based upon a public note in the CyberBits series, issued by Europol in October 2014, with later updates from 2015 and 2016.

The creation of botnets is often motivated either by financial gains or to use their destructive capacities. Botnets can be used as a means to accomplish several types of criminal or fraudulent actions:

- Distributed Denial of Service Attacks (DDoS);
- Generating disturbance on the network to camouflage other criminal activity;
- Sending of spam;
- Click fraud;
- Data harvesting (collection of logon credentials and other potentially sensitive data);
- Spreading of malware (adware, scareware, ransomware etc.);
- Source of anonymity – to hide the botmaster's real address and location;
- CAPTCHA solving;
- Brute force attacks;
- Mining virtual currencies;
- Manipulation of online polls.

In particular Botnets are key resources to DDoS attacks. The bots may be under direct control of the perpetrators carrying out the attack, or they can be hired from a specialised criminal offering botnet-as-a-service. The availability of botnets-for hire has led to more intensive attacks, but most of them last for a short period of time (30 minutes or less). While criminals can go to the effort of infecting multiple vulnerable devices and creating their own botnet to carry out DDoS attacks, it's often much easier to hire pre-made botnets for a set amount of time. The bigger the botnet, the more simultaneous requests it can send, and the potential for destruction will be larger.

Most successful botnets have until now mainly consisted of personal computers, and botnets containing several millions of computers have been observed. There have also

been examples of botnets exploiting mySQL servers which usually have a larger bandwidth capacity.

In 2015, we also saw the first examples of criminals making use of devices on the Internet of Things (IoT). Recent events (the DDoS attack against the blogger “Krebs on Security” in September 2016) have seen botnets consisting of a large number of IoT-devices (internet of things), e.g. routers, surveillance cameras or digital video recorders. The attack against Mr Krebs used a bandwidth of 620 Gbps. Many of these IoT-devices are exposed to the Internet and protected with weak and hard-coded default passwords. For the first time Kaspersky Labs reported in Q2 2016 that there were a large majority of Linux-based botnets compared to Windows.

The source code of the malware causing the DDoS-attack against Brian Krebs has been made publicly available, and may be used by anyone. This will make it easier for new perpetrators to build a botnet and launch attacks.

A device which gets added to a botnet, will usually continue to operate normally without showing any indication of being compromised.

Traditionally the botnets were controlled centrally by a botmaster from one Command & Control centre which gave the bots orders. Newer botnets use a P2P configuration where Command & Control is embedded into the botnet. This makes the botnet more resilient to takedown, especially when combined with creative use of cryptography.

Some botnets are also capable of detecting and reacting to attempts to investigate them, a potential reaction might be to launch a (D)DoS attack against the investigator.

Impact & Context

Botnets are mainly used as a tool to perform other criminal or malevolent actions. A compromised computer or device is no longer under the legitimate user’s control, and sensitive data may be harvested by attackers.

Botmasters have developed techniques that make their network of infected computers more resilient to takedown and also to evade detection by cyber security solutions. This implies for instance use of address changing techniques where the compromised computers are instructed to frequently change the domain name hosting. That means that the addresses which the infected computers refer to, change and point to a different computer within a few minutes. An alternative technique for this is the Domain Generation Algorithm.

Looking ahead, it is likely that criminals will make increasing use of vulnerable IoT devices to execute large-scale DDoS attacks. The Internet of Things is growing rapidly, so a large number of potentially inadequately protected machines can be exploited for launching attacks. As an example Symantec states that there are hundreds of millions of Internet-connected smart TVs.

In addition to this there is a continuous increase in broadband access in countries like China which means that hundreds of millions of inadequately protected PCs and other devices might be available for cybercriminals seeking new high-speed internet-connected computers and devices.

Figures from Kaspersky Labs indicate that South Korea is the leader in terms of number of Command & Control Servers. There is also significant activities in China, USA and Russia.

Suggested Controls and Mitigation

Since 2010 there have been several highly profiled takedowns of botnets through coordinated efforts, and this continues. In December 2015 law enforcement and Microsoft disrupted Dorkbot, a botnet which had infected more than 1 million computers the previous year. In December 2016 Europol[24] reported that they cooperated on the takedown of the Avalanche network. It has caused an estimated EUR 6 million in damages in concentrated cyberattacks on online banking systems in Germany alone. In addition, the monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the high number of malware families managed through the platform. The operation marked the largest-ever use of sinkholing[25] to combat botnet infrastructures and is unprecedented in its scale, with over 800,000 domains seized, sinkholed or blocked.

The takedown of a botnet will often give law enforcement insight in other cyber-criminal activities. The examples above show that it is sometimes possible to stop even the largest and most successful botnets. The geographic dispersal of the botnets – and of the command & control centre indicates that it is hard to succeed without an internationally orchestrated operation. Cooperation and exchange of information across borders and sectors is necessary to reduce damage and fight botnets. In some countries there are initiatives from internet service providers to collect information on (by botnet) infected PCs and to clean up these PCs. Examples include the "botfrei" initiative in Germany and the "Abuse Information Exchange" in the Netherlands. A similar European initiative is the "ACDC initiative"[26].

The individual end user cannot do much to fight botnets, but should use anti-virus/ anti-malware, personal firewalls and IPS/IDS functionalities on their devices and keep software up-to-date to remove known vulnerabilities. In addition, all devices connected to internet should be protected by a strong password that is different from the default usernames and password. This does also include non-traditional devices.

On the other hand, PSPs should invest in new state of the art technologies such as the ones protecting from Advanced Persistent Threats (APTs). Such kind of attacks, often called 0-day attacks, are more sophisticated and difficult to be detected and blocked with the usual antivirus / antimalware technologies. Botnets are easier to be distributed across a PSP's network, if these technologies are not used.

Final Considerations

Though there are several success stories of botnet takedowns, existence and usage of botnets will continue to be a problem. The proliferation of internet-connected devices creates a new set of possibilities for attackers who want to build a botnet. As for other information security aspects, there is a continuous game of cat and mouse here where the bad guys develop their techniques and get more professional, both in terms of better hiding and faster re-location of their command and control structures.

---

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

[25] sinkholing is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company.

[26] see https://www.acdc-project.eu/

2.6 Card related fraud

Definition and Fraud Description

Card related fraud is the term defining every theft committed using a payment card. The purpose is to obtain goods / services or unauthorised funds from the victims account.

The fraud scenario could start in different ways:

- Theft of the physical card;
- Loss of the physical card;
- Card not received by the legitimate customer;
- Counterfeit card;
- Card data stolen.

Stolen, lost or not received cards can be easily identified by the cardholder and quickly reported.

Cloning a card in Europe can be hardly done due to the EMV chip card. This chip is tamper-proof and nearly impossible to clone. EMV cards generate a unique numeric code for every transaction, which means a fraudster cannot use stolen account data to make fraudulent transactions at any merchant that requires an EMV card. European countries have experienced reductions in fraud from counterfeit cards.

The card information is composed of four data fields: the name of the card holder, the card number or PAN (Primary Account Number), the expiration date and Card Verification Code (CVV).

The compromise of this data could be used for fraud (i.e. mainly on the internet and outside Europe) or be stored and used months later, making it very difficult to identify the source of the breach.

Incident Impact & Context

With the rise of the internet, we have experienced how the common card fraud has been migrating to card not present (CNP) fraud. The internet is the main route to buy goods or services where the card is not physically present and the merchant must rely on the information indirectly. According to the latest report of the European Central Bank (ECB) published in 2015[27] CNP payments fraud are between 60-70% of total card fraud because of the greater risk it poses, and more recent reports from VISA Europe[28], and Europol[29] show there are still an increasing number of cases occurring

The total value of card fraud using cards issued in SEPA amounted to €1.44 billion in 2013. This represented an increase of 8.1% compared with 2012, however, since the value of all card transactions grew by 5.4% in 2013 compared with the previous year,

[27] https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

[28] https://www.visaeurope.com/media/pdf/managing%20fraud%20in%20the%20cnp%20environment_june%202016%2007.11.16%20(1).pdf

[29] https://www.europol.europa.eu/iocta/2016/exec-summary.html

fraud as a share of the total value of transactions increased by only 0.001 percentage point. Compared with 2012, CNP has become an even more important channel for fraud, whereas ATMs and POS terminals have become less important. CNP accounted for 66%, POS for 20% and ATM for only 14% of the total value of fraud.

Suggested Controls and Mitigation

We should divide the countermeasures between merchants and card issuers.

For Merchants:

- 3D Secure: authentication protocol based on a three-domain model (Acquirer, Issuer & Interoperability domain) to ensure authenticity of both peers through internet transactions.
- Tokenisation: process of substituting sensitive data with non-sensitive equivalent called token.
- PAN truncation: replaces the card number printed in any system with a printout of only the last four digits, the remainder being replaced usually by asterisks.
- Geolocation.

For Issuers:

- Geoblocking: To protect cards from being misused by skimming fraud, it is strongly recommended to protect cards with a geographical region of use.
- Blocking:To limit the usage of cards to specific channels or specific contexts.
- Fraud monitoring - Deploy a responsive, real-time fraud system with prevention capabilities. Ensure your fraud system identifies suspicious patterns of behavior to stop fraud based on tailor-made scenarios and rules.
- Strong Customer Authentication: The PSD2[30] defines it as "*an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.*"

Final Considerations

Card Not present (CNP) fraud is the dominant fraud type across Europe and will continue rising in the immediate future as an effect of cybercrime and consumers' data thefts. SEPA pushed criminals towards CNP through the introduction of strong authentication with the rollout of chip & PIN. However, the new PSD2 and the supporting Regulatory Technical Standard (RTS) on Strong Customer Authentication and common and secure communication aim to mitigate the CNP fraud.

[30] 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

The digital revolution boosts the migration, creating an online funds exchange too tempting to resist while connected business landscape collects more and more data everyday creating new vulnerabilities for criminals to exploit.

2.7 ATM attacks

Definition

ATMs are vulnerable to a number of different attacks which can essentially be regrouped in three different types, namely attacks:

- Against the *Cards- and PINs* used at the ATM (e.g. skimming and shimming attacks);
- Against the *logical integrity of the ATM* itself or its *ATM Environment* (logical attacks) (e.g. via ATM malware which typically compromises the ATM's software and operating system);
- Against the *physical integrity* of the ATM.

Fraud Description

The following description of the modus operandi is based on the European ATM Security Team (EAST) industry guidelines (see http://www.european-atm-security.eu/).

Attacks against Cards and PIN

- Target: Obtain Card Data and PIN (Card Data Compromise Devices) - With these types of attacks criminals obtain details of the victim's debit or credit card by affixing special devices in or on ATM's card reader. These devices then copy the magnetic stripe or get equivalent data from the chip. The criminals obtain the PIN using miniature cameras or false keyboards, which they have likewise attached beforehand. In non-chip countries, it is possible to withdraw cash without a forgery-proof chip (EMV), so the criminals procure money with a copy of the card in countries, not using EMV chip technology.
    - Card Skimming - Skimming is the installation by a criminal of a foreign device on an ATM to capture data from the magnetic stripe of a customer's card. The defining characteristic of a skimming device is the presence of at least one magnetic read head on the device.
    - Eavesdropping - Eavesdropping is the installation by a criminal of a foreign device on an ATM to capture data from a customer's card. This is typically achieved via a wiretap, sniffing the functionality of the card reader, or connection to a magnetic read head within the card reader. The defining characteristic of an eavesdropping device is the use of the legitimate card reading functionality of the card reader to capture the customer's card data.
    - Card Shimming - Card shimming is the installation by a criminal of a foreign device on an ATM to capture data from the chip of a customer's card. The defining characteristic of a card shimming device is, therefore, the targeting of the data contained on the chip on the customer's card, typically by placement of the foreign device between the customer's card and the contacts of the card reader.

- Software Skimming – Skimming 2.0 (ATM Malware Card/PIN compromise) - Target of this type of attack is to infect the ATM with malware, that intercepts card and PIN data at the ATM. A non-PCI compliant EPP Firmware is a precondition for the malware to intercept PIN data.

- Target: Obtain original Card & PIN
  - Card Trapping - The card is physically captured at the ATM, and the PIN is captured separately. Later the card is used to make fraudulent cash withdrawals. The customer loses the card. One card is lost in each attack.
  - Theft by trickery/Shoulder surfing -In case of theft by trickery the criminals watch their victim beforehand when withdrawing money. By spying on them, they manage to get the victim's PIN and then steal the card. Criminals often use a simple trick here. They create a diversion (drop something, let money fall out of a wallet, spill a drink on the victim, etc.). The victim is then distracted, and the criminals strike. Once they have the card and PIN, they can steal money from the victim's account.

Logical attacks against the ATM (-Environment)

- Transaction Reversal Fraud - An error condition is created at the ATM which makes it appear that cash will not be dispensed. This forces a re-credit of the amount withdrawn back to the account when in fact the criminal gets the cash (through the insertion of device, e.g. a Claw, manipulation of the ATM dispense mechanism by hand, or more rarely through corruption of the transaction messages).
- Jackpotting / cash out attack - Jackpotting is a term for attacks where malware takes control of the ATM PC and the cash dispenser function, thereby allowing the fraudster to directly cash out money. In most cases the malware is adapted to a specific environment, but the concepts can be easily migrated to different systems.
- Black Boxing - Black Boxing is a variant of Jackpotting, where the ATM PC is not used. Instead the fraudster brings his own PC with him and targets the communication between the PC and the dispenser unit. As the malware communicates directly with the dispenser, each Black Box attack is only valid for one type of dispenser.
- Man-in-the-Middle -Man-in-the-Middle attacks focus on the communication between the ATM PC and the acquirers host system. The malware can, for example, fake host responses to withdraw money without debiting the fraudster's account. Typically the malware is triggered during transactions with pre-configured card numbers. It can be implemented at a high software layer of the ATM PC or somewhere within the network.

Physical Attacks

- Cash Trapping - The criminal attaches a device to the ATM so that when the ATM tries to dispense cash the cash is trapped and the customer cannot retrieve it. The criminal then returns to the ATM and retrieves the trapped cash.

- Ram Raids - The ATM is attacked and either ripped out or the safe is attacked in-situ.
- ATM Burglary -The attacks can be carried out by brute force, or by using explosives or gas.

Impact & Context

General overview of the European ATM crime situation

EAST published the European Fraud Update 3-2016 (14th November 2016): Card skimming at ATMs was reported by nineteen countries, four of which reported an increase in attacks. Three countries reported decreases and in twelve countries attack levels were broadly unchanged. The usage of card reader internal skimming devices continues to spread. The trend of losses due to skimming occurring outside of EMV Chip liability shift areas, or in countries where the ATM EMV rollout has not been completed, continues. From the perspective of European card issuers the Asia-Pacific region and the USA are where the majority of such losses continue to be reported. The top three locations where such losses were reported were the USA, Indonesia and India.

Ten countries reported card trapping attacks and twelve countries cash trapping incidents.

Two countries reported transaction reversal fraud incidents. One of them continues to experience a significant increase in the number of attacks.

ATM malware and logical security attacks were reported by eight countries – one of them reporting a significant increase of black-box attacks. In two other countries all reported black-box attacks were unsuccessful.

To help counter these threats Europol has published a document entitled 'Guidance and Recommendations regarding Logical attacks on ATMs'. It covers mitigating the risk, setting up lines of defense and identifying and responding to logical attacks. The document is now available in English, German, Italian and Spanish.

Ram raids and ATM burglary were reported by nine countries and eleven countries also reported explosive gas attacks. Six countries also reported attacks using solid explosives. The use of solid explosives is spreading and is of increasing concern to the industry due to the risk to life and to the significant amount of collateral damage to equipment and buildings.

Trend Figures based on the European ATM Crime Report covering the first six months of 2016

ATM related Fraud Attacks

ATM related fraud attacks are split into Card Skimming, Card Trapping and "Other Fraud" (cash trapping and transaction reversal fraud).

During this period there were 10,820 such attacks[31] reported against European ATMs. This is a 28% increase from the same six month period in 2015 and equates to 29 attacks per 1000 ATMs over the period. Since 2011 there has been a continuing shift

[31] One attack is defined as one incident per ATM for card skimming (involving multiple cards) and one incident per card for card trapping.

away from high tech skimming attacks to lower tech card and cash trapping attacks, as well as to transaction reversal fraud. Overall skimming incidents have been declining since 2010. The current figure of 1,573 incidents is the lowest reported since H2 2005.

Reported Losses

During this period total losses of 173.72 million euros were reported. This is a 12% increase when compared to the total losses of 155.98 million euros reported for the same period in 2015 and equates to losses of 472,806 euros per 1000 ATMs over the period. Despite a shift towards lower tech incidents, the majority of losses are still due to higher tech card skimming.

ATM related physical attacks

Physical attacks are split into Ram Raids/ATM Burglary, Robbery, Explosive & Gas Attacks and "Other" (distraction theft and vandalism).

In this period there were 1,604 such attacks reported against European ATMs (Complete information was not received from all the participating countries). This total also includes data from solid explosive and explosive gas attacks and is a 30% increase from the same period in 2015 and equates to 4.4 attacks per 1000 ATMs over the period.

Reported Losses

Losses due to ram raids and ATM burglary account for the largest amount, but losses for explosive and gas attacks are rising. The average cash loss for a ram raid or burglary attack is estimated at €17,327, the average cash loss per explosive attack is €16,631 and the average cash loss for a robbery is €20,017 per incident.

ATM Malware

During the first six months of 2016 there were 28 such attacks reported against European ATMs. This is a 460% increase from the 5 attacks reported during the same period in 2015.

Three countries reported such attacks. All the attacks were 'cashout' or 'jackpotting' attacks using equipment typically referred to as a 'black box'.

Reported Losses

Related losses of €409,100 were reported. That is a 190% increase from the losses of €141,000 reported over the same period in 2015.

Suggested Controls and Mitigation

Countermeasures 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.
- EMV Fallback: Ensure that no fallback to Magnetic strip transactions will be authorised.
- Fraud monitoring: Deploy a responsive, real-time fraud system with prevention capabilities. Ensure your fraud system identifies suspicious patterns of behavior to stop fraud based on tailor-made scenarios and rules.

Countermeasures for ATM Operators

To counter the malware threat, the EAST Expert Group on ATM Fraud worked with Europol to create a document on guidance and recommendations on countermeasures regarding logical attacks on ATMs, which was published by Europol in June 2015.[32]

Final Considerations / Conclusions

Skimming and low tech fraud is still the most common fraud at ATMs. Financial impact from this type of fraud is often covered by the issuer of the compromised/stolen card. Thus, countermeasures should be taken by the card issuer.

For ATM operators, high tech fraud such as usage of malware is currently rare, but the financial impact is so much worse in individual cases. Therefore, it is recommended to establish the guidelines provided in the Europol Guide.

2.8 Multi-vector attacks

Multi-vector attacks exploit common weaknesses in the security chain - such as poorly configured servers, gullible staff, vulnerable applications or lack of multiple levels of defence - by combining elements like social engineering, spear phishing, contaminated USB drives and voice phishing with malicious attachments carrying code that exploits known or unknown vulnerabilities on the target system. Oftentimes, multi-vector attacks are designed to avoid traditional defences like anti-virus software, intrusion detection systems and other endpoint protection programs, which makes them elusive, difficult to detect and hard to defeat. Combined with the constantly evolving threat landscape and the fact that the speed, frequency, and severity of attacks have accelerated, it has become evident that financial institutions must keep investing in new state of the art security technologies (Advanced Threat Protection), ensuring that their cyber defense frameworks provide adequate response and defense-in-depth for identifying, stopping and recovering from multi-vector attacks.

Examples of multi-vector attacks in 2016 include cyber attacks on Swift bank customers[33] (attacking banks in Vietnam, Ecuador and Bangladesh) and the Tesco Bank Breach in the UK[34] (see also

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/).

3 Early warnings

3.1 Cloud Services and Big Data

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

[32] https://www.ncr.com/sites/default/files/brochures/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf

[33] http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C

[34] https://www.theregister.co.uk/2016/11/10/tesco_bank_breach_analysis/

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.[35]

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

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

Big Data is a broad term for data sets (both structured and unstructured) that is so large or complex that traditional database techniques and data processing applications are inadequate. Challenges include analysis, capture, data curation, search, sharing, storage, transfer, visualisation, and information privacy. The term often refers directly to the use of predictive analytics or other particular advanced methods to extract value from data.[36]

Fraud Description

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

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

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

Impact & Context

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

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

Suggested Controls and Mitigation

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

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

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

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

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

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

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

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

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

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

Final Considerations / Conclusions

Cloud computing and big data analytics are already mainstream, and some PSPs are commencing to move both non-core and core applications to cloud providers. Obviously this will result in a reduction of IT costs, complexity and time to market for those PSPs. However, necessary steps need to be taken to mitigate the risks under cloud computing as lack of the appropriate security controls and governance could easily lead to fraud. Besides traditional security best practices, care should also be taken in complying with regulations such as data privacy and security. Having a strict cloud governance control over the whole lifecycle of the applications running and data processed or stored by a cloud provider is vital. Moreover, particular emphasis should be put on achieving the control of the security mechanisms in the cloud services, contractual clauses that ensure the necessary security checks, fulfil the compliance obligations (e.g. data privacy, exit clause, right to audit) and share liabilities between both parties. Finally, international standards such as NIST, ISO 27001, SSAE 16 and COBIT should be carefully considered and applied on these new technologies, as well as internationally recognised frameworks such as the one developed by the CSA. Moreover new standardisation and guidelines developments on cloud computing services[37] need to be monitored and applied as they become available.

3.2 Internet of Things (IoT)

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.

Fraud Description

Like traditional computers and networks, IoT devices pose at least similar risks. Because IoT devices are connected to the internet, they represent new targets for data exposure and attacks. They can be infected by a malware and be compromised by fraudsters or their communications could be intercepted (unauthorised access and use of the device, misuse and disclosure of personal information). But due to the nature and the different types of the IoT devices (different hardware, firmware and operating system), the risks and the type of attacks may differ from those of the traditional computing devices. Today, with a smart TV, which is connected to the internet and has built-in capabilities and applications, a consumer could perform payments. The same exists for point of sales or other similar devices which support contactless technologies (NFC). Wearable

[37] see for instance:

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

objects are another example. All these IoT devices change the traditional means of payment (they actually expand the scope of use of these means) but it is more complex to enforce security upon them. For example, how easy is it to notify and apply a security update or hotfix to mitigate a critical vulnerability in a smart TV? On the other hand, many enterprises do not take seriously the security of an IoT device, as they do for the traditional computing devices. They do not even lock down the devices in order to be secure against typical attacks, because they do not realise that these new devices pose similar risks and are targets for attacks too. The lack of usage and incentive of common standards in security such as encryption in IoT devices make them more attractive for attacks, and we are increasingly seeing new forms of extortions, botnets hacks, data theft and even physical harm. New potential use of 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.

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 be increased 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 be increased if no countermeasures be taken. Both consumers and enterprises will face new types of attacks, depending on the types of the IoT devices. These devices will be hard to be controlled if an adequate security level is not designed from the beginning and maintained through their lifetime.

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 defense mechanisms.
- Adopt security and privacy by design: security for the devices, infrastructures, software and data must be adopted from the beginning and follow each phase of the project.
- Implement strong authentication and authorisation controls in every communication and exchange of data. Ensure the identity of the interconnected devices, sign and certify, where applicable, the associated applications.
- Monitor all service providers involved for security and privacy compliance.
- Device to device communication must be always secure (e.g. use of encryption, devices identification).
- 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.

Final Considerations / Conclusions

Enterprises across the world try to find new ways of doing business and IoT provides new opportunities. As an example, Distributed Ledgers is one of these technologies entering the market. But like every new way of business, this incurs risks that should be handled appropriately. Since these "things" don't look like traditional computers, they aren't treated like computers. As a result enterprises are often not taking adequate measures to ensure that they have an acceptable security level. The latest DDOS and attacks provoking a massive attack on Twitter, Spotify and Google due to a botnet partially created out of CCTV, routers, intelligent bulbs and other IoT is revealing that this type of malware is here to stay and is due to create new frauds related to IoT and payments or ransomware attacks on IoT such as heaters, air conditioning, door locks or intelligent refrigerators.

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

3.3 Virtual currencies

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"[38] 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"[39], 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. As a consequence, 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

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

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

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 decentralized 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.

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 using a combination of open source research, commercial tools and information provided by private sector, so there are solutions that can be put in place to avoid or at least diminish fraudulent transactions.

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 bitcoin transactions

Although all bitcoin transactions are stored publicly and permanently on the network by means of blockchain technology, the identity of a user behind an address can remain unknown allowing the fraudsters to move and cash-out the stolen funds anonymously. As such it is used as a vehicle for criminal activities such as money laundering.

Attacks to large bitcoin exchange traders

There have been a few cases[40] of bitcoin exchange traders suffering data breaches were customer bitcoin accounts have been hacked, massively compromised and as a consequence bitcoin funds retrieved from those accounts. Many of these hacks have caused the company failure and subsequent bankruptcy.

---

[40] http://www.forbes.com/sites/cameronkeng/2014/02/25/bitcoins-mt-gox-shuts-down-loses-409200000-dollars-recovery-steps-and-taking-your-tax-losses/#7b52c5a57ed6,

http://www.theverge.com/2012/8/10/3233711/second-bitcoin-lawsuit-is-filed-in-california,

http://observer.com/2011/08/mybitcoin-spokesman-finally-comes-forward-what-did-you-think-we-did-after-the-hack-we-got-shitfaced/,

http://www.breitbart.com/news/bitcoin-tanks-after-hong-kong-exchange-hacked/,

http://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/

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

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

Bitcoin Wallet compromise

The increase of interest showed by fraudsters in bitcoins currency held by individuals is boosting the number of stolen credentials to gain access to bitcoin wallets.

Bitcoin wallets typology are diverse like desktop wallets, mobile wallets, online wallets, hardware wallets 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 this wallet credentials.

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.

Impact and context

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

Suggested controls and mitigations

There are some recommendations that can help prevent fraud such as the Ponzi schemes. The Securities and Exchange Commission suggests several red flags42 to detect their characteristics. There are also some Bitcoin wallet security best practices that help to protect these wallets.[43]

The links to this document highlights the importance to establish controls and mitigation plans under the daily cybersecurity plan based on risk management. Particular care

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

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

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

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 resilience in worst case scenarios.

Conclusions and final considerations

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

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

4 Conclusions

During the last year cybercrime has proven to have a greater degree of professionalism regarding organisation and sophistication of the attacks.

The number of D(DoS) attacks is still growing and they are still frequently targeting the financial sector.

Also social engineering attacks and phishing attempts are still increasing and remain instrumental in combination with malware. Whereas before customers, retailers and SMEs have been the main focus, the last year more and more company executives, employees (through CEO fraud), financial institutions and payment infrastructures appear to become preferred targets.

Malware remains a major threat against cyber security for everybody in the society. More in particular ransomware has been on the rise during the past year. This type of attacks 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, by following a few simple advices the risk of such attacks can be reduced. The main problem is to make users understand and follow up on these advices. Awareness campaigns are one of the best tools to do this for customers. Such campaigns could be coordinated on a national level to ensure the best penetration. Such advices as, update your software, do not use an administrative account, disable macros from office documents, utilise an antivirus package and firewall if possible are all solid, but the most important advice is to use common sense and think before you click. By following these advices the risk of being affected by malware, social engineering and phishing is reduced significantly. Similar awareness must be in place for the employees of the PSPs.

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 a still increasing level of professionalism among the attackers whereby addresses of infected computers or bots are sold or rented, the usage of IoT devices (such as CCTVs and home routers)

for launching DDoS attacks was 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.

Also multi-vector attacks are on the rise and have been targeting a number of financial institutions over the past year. Advanced Persistent Threats and 0-day attacks cannot be detected and encountered with the traditional defense mechanisms.

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

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

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

Another important aspect to mitigate the risks related to payments is the sharing of fraud intelligence and information on incidents amongst PSPs. However often this is being limited by existing regulations related to data protection, even more so in the case of cross-border sharing.

Finally, PSPs must understand the emerging threats, the possible impacts and should keep investing in appropriate security technologies.