enisa

THE EU CYBERSECURITY AGENCY

FINANCIAL FRAUD IN THE DIGITAL SPACE

November 2018

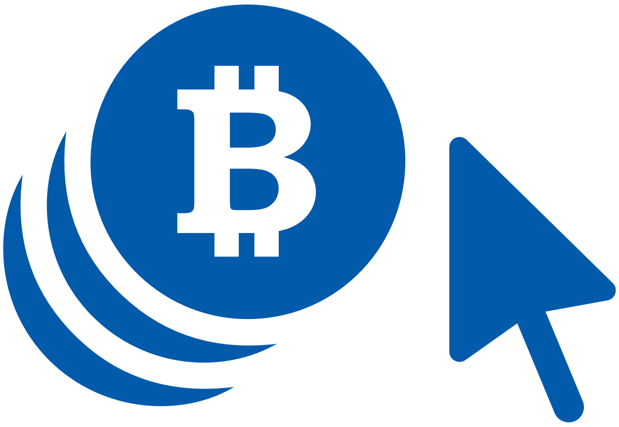
EUROPEAN AND GLOBAL PERSPECTIVE ON ONLINE FRAUD

Today, more and more purchases are done through online payments. The online world offers the convenience and ease of buying goods or paying for services through payments via your computer, tablet or mobile phone.

However, the use of online payments is not without its risks. Every year, the finance sector reports losses in the billions. According to the UK National Audit Office (1), individuals lost £10 Billion in 2016, which translates to almost 2 million cyber-related fraud incidents. If current trends continue, online fraud may overtake plastic fraud by the year 2020.

Based on a report from Worldpay (2), the EU will continue to be amongst the leaders regarding the use of digital wallets and conducting mobile payments in the next three years. According to the report, digital wallets, like PayPal and AliPay, are still considered to being the norm for online purchases and their use will continue to grow making them the number one payment choice for online purchases in the next three years as meanwhile the use of credit and debit cards will decrease.

In 2015 and 2016, the practices of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) came under SWIFT members’ scrutiny as they allowed for too much discretion on the use of the end equipment, which was thought to be a vulnerability. Allegedly, a Central bank in Asia that used the SWIFT network was involved in one of the major cyber-attacks, which led to the loss of 81 million dollars (4). The SWIFT network allows banks to process international transfers each day and is considered to be the backbone of international money movement. An organized crime organization was able to obtain a bank employee’s SWIFT logon, which they then used to take advantage of previously cancelled or rejected payment requests. They were able to alter the amounts and destinations on the transfer requests and reissue them. As a result, the crime organization was able to withdraw money from specific bank branches at specific timing from the other side of the world as well as launder it in gambling establishments across the border.



In another attack early in August 2018, US $13.5 million were stolen from India's Cosmos Bank (5). It was an attack that has exposed limitations in the measures banks use to defend against targeted cyber threats. The attack was a more advanced, well planned, and highly coordinated operation that focused on the bank’s infrastructure, effectively bypassing the four main layers of defence. As a result, the details sent from the payment switch to authorize transactions were never forwarded to the core banking system, so the checks on card number, card status, PIN, etc. have never been performed. Instead, the request was handled by the malicious proxy deployed by the attackers sending fake responses and authorizing transactions.

A similar attack was carried out against British Airways in August 2018 (6), when credit card data was stolen by injecting code directly onto the company's website, which is also used by the mobile app. Through the injected code, credit card data was transmitted to a website controlled by the criminals.

Stolen or compromised data usually is found in the Dark Web where it is usually offered for sale in Dark Web marketplaces alongside other illegal content. Latest exploits, drugs and stolen sensitive data (credit cards, identities) are some of the most common items that can be found there.

The Dark Web exists in the Internet, but requires specific software to access it, e.g. The Onion Router (ToR) or Invisible Internet Project (I2P). The idea behind this type of network is that access is anonymous and untraceable, although reports exists that government agencies were able to find a way to trace and find people using such services.

Hacking groups and hacking services can also be found in the Dark Web. They offer different services like network penetrations and/or denial of service attacks on behalf of someone who is willing to pay.

In the Dark Web payments are usually conducted via cryptocurrencies, mainly because these types of payments only require a unique identifier from both sides. This unique identifier is not officially associated with any identity which makes payments difficult to attribute to a specific person or organization.

CHALLENGES IN RESPONDING TO ONLINE FRAUD

In this article, online fraud is considered to be any fraudulent activity done through any Internet related means. Some key fraudulent schemes are using email, websites or online communication messengers (e.g. WhatsApp, Facebook Messenger) to conduct fraudulent transactions or to trick victims into giving away their personal information. In most cases, the criminals are looking for bank logins, credit card data, or personal data that can be used to impersonate a victim. There are a wide range of challenges that the financial system needs to tackle to protect against online fraud. They can be split into technical and legal challenges.

2.1 TECHNICAL CHALLENGES

Phishing and social engineering

These schemes target the user by phishing emails and social engineering exploiting different communication channels (e.g. phone, email, SMS) and data about the user available in the public domain (e.g. social media sites, search engines). The data sought by attackers using social engineering are often credit card data and personal data that the user knows about. Stolen credit/debit card or prepaid card details, can be either monetized (e.g. sold in underground market forums like the Dark Web) or used for fraudulent payments. Stolen personal data of the user can be used for impersonation attacks and for identity theft.

Malware

Malware is any piece of software or code that has a malicious intent. Once again, in 2017 malware is the most frequently encountered cyber threat, according to the latest ENISA Threat Landscape (3). Also based on that report, businesses have experienced far more threats in 2017 than they had in 2016. Financial malware still relies on web-based attacks. Most of the known financial malware (i.e. Zeus, SpyEye, Carbanak, and many others) take advantage of browser exploits such as the latest one called Disdain or utilize man-in-the-browser techniques.

Uploading malware to Poinf-of-Sale (PoS) or automated teller machines (ATMs) (e.g. Carbanak, Malum PoS) exploits security weaknesses such as use of insecure access to PoS or ATM devices. Once the malware is installed on the terminal, the attacker can remotely steal payment data that transact through the card readers and conduct fraud.

Mobile devices threats

Mobile devices have become the norm today for making online payments. Most of the threats affecting these devices are very similar to a desktop computer or a laptop, but due to its size, mobile devices offer additional opportunities for an attacker.

Mobile devices usually do not offer the same protection as desktop PCs as they rarely run an antivirus software, a firewall, etc. With the introduction of new mobile payment services , they will be a more interesting target for attackers. Abusing a lost or stolen device to make online transactions is a very common threat. Another could be, installing malware on the device to tamper with or gain access to mobile application for online transactions.

Payment systems compromise

Payment Service Providers (PSPs) offer terminals for payments as well as aggregated payment services for merchants by processing data from different channels, including face-to-face (card present) payments, online payments and mobile/contactless payments. PSP payment gateways represent an interesting target for attackers that seek to compromise the payment data in transit from the merchants to the different acquiring banks. Attackers might seek to compromise software vulnerabilities, the payment gateways hosted at the payment service providers for instance by exploiting unauthorized access to payment gateways and weaknesses in enforcement of internal payment service providers' security controls and measures.

Network Attacks

Denial of Service and/or Distributed Denial of Service (DoS/DDoS) attacks targeting the availability of any internet-exposed services hosted by payment network organization (banks, payment service providers, etc...) can affect online payment services. These attacks might affect transactions that require real time access by payment applications to the payment services. They may also block the legitimate access for the consumers to their bank accounts, and thwart online payments.

Man-In-The-Middle (MiTM) attacks against the POS and ATM terminals are enabled by weaknesses regarding the end-to-end encryption between the terminal and the server. If encryption is not properly configured or non-existent, information could be stolen and used for abuse later. Attackers can also attempt to exploit network security weaknesses such as a lack of firewalls to protect the internal network or vulnerabilities in POS/ATM software and misconfigurations (e.g. not enforcing minimum privileges to access terminals and servers).

The complexity of the financial ecosystem makes it difficult to recognize new attack vectors, as well as attacks involving the abuse of connectivity between multiple organizations in the system.

Third party trust

Cloud services are an on-demand service model for IT provision often based on virtualization and distributed computing technologies. More and more financial institutions are moving their systems into the cloud. The benefits of the cloud are very clear to the institutions – cost savings, flexibility and resilience, are just some of the key advantages.

With cloud services, the security model changes. Although the liability stays with the financial institution, some of the security controls are with the cloud provider and this brings additional security challenges. One of the key challenges that we have seen in cloud adoption is isolation failure, which means that there is no proper access to the resources. Another challenge is the customer management interfaces of public cloud providers, which are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities.

2.2 LEGAL AND POLICY CHALLENGES

It is often argued that law follows technology. Finance is another area where this mantra holds true. In the rush to deliver business models that cut costs, appear more convenient and flexible, the opportunity for financial fraud in the digital world increases. The deployment of new digital technologies continues to challenge law makers and regulators. A mobile phone being used as a digital wallet for transactions of cryptocurrencies will pose a challenge for most lawyers and law enforcement officials working in the digital ecosystem.

While the financial industry seeks to capitalise on the use of digital technology and users follow as unwitting or unwilling participants, some basic questions remain unanswered from the end user perspective. The end user has been pushed to using online platforms and mobile apps that pose a challenge even to the most literate computer user. But what happens when something goes wrong and money is mislaid, lost or stolen? Is there any insurance to cover the loss? And who is liable? Is it the app manufacturer, the financial institution that promoted these technologies, the security consultants who should ensure that the technology is secure or the innocent end users who will be accused of negligence and may thus not be in a good position to defend themselves?

The concept of a zero-day software vulnerability is mentioned scarcely and even more rarely understood by many stakeholders in the digital financial transaction process. What this means is that the exploit may allow the confiscation of passwords, control of end user computers or mobiles at a time where there is no defence. Money can be moved to any part of the world in under a second.

This type of issue is rarely communicated to end users. While nobody is interested in undermining the need to use digital financial services, the risks need to be fully understood and addressed by all parties in an open and transparent way across all Member States in Europe.

It is submitted that only when this type of challenge is addressed that the necessary confidence of all stakeholders will be achieved and legislators and regulators have a clear role to deliver in this area.

EU’S RESPONSE TO ONLINE FRAUD

The European Union has recognized online fraud as a major challenge and has produced numerous policy initiatives to address the problem:

- **Directive (EU) 2015/849** on preventing the use of the financial system for money laundering or terrorist financing (4th Anti-Money Laundering Directive)
- **Directive (EU) 2015/2366** on payment services in the internal market (PSD2)
- **Regulation (EU) 2016/679** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- **Directive (EU) 2016/1148** on security of network and information systems (the NIS Directive)
- **Proposal for Directive 2017/0226 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA**

The 5th Anti-Money Laundering Directive, which amends the 4th Anti-Money Laundering Directive was published in the Official Journal of the European Union on 19 June 2018. The Member States must transpose this Directive by 10 January 2020. The new revisions will include virtual currencies, digital wallets and crypto currency exchanges in its supervision. This inclusion is based on the increasing use of crypto currencies by criminal organizations in cases like ransomware (Petya, NotPetya) and money laundering.

The EU institutions have shown a growing interest in the security of electronic payments. This interest has materialised in **the Directive 2015/2366/EU (17) on payment services in the internal market (PSD2)**.

In response to the start of the application of the **General Data Protection Regulation (GDPR)** on the processing of personal data, the European Banking Authority has published guidelines that aim at incident notifications, as well as guidelines on security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2).

The Digital Single Market Strategy further acknowledges the importance of a secure and trustworthy cyberspace. In order to support the needs of cybersecurity, the European Parliament and the Council approved the NIS Directive concerning measures for a high common level of security of network and information systems across the Union. The **NIS Directive** defines common security measures in terms of incident reporting and security measures for the Operators of Essential Services (OESs) and Digital Service Providers (DSPs). The NIS Directive came into force on August 2016.

The proposal for the Directive on combating fraud (2017/0226) is considered a major milestone as its idea is to strengthen the Digital Single Market Strategy and stop the organized cyber criminals in the EU. Its main objective is preparation for new technology cyber-crimes and cross-border cooperation.

The European Commission is pursuing the implementation of the European Cybersecurity Strategy, which, in combination with the European Agenda on security, provides a strategic framework for initiatives on cybersecurity and cybercrime. The European Union works on different initiatives supporting and ensuring cybersecurity, from enhancing the capabilities of the Member States to supporting international cooperation on cybersecurity and cybercrime. The following main EU bodies specialized in these topics are:

- The European Union Agency for Network and Information Security – ENISA
- The European Cybercrime Centre within Europol – EC3

ENISA was established in 2004 to bring a high level of network and information security to the European Union. The Agency works closely together with Member States and the private sector to offer advice and solutions on cyber security related issues. In September 2017, the European Commission launched the cyber security package, an important milestone for ENISA, as it contained proposals on the new mandate of ENISA, and on the EU cybersecurity certification framework within the Cybersecurity Act.

Besides these activities, 2018 is a year in which ENISA continued to invest in its core activities related to the NIS directive, the recently adopted GDPR Directive, eIDAS, European Cyber Security Month, European Cyber Security Challenge, Internet of Things, eHealth, etc.

ENISA aims to strengthen cyber security in three main areas: expertise, policy and capacity. Amongst the key tasks of the agency are identifying the cyber threat landscape and Computer Security Incident Response Teams (CSIRT) cooperation. Although, cooperation is on a more global level and related to many sectors, the financial sector is one of the key sectors involved in the information sharing.

ENISA was also one of the founding members of the European Financial Institutes – Information Sharing and Analysis Centre (FI-ISAC). The European FI-ISAC, is an independent organisation, that was founded in 2008 to facilitate the information exchange, e.g. between CSIRTs, banks and law enforcement. The institution has signed a Memorandum of Understanding with Europol EC3 to improve co-operation between the European banking community and European Law Enforcement Agencies.

Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU. Since then, it has been involved in many cyber-crime operations, one of the latest lead to arresting a criminal organization which was responsible for losses of EUR 1 billion. In March 2018, Europol's EC3 was involved in arresting the people behind the Carbanak malware that was targeting financial institutions. With the help of the cybersecurity group of the European Banking Federation, EC3 was able to identify related cyber incidents and trace financial flows.

THE WAY FORWARD

In general, it can be concluded that online or digital access brings ease of use to the consumers, but it also creates more requirements towards the industry with regard to securing the online services. An effective risks management program is of paramount importance. Identification of new threats and modus operandi needs to be included in the regular risk management programme.

Based on the trends from ENISA's latest threat landscape report, the complexity of attacks and sophistication of malicious actions in cyberspace will continue to increase. This will require more collaboration between institutions in the ecosystem to be able to respond to an ever-changing environment.

It is also safe to assume that most of the fraudulent activity will move to the digital world and will require additional measures to combat the threats. This also requires developing the needed skill set, both for the business side and for the regulatory side. Policy makers need to create proper conditions that will lead to better education in the area of cybersecurity. It will also require the adoption of new technical and procedural measures to understand emerging trends in malware, attack and malicious infrastructure tactics and adapt defences accordingly. Potential use of machine learning and artificial intelligence methods may be something to be desired in the future.

Recent developments in lawful interventions in cyber-space show the need to regulate various critical elements of the threat landscape such as state support of vulnerability discovery and utilization. These issues will require the development of practices regarding procedural, technical and legal aspects.

Governance Structure

In the cybersecurity strategy of the European Union, the EU reaffirms the importance of all stakeholders in the current Internet governance model and supports the multi-stakeholder governance approach. Indeed, the multi-stakeholder approach is fundamental to the development of successful standards, particularly in the area of Cybersecurity where public-sector requirements are implemented to a large extent by private sector service providers.

The European Commission has created the Cyber Security contractual Public-Private Partnership (cPPP). The aim of the partnership is to drive the cooperation between public and private actors in the research and innovation process in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software).

Incident Reporting

In order to gain an overview of the EU risk situation and on potential threat scenarios, the EU is dependent on the input from national competent authorities. Only with comprehensive data, the EU will be able to gain knowledge on current dangers to the sector.

ENISA plays a significant role in this process by providing support in the execution of aligned reporting schemes at EU level. With the help of ENISA a consistent implementation of incident reporting would make it easier for the different Member States. Monitoring of IT-infrastructure can be conducted by the institutions themselves or, in cases of smaller institutions with limited financial resources, by third parties. If needed, institutions should be supported in the development of the capacities for monitoring and incident reporting by public agencies.

Mandatory security incident reporting should also include obligations for competent authorities to report back to the affected institutions and inform them about security threats and other related issues. This will create additional incentives for institutions to cooperate with the government on incident reporting and ensures that vulnerable institutions are informed quickly about potential threats.

Trusted Information sharing

The identification of new threats and attack vectors is something that the community needs to be able to share and act upon in an efficient and effective manner. Being able to quickly deploy new protection mechanisms, or identify new attack patterns is something that will help the community in limiting the losses.

An information sharing platform is something that the EU commission has identified as something very valuable. As a result, the CSIRT network, created by the NIS directive, will use a common platform for information exchange between Member states.

Risk management programme

An effective risk management programme that focuses on mitigation of online payment application risks and identifies measures including detection of possible data compromise and fraud should be in place. To this end, all players in the chain should have a reliable and accurate fraud monitoring system, which reliably detects transactions outside the customer's baseline. They should also be able to effectively prevent further payments from a compromised online payment account.

To prove that adequate security measures are taken, regular testing on critical points of the network should be done. This should also be supplemented by the use of a proper threat intelligence to follow the modus operandi of the organized criminals. As the system is very complex and involves many players, it should be properly scoped and executed with minimal disruption of the system.

REFERENCES USED:

1. https://www.nao.org.uk/wp-content/uploads/2017/06/Online-Fraud.pdf
2. https://worldpay.globalpaymentsreport.com/ , 2017
3. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
4. https://www.theregister.co.uk/2016/03/11/bangladesh_bank_cyber_heist_1bn_dollars_nearly_stolen/
5. https://www.enisa.europa.eu/publications/info-notes/atm-cash-out-attacks
6. https://www.telegraph.co.uk/business/2018/09/06/british-airways-hacked-380000-sets-payment-details-stolen/

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For media enquires about this paper, please use press@enisa.europa.eu.

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This ublication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

Vasilissis Sofias Str 1
Maroussi 151 24
Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu