EUROPOL

EC3 | European Cybercrime Centre

The Hague, November 2019

Spear Phishing

A Law Enforcement and Cross-Industry Perspective

Recommendations & guidelines on how to prevent, respond to, and investigate spear phishing attacks.

Author: Europol EC3

Europol Public Information

EUROPOL | EC3 European Cybercrime Centre

www.europol.europa.eu

Executive Summary

This report is the result of the joint Advisory Group Meeting from March 26 – 27 2019, gathering over 70 representatives from private industry at Europol to discuss the threat of spear phishing. It contains the meeting's main conclusions and recommendations for organisations on how to combat this threat effectively on a technical, educational, as well as operational level. It concludes that spear phishing is still the main attack vector for cybercriminals to target their victims and shows that there are a number of readily available solutions that can help minimise the risk of a successful attack. At the same time, this report highlights some of the challenges related to information sharing and the investigation of spear phishing attacks, as well as what can be done collectively to improve the situation.

Contents

1 Introduction

In March 2018, the leader of the organised criminal group behind the Carbanak and Cobalt malware, causing over EUR 1 billion in losses for the financial services industry, was arrested by the Spanish National Police in an international, European Cybercrime Centre (EC3)-coordinated operation. Having started their criminal activities in late 2013, the group targeted ATM networks and financial transfers around the world by sending spear phishing emails with malicious attachments to bank employees. Responsible for up to EUR 10 million per heist, the arrest of the group's leader was hailed as a significant success for law enforcement in one of the most high-profile investigations into cybercrime targeting the financial services industry to date.

The Carbanak/Cobalt case is significant for two reasons. First of all, the modus operandi employed by this group provides a fitting reflection on the way sophisticated, and highly targeted spear phishing attacks are used by organised criminal groups to carry out various cybercrimes. Second, the investigation did not only involve successful cross-border cooperation between several law enforcement agencies, but also direct involvement of the private sector. The European Banking Federation, through their vast network of partners, provided intelligence, which turned out to be critical for the investigation of the gang and the eventual arrest of its leader.

The role played by the private sector in this operation is of particular importance, not only in this investigation, but in the fight against cybercriminals in general. Not only does the private sector hold much of the evidence of cybercrimes, but private party reporting of fraudulent transactions, information on criminal networks and data breaches are among the most effective measures to prevent and investigate cybercrime.

For this purpose, EC3 has established a vast network of partners. The EC3 Advisory Groups on Financial Services, Communication Providers and Internet Security, are networks of trusted private sector partners, each meeting at Europol three times a year to discuss and identify industry-specific cybercrime threats and trends, as well as to cooperate on concrete joint actions.

One year after the arrest made in Spain, spear phishing is still one of the most common and most dangerous attack vectors seen by both, law enforcement and industry. As a result, EC3 organised a Joint Advisory Group meeting from 26 – 27 March 2019 at Europol to discuss what industry and law enforcement can do together to combat phishing[1]. Over the course of two days, 70 global financial institutions, internet security companies and telecommunications providers shared insights into how phishing affects their respective industries and what can be done together with law enforcement to combat this type of cybercrime.

This report reflects one of the concrete outcomes of this meeting: to provide a unique, law enforcement-industry view on the threat of spear phishing. As such, the first section will give a brief introduction to phishing, before outlining some of the most common modi operandi. The guidance and recommendations are then structured around three main areas: technical solutions, prevention and awareness, as well as attribution and operational response. Finally, a conclusion will summarise the main points and offer a look ahead.

The scope of this product is deliberately broad; it is aimed at the general public, as well as at industry and law enforcement. It is meant to give an overview of the threat and what can be done to respond to it. For additional details, further reading is recommended and will be referred to.

Europol's European Cybercrime Centre would like to thank each and every partner in the private sector who has contributed to this report by attending the two day workshop or by providing written feedback.

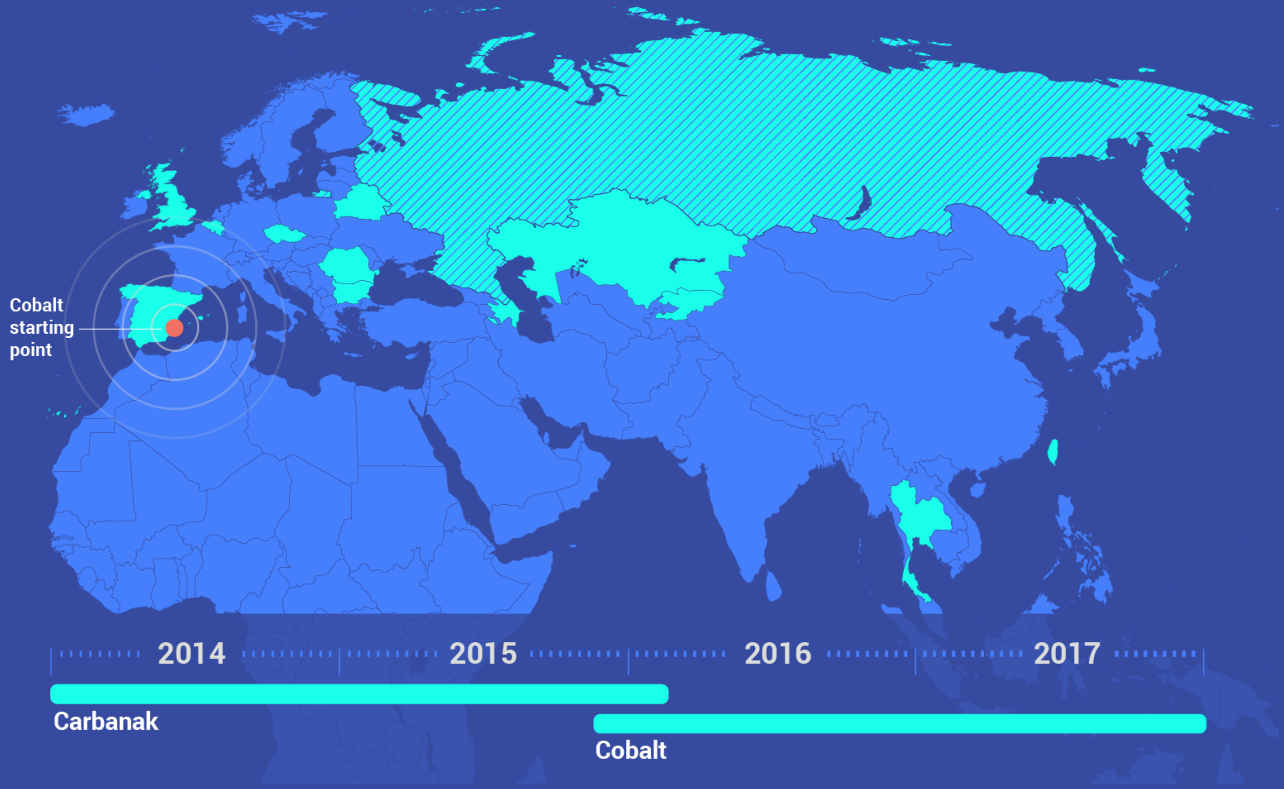
[1] Europol, "*Europol Teams up with Industry Experts to Combat Phishing*", https://www.europol.europa.eu/newsroom/news/europol-teams-industry-experts-to-combat-phishing, 2019

Carbanak / Cobalt

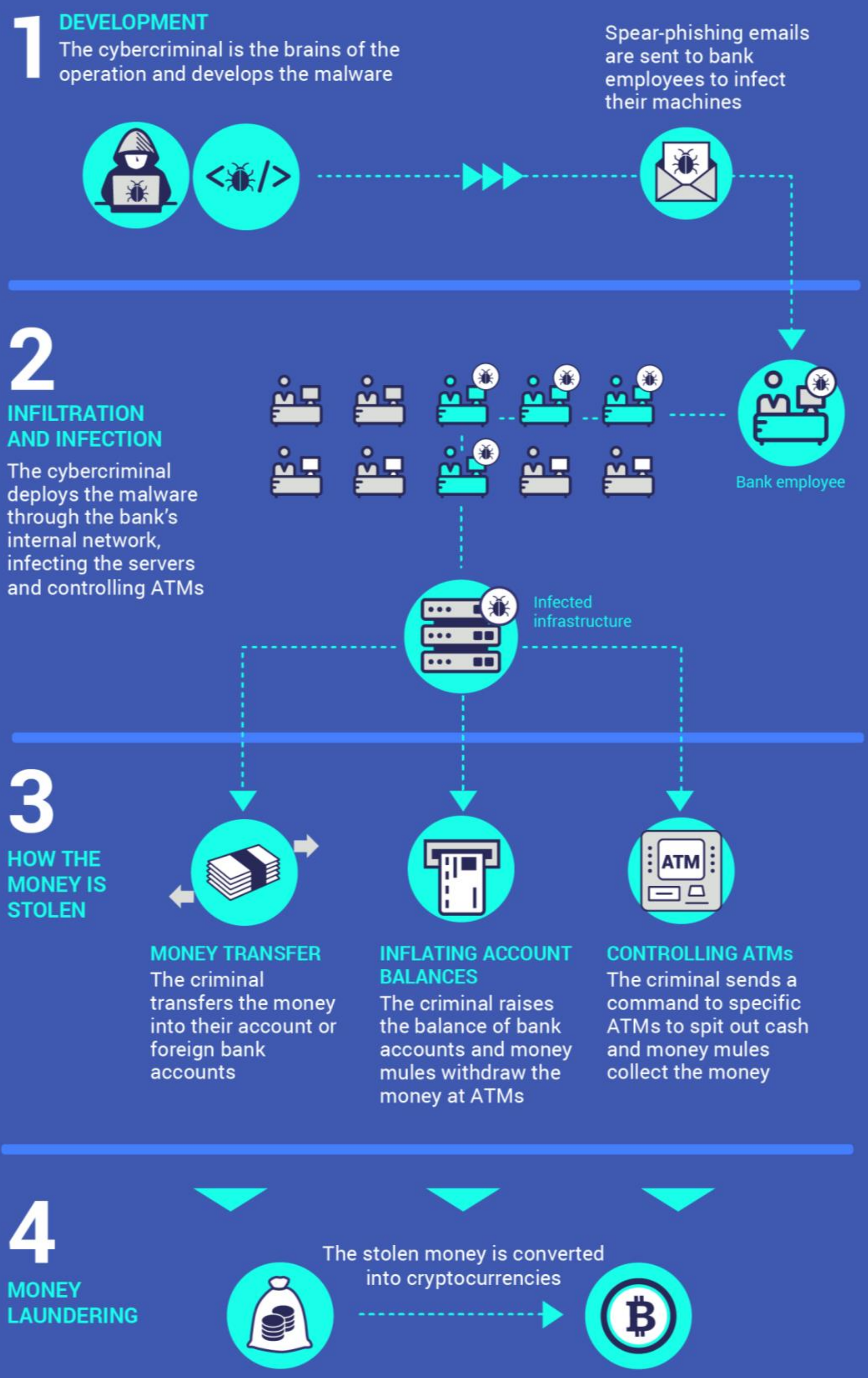
A global threat to financial institutions

● Countries affected by **Cobalt**

▨ Countries affected by **Carbanak** and **Cobalt**



How it works



1 DEVELOPMENT

The cybercriminal is the brains of the operation and develops the malware

Spear-phishing emails are sent to bank employees to infect their machines

2 INFILTRATION AND INFECTION

The cybercriminal deploys the malware through the bank's internal network, infecting the servers and controlling ATMs

3 HOW THE MONEY IS STOLEN

MONEY TRANSFER
The criminal transfers the money into their account or foreign bank accounts

INFLATING ACCOUNT BALANCES
The criminal raises the balance of bank accounts and money mules withdraw the money at ATMs

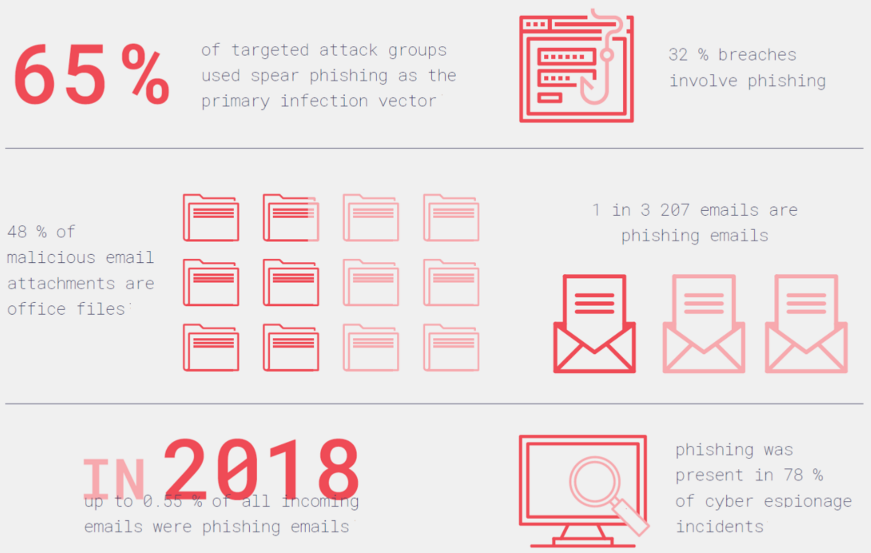
CONTROLLING ATMs
The criminal sends a command to specific ATMs to spit out cash and money mules collect the money

4 MONEY LAUNDERING

The stolen money is converted into cryptocurrencies

2 Background on the Concept of Phishing

Phishing is one of the oldest threats on the internet and a major vehicle for enabling the majority of cybercrime[2]. Phishing is a method of carrying out cybercrimes through the use of social engineering. Because it is a powerful facilitator of a broad range of crimes and because of the proliferation of leaked email addresses, the rate of phishing attempts keeps increasing, with the number of unique phishing sites detected being at an all-time high. In 2018, 75% of EU Member States had active investigations into phishing, while Europol stakeholders[3] consistently highlight phishing or related attacks as the single most common attack vector with 65% of all reported cases[4].



Phishing can be the vector for fraud, extortion, espionage or other malicious cyberattacks. It is an attack with a variety of sophistication and purpose used by malicious actors ranging from script kiddies and fraudsters to serious organised criminal groups and nation states[5] [6].

[2] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2019
[3] Europol manages a large network of stakeholders, including experts from Member States, partner organisations, as well as industry and academia
[4] Europol, *OSINT Dashboard*, 2019
[5] Bankinfosecurity.com, "*Nation-State Spear Phishing Attacks Remain Alive and Well*", https://www.bankinfosecurity.com/blogs/nation-state-spear-phishing-attacks-remain-alive-well-p-2643, 2019
[6] Wired, "*Russia's Elite Hackers May Have New Phishing Tricks*", https://www.wired.com/story/russia-fancy-bear-hackers-phishing/, 2019

In general, the goals of a phishing attack are the following:

- Obtaining login credentials to be used to gain access to assets (an account, a server, a network or similar)
- Obtaining other sensitive information, such as financial or personal data
- Delivering a malicious payload (such as ransomware, a keylogger or RAT[7])
- Convincing the victim of carrying out any other activity against their self-interest, such as transferring money or sharing personal data

Phishing can be targeted at specific individuals (e.g. targeted spear phishing attacks) or sent to a large distribution of email addresses with a varying degree of tailoring (e.g. untargeted phishing attacks).

Untargeted phishing campaigns aim to reach as broad an audience as possible with the goal of tricking recipients into clicking a link, opening a malicious attachment, disclosing sensitive information or transferring funds[8]. In the grand scheme of things, large-scale, untargeted phishing campaigns have become increasingly less of a threat. Given that successful phishing attempts largely rely on deceiving the victim through the use of social engineering, untargeted campaigns can often easily be identified and mitigated. The large number of emails sent out typically also means that relevant patterns (such as speech, content, domain registration information and even indicators of compromise) can be detected and filtered out automatically before ever reaching the intended recipients.

Targeted spear phishing attacks, however, are much harder to detect and to stop for the exact opposite reasons. A great deal of knowledge about the targets (and target environments) makes social engineering highly effective and means that a smaller number of attacks can lead to a much greater damage overall. Although generally only a small proportion of victims click on the bait, the significant danger of phishing lies in the fact that one successful attempt can be enough to compromise a whole organisation. Given this challenge, the focus of this paper lies on spear phishing attacks. **While other types of spear phishing exist[9], email continues to be the most widely used vector with the most severe potential consequences**.

Phishing attacks are becoming increasingly sophisticated and increasingly easily available also for non-technically skilled criminals through **ready-made phishing**

[7] Remote Access Trojan
[8] Advance Fee Fraud is a popular scam whereby the fraudster aims to convince the recipient to transfer money in exchange for an even larger sum, see Nigerian Prince Scam
[9] Other types of phishing, such as the less frequent Vishing (via telephone) and Smishing (via SMS) may be just as dangerous and are increasingly reported

kits. For instance, an increase in HTTPS encryption protocols and SSL certificates used by phishing sites may mislead victims into thinking that a website is legitimate and secure. Other methods, such as web page redirects, URL padding and others can further help obfuscate the true nature of a phishing attack. A recently discovered phishing attack, dubbed NoRelationship, successfully bypassed even sophisticated malicious file filters by exploiting link parsing weaknesses[10].

As the threat of phishing remains prevalent, the public and private sector are making significant efforts to raise prevention and awareness on the issue, to develop sophisticated tools to automatically detect and flag suspicious messages, as well as to investigate and go after the organisers of phishing campaigns.

The following sections outline the various types of spear phishing attacks, what can be done to counter them and provide guidance and recommendations on the way forward.

[10] ZDNet, "*NoRelationship phishing attack dances around Microsoft Office 365 email filters*", https://www.zdnet.com/article/norelationship-attack-dances-around-office-365-email-filters/#ftag=RSSbaffb68, 2019

3 Spear Phishing: Modi Operandi

3.1 Reconnaissance

The success of a spear phishing attack relies heavily on the criminal's ability to effectively deceive the target. This type of social engineering – convincing the target to trust the sender of the email as well as its contents – works best, the more information the criminal is able to gather. The information required to identify the right targets, as well as to create convincing spear phishing emails, is in most cases easily found online.

Depending on the goal of the attacker, both private, as well as corporate email addresses may be targeted. In the case of the latter, so as not to raise any suspicion, the attacker will often aim to demonstrate detailed knowledge, which only someone working within or with this organisation could possibly possess. This assumed credibility generally rests on two factors:

- Knowledge about an organisation's internal structure, processes and software
- Knowledge about an organisation's staff

In many cases, no sophisticated **espionage** is needed to acquire this information. On the contrary, most organisations keep a web presence offering a wealth of relevant information. In terms of detail about the first category – knowledge about an organisation's internal structure, processes and software – little can beat what organisations themselves publish as job listings for potential employees. A typical vacancy notice not only covers detailed descriptions of the tasks and responsibilities for a specific role in the organisation in question (*processes*), but also often includes information about whom the job holder reports to and manages (*structure*), as well as what skills and knowledge are needed (*software*). In addition, a mapping of vacancy notices may also provide a bigger picture of an organisation's strategic focus.

Similarly, it is often trivial to gather extensive **knowledge about an organisation's staff**. LinkedIn, for instance, is an online professional networking platform and counts over 610 million users in over 200 countries worldwide[11]. Websites such as these (in addition to other, country-specific equivalents) provide large amounts of information about individuals and organisations of interest to potential attackers. Through connections to other members, role descriptions and publicly available

[11] LinkedIn, "*About*", https://about.linkedin.com/?#, 2019

CVs, it is possible to gain a detailed understanding not only about an organisation's staff structure, but also identify potential interests of staff employees, which may subsequently be exploited[12]. LinkedIn, in combination with tools such as hunter.io[13], additionally provides a significant resource for identifying corporate email addresses, which can then be targeted by spear phishing emails.

Finally, **data leaks of email addresses and passwords** which are offered in batches on the dark web can provide an easy access for the criminal if basic cybersecurity hygiene practices are not followed. As will be shown in the following section, getting the target to trust the sender of the email is key to carrying out a successful spear phishing attack. And what sender is more trustworthy for employees than their own company's CEO?

3.2 Attack

Once criminals have identified their targets, spear phishing emails can be sent out to the respective address(es). Generally in spear phishing, an organisation can be breached in two ways: from the outside (i.e., phishing email sent from an external email address) or from the inside (phishing email sent from an email address belonging to the organisation).

The latter is often used for fraud and referred to as **Business Email Compromise** (BEC, also referred to as man-in-the-email or CEO fraud). **BEC is often aimed at convincing employees to transfer large sums of money to the criminal's bank account**, making use of the fact that an email coming from a trusted address – in many cases from a high-ranking staff member, such as the CEO – are typically met with little scepticism and significant trust. BEC has also been used to passively monitor an organisation's activity for the purposes of intelligence gathering. In most BEC cases, fraudsters gain access to email accounts of an organisation's employee, mainly as a result of obtaining leaked credentials on the usual dark web market places and similar communities.

[12] Criminals posing as recruitment agents, for instance, may approach their targets with a tempting job offer, for which they have to open a malicious attachment

[13] https://hunter.io/ can be used to identify patterns for organisations' email addresses

CEO/BUSINESS EMAIL COMPROMISE (BEC) FRAUD

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

HOW DOES IT WORK?

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

They have a good knowledge about the organization.

They require an urgent payment.

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

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

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

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

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

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

WHAT ARE THE SIGNS?

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

WHAT CAN YOU DO?

AS A COMPANY

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

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

Implement internal protocols concerning payments.

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

Establish **reporting routines** for managing fraud.

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

Upgrade and update technical security.

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

AS AN EMPLOYEE

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

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

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

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

Restrict information and show caution with regard to social media.

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

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

Spear phishing attacks may also make use of more technical means to gain access to an organisation. In general, we can distinguish two different technical MOs: files with attachment (which, once opened, infect

the target) or files without attachment (containing links or requests to browse to a website).

Regarding the former, as with BEC, the attack relies heavily on its ability to successfully deceive the target. The attacker aims to generate trust by reproducing familiar and trusted content. As such, the email may be formatted in a way to appear as though it was sent from a trusted bank, insurance or other third party, usually with a request to follow a link to a website. These links may appear legitimate and entice the target to click on them since they might be subdomains of legitimate websites (subdomain attack[14]), look similar (homograph attack[15] or misspelled URL[16]), be shortened (with the help of services such as tiny URL[17] or bitly[18]) or hidden in an image (such as company logo or a login button).

Once the target has clicked on the fraudulent link, a **replica of a trusted website** (phishing site) with legitimate branding usually appears with a prompt to enter login credentials or other sensitive information (including security questions, ID documentation and credit card details)[19].

In addition to appearing trustworthy by spoofing the look and functionality of legitimate websites, the use of Secure Sockets Layer (SSL) by phishing sites, encrypting traffic between a user's browser and the site, further deceives the target into believing a website to be legitimate[20].

Finally, an attacker may aim to get the target to **download and open a malicious file** in order to gain access to the system in question. The attached file may be disguised as an invoice or other business-related document, or even target an employee's specific personal interests. The malicious attachment, once opened, will then execute a script to infiltrate the target's system. Depending on the goal of the

[14] Such as: support.example.com, whereby the 'support' subdomain was previously used by example.com, before expiring and having been taken over by the attacker

[15] Such as: examp1e.com

[16] Such as: exemple.com

[17] Such as: tinyurl.com/yvdle

[18] Such as: bit.ly/1cY78RZ

[19] Trend Micro, "*Website Spoofing*", https://www.trendmicro.com/vinfo/us/security/definition/website-spoofing, 2019

[20] Krebs on Security, "*Half of all Phishing Sites Now Have the Padlock*", https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/, 2018

attacker, the attacker may choose to encrypt the target's files and demand a ransom payment (**ransomware**), escalate access rights and take remote control over the target's system (**Remote Access Trojan**), steal relevant credentials (**key loggers**), or monitor the network and gather as well as extract files.

While the execution of each of the two categories of attack differs slightly, they are often linked and one may be used to facilitate the other.

4 Responding to Phishing: Guidance and Recommendations

4.1 Technical Solutions

Given the prevalence of spear phishing attacks and the threat they pose to the greater cyber-ecosystem, a range of well-established measures aimed at addressing this problem are generally available and range from public to commercial solutions[21]. Technical defences against phishing attacks can be grouped into two principal categories: policies and software.

4.1.1 Security Policies

IT security policies identify rules and procedures governing how an organisation's staff can use and access IT assets and resources. Security policies can enforce the adherence to best practices and proactively close many of the gaps exploited by common phishing attacks. The below shall give a non-exhaustive overview.

Security policies can aim at preventing users from engaging in risky behaviours by:

- Disabling uncertified macros
- Enforcing two-factor authentication
- Communicating clear procedures to customers, such as correspondence only through the organisation's website[22]
- For phishing emails with file attachments, particular interest can be focussed on the file types. Organisations should define and enforce policies, such that unwanted, suspicious, or dangerous file types are not permitted. For example, many malicious phishing emails have EXE attachments, which is highly suspicious in many (if not all) organisations. The same may be said for LNK files, some archive file types, and so on.

Additionally, best practices related to monitoring and internal incident response policies can help shorten response times and mitigate potential damage. This further includes:

[21] A good overview has been compiled by the Global Cyber Alliance: https://gcatoolkit.org/smallbusiness/prevent-phishing-and-viruses/, 2019
[22] Instead of through email, for instance

- Running anti-leeching scripts on the web server to prevent images and resources from being abused by criminals when aiming to replicate a trusted website[23]
- Setting up a Sender Policy Framework (SPF) in the DNS[24] to validate all SMTP servers[25] and reject emails sent from non-listed servers
- Address filtering through protocols such as DMARC (Domain Message Authentication Reporting and Conformance), which helps organisations and people protect their own domain from unauthorised use (email spoofing)[26]
- Monitoring unusual account activity (multiple accounts ordering goods to the same shipping address, multiple transactions performed quickly from the same IP address)

Finally, coding best practices can minimise opportunities for attackers to exploit a vulnerable website, by:

- Checking for cross site scripting (XSS) vulnerabilities in network[27] [28]
- Employing the TARGET_top[29] directive to ensure that phishers cannot overlay a website with their own interface (iFrame traps)[30]
- Implementing an HTTP referrer header to check the origin of a request and to block email links as potential attack vectors[31]

4.1.2 Software

There are a number of commercial and open source solutions to mitigate the threat of phishing and automatically detect phishing attempts. Additionally, with the continuous progress made in artificial intelligence and machine learning, it may

[23] Attackers may try to use actual live images from a legitimate website. Anti-leeching can be implemented at the web server level and force attackers to save local copies of images, resulting in more effort required for a successful phishing attempt.

[24] Cloudflare, *"What is DNS"*, https://www.cloudflare.com/learning/dns/what-is-dns/, 2019

[25] Digital Shadows, "*Security Practitioner's Guide to Email Spoofing and Risk Reduction*", https://www.digitalshadows.com/blog-and-research/security-practitioners-guide-to-email-spoofing-and-risk-reduction/, 2019

[26] DMARC, "*Overview*", https://dmarc.org/overview/, 2019

[27] Acunetix, *"Cross-site Scripting (XSS)"*, https://www.acunetix.com/websitesecurity/cross-site-scripting/, 2019

[28] Subgraph, "*Vega Vulnerability Scanner*", https://subgraph.com/vega/, 2019

[29] A HREF="http://www.mysite.com/login.aspx" TARGET="_top" loads websites into the full body of the browser and breaks iFrame traps

[30] Smashing Magazine, "*How to Secure your Web App with HTTP Headers*", https://www.smashingmagazine.com/2017/04/secure-web-app-http-headers/, 2019

[31] Mozilla, *"Referrer-Policy"*, https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy, 2019

well be possible to use these techniques to help optimise successful detection and filtering of even sophisticated phishing attacks.

Generally, anti-phishing software employs a number of instruments:

- Meta data can be used to spot patterns regarding spoofed domain origins, display names, look-alikes and other techniques used by attackers to disguise their phishing attempts
- Technical data can analyse common patterns found in phishing attacks, such as location data (through IP address if available), timestamps and automatically blocking known malicious IP addresses/domains through DBLs[32]
- Linguistic data can spot commonly recurring linguistic patterns found in phishing attempts, for instance asking for credentials, personal information or other actions against the self-interest of the target
- Provision of email validation systems to facilitate filtering
- Chrome (as well as some other browsers) have extensions (e.g. https://toolbar.netcraft.com/) providing phishing protection, or the ability to monitor where login credentials are being used. It is possible to configure only using said credentials at trusted sites, which are regularly accessed, and block others
- Security Orchestration Automation and Response (SOAR) software can be used to automate the process of analysing a possible phishing attack to more easily know if someone has become a victim, to gather necessary information for investigations and to alert the correct contact points both internally and externally of an organisation

Software solutions can typically be acquired for free, or through the purchase of commercial licenses. Aside from technical detection capabilities, anti-phishing software further relies on extensive databases or feeds, according to which automatic filtering mechanisms are executed in or near real-time. Depending on the nature of the software, priced or for free, these databases are fed by either the developers themselves, or (more frequently) commercial or public third-party stakeholders, respectively. Because many feeds exist, different software and tools can convert them for a particular purpose (such as MineMeld or many others listed here: https://github.com/hslatman/awesome-threat-intelligence#frameworks-and-platforms).

[32] Domain Blocking Lists, used to block known malicious domains and IPs

4.2 Prevention & Awareness

Targeted spear phishing attacks can be difficult to detect even for professionals[33]. The use of social engineering, as per the previously outlined reconnaissance phase, makes this type of attack highly effective and – since it is targeting human judgement – hard to defend. Given that technical solutions cannot stop all phishing campaigns from reaching their intended targets, particularly not those of highly advanced actors, any efforts to fight against this type of crime must also have a strong educational component focusing also on **public awareness for both individuals and businesses**.

Prevention and awareness efforts focus mainly on general knowledge about the threat and specific training about how to detect and respond to a phishing attempt. Since spear phishing is highly targeted, it is equally important to address specifically tailored training to those employees, which are more likely to be targeted by cybercriminals (e.g. corporate financial departments and C-level executives).

4.2.1 Recognising the role of the user

Spear phishing relies on deceiving the target into clicking on a malicious link or attachment. In turn, a solid defense against phishing attacks needs to include a user base that is capable of identifying and responding to such emails in the correct manner.

Spear phishing emails can be identified through a number of indicators, although increasing technological sophistication of certain attackers can make a successful identification increasingly difficult. Whereas obvious spelling and grammatical mistakes could often give away the true origin of an email, attackers are now able to spoof websites and domain names, use secure certificates and even understand and exploit many organisation’s internal processes.

Still, there are a number of indicators, which can help successfully identify a spear phishing attack:

- **Spoofed a display name**. The actual email address of the sender can be revealed by hovering with the mouse pointer over the display name.

[33] NCSC, Cyber Security: Small Business Guide, 2019

- **Imitation of legitimate email addresses by slightly changing the spelling**. The authenticity of an email can be verified by careful reading the email address and making sure it is legitimate (i.e. gmaill.com instead of gmail.com).
- **Hidden links.** Are they hidden in images or texts? Hovering over them and taking a look at the URL will show where the links lead to. Additionally, domains can be checked for signs of malicious use with the help of publicly available websites:
    - https://urlquery.net/
    - https://checkphish.ai/
    - http://phishcheck.me/
- **No previous correspondence**. Has the sender been in touch before? Does the email come from an internal address? Is there anything out of the ordinary? Usually attackers will try to get the target to commit an action through a sense of urgency, i.e. to click on a link or to initiate a financial transfer.
- **Still suspicious?** Checking the email header will reveal information about the emails 'from' and 'return-path' addresses, the geo-location of the sending computer and the name of the sending computer or server.

If in doubt, the email should be forwarded as an attachment to a dedicated contact point within the targeted organisation.

Clear processes help employees identify attacks and report them accordingly. Similarly, organisations should have processes in place to deal with common threats such as Business Email Compromise. Secondary validation mechanisms, for instance, in case the usual point of contact is not available, can help an employee make the right decision under pressure.

The key to establishing a strong and resilient user base is training. The better users become at detecting spear phishing, the less likely the organisation is to be compromised by an attacker. The following sub-section takes a look at what organisations can do to get to their desired target state.

SPOOFED BANK WEBSITES

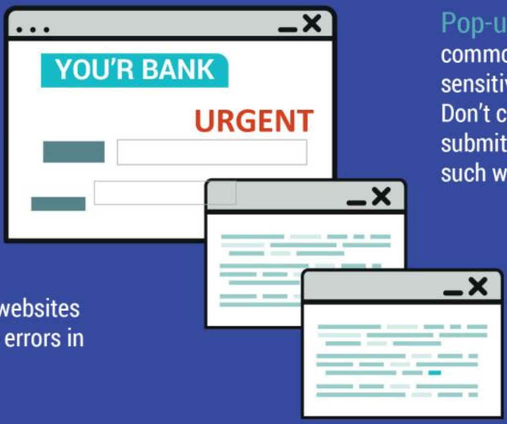
Bank phishing emails usually include links that will take you to a spoofed bank website, where you are requested to divulge your financial and personal information.

WHAT ARE THE SIGNS?

Spoofed bank websites look nearly identical to their legitimate counterparts. Such websites will often feature a pop-up window asking you to enter your bank credentials. Real banks don't use such windows.

These websites usually display:

Urgency: you will not find such messages on legitimate websites.



Pop-up windows: they are commonly used to gather sensitive information from you. Don't click on them and avoid submitting personal data on such windows.

Poor design: be cautious with websites that have flaws in their design or errors in spelling and grammar.

WHAT CAN YOU DO?

Never click on links included in emails leading to your bank's website.

Always type the link manually or use an existing link from your 'favourites' list.

Use a browser that allows you to **block pop-up windows**.

If something important really needs your attention, you will be alerted about it by your bank **when you access your on-line account**.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation

#CyberScams

EUROPOL | EC3 European Cybercrime Centre

BANK PHISHING EMAILS

Phishing refers to fraudulent emails that trick the receivers into sharing their personal, financial or security information.

HOW DOES IT WORK?

These emails:

may look identical to the types of correspondence that actual banks send.

replicate the logos, layout and tone of real emails.

ask you to download an attached document or click on a link.

use language that transmits a sense of urgency.

WHAT CAN YOU DO?

- **Keep your software updated,** including your browser, antivirus and operating system.
- Be especially **vigilant** if a 'bank' email requests sensitive information from you (e.g. your online banking account password).
- **Look at the email closely**: compare the address with previous real messages from your bank. Check for **bad spelling and grammar.**
- **Don't reply to a suspicious email,** instead forward it to your bank by typing in the address yourself.
- **Don't click on the link or download the attachment,** instead type the address in your browser.
- When in doubt, **double check** on your bank's website or give the bank a call.

Cybercriminals rely on the fact that people are busy; at a glance, these spoof emails appear to be legitimate.

Watch out when using a mobile device. It might be harder to spot a phishing attempt from your phone or tablet.

#CyberScams

4.2.2 Reinforcing anti-phishing training among employees

For prevention campaigns to be most effective, they should be dynamic and interactive. Awareness and education can, for instance, be achieved by systematically attacking users with real case scenarios by means of **a phishing simulation (phish your own employee**) with appropriate follow-up steps taken depending on the click-through-rates (CTRs) of the staff (increasing difficulty for good performers and providing tailored guidance for others). Other options may range from providing e-learning activities, to in-person workshops, can be an effective way to educate a large amount of staff in case of the former, or, in case of the latter, to tailor the educational content precisely to different departments' business realities.

In line with the above, board management influence is key in the creation and diffusion of prevention campaigns in order to make these initiatives more relevant to employees and consider them as a priority. At the same time, more senior level staff often lack basic awareness of the dangers of spear phishing and, thus, are often themselves one of the primary targets.

Much of prevention and awareness is closely linked to the aforementioned technical solutions. An intuitive user experience, which makes it easy to flag suspicious emails and which warns the user of potentially malicious content could significantly help users stay alert and make the right decisions when encountered with a phishing campaign.

Other areas of raising awareness should further not only focus on how to detect a phishing email, but also serve as a reminder to use several, strong passwords and multi-level authentication.

Examples of public prevention & awareness campaigns on phishing include:

- Europol's 2018 #CyberScams[34] campaign: The #CyberScams awareness campaign was launched in collaboration with 28 EU law enforcement agencies, 5 non-EU Member States and 24 banking associations in the context of the 2018 EU cybersecurity month. The awareness-raising material was developed in 27 languages and included information on the 7 most common online scams and how to avoid them, including various types of phishing.

- "Take Five to Stop Fraud"[35]: This national awareness campaign was launched by the Financial Fraud Action UK in order to help the public take back control and beat financial fraud – particularly bank transfer scams. The campaign is backed by the Government and delivered with and through a range of partners in the UK

[34] Europol, "*Take Control of Your Digital Life. Don't Be a Victim of Cyber Scams!*", https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/take-control-of-your-digital-life-don%E2%80%99t-be-victim-of-cyber-scams, 2019
[35] Take Five, "*About Take Five*", https://takefive-stopfraud.org.uk/about/take-five, 2019

payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector, urges you to stop and consider whether the situation is genuine – to stop and think if what you're being told really makes sense.

- EU Phishing initiative (EU-PI): EU PI is an EU-funded pilot project that provides an online reporting platform to identify new cases and trends as well as block attacks in most web browsers. The platform is available in France, Luxemburg and the Netherlands[36].

- The Anti-Phishing Working Group (APWG) is an international public-private partnership consortium aimed at uniting key stakeholders in the fight against phishing-based cybercrime. The group has over 2200 members ranging from business to government and law enforcement agencies, as well as NGOs, and facilitates data exchange, research and public awareness raising[37].

- The London Protocol[38] is an initiative launched by the Certificate Authority Security Council (CASC) in order to minimise phishing for sites with OV and EV certificates. The initiative is being implemented on a voluntary basis with the involvement of certification authorities.[39]

4.2.3 Way forward

There are a number of measures that can be taken as success stories and considered when planning a prevention and awareness campaign on phishing:

1) Encourage companies to provide corporate training for their own employees;
2) Explore the use of new channels to amplify the message, specifically social media platforms to spread phishing alerts among individual users;
3) Gather support from national authorities which could potentially sponsor anti-phishing campaigns;
4) Leverage public-private partnerships, such as the EC3 Advisory Groups, to create joint awareness campaigns;
5) Explore the use of proactive defence mechanisms.

[36] Phishing Initiative, "*About EU-PI Info*", https://phishing-initiative.eu/about/?lang=en, 2019

[37] Anti-Phishing Working Group, *"About Us"*, https://apwg.org/about-us/, 2019

[38] Imperial College London, *"Systems Analysis of Clinical Incidents: The London Protocol"*, https://www.imperial.ac.uk/patient-safety-translational-research-centre/education/training-materials-for-use-in-research-and-clinical-practice/the-london-protocol/, 2019

[39] Hashedout, *The London Protocol: Reducing Phishing on Identity Websites"*, https://www.thesslstore.com/blog/london-protocol/, 2018

4.3 Investigations & Attribution

The aforementioned technical solutions are designed to mitigate phishing campaigns before they reach their intended targets, whereas prevention & awareness campaigns are intended to educate potential targets in how to detect and report a phishing attack. Advanced threat actors, however, are capable of carrying out sophisticated phishing campaigns, which bypass conventional defences and are able to cause considerable damage. As such, if a phishing campaign can be attributed to a particular threat actor, law enforcement may decide to launch an investigation with a view to stopping their activities. The investigation of a spear phishing campaign, however, bears with it a number of challenges which need to be understood and which will be addressed below. Following that, guidance and recommendations on how to improve procedures and methods for better incident handling and cooperation with law enforcement will be given.

4.3.1 The Challenges for Incident Responders

Spear phishing attacks are arguably among the most severe threats faced by organisations today and can lead to persistent and significant damage in a variety of ways. In this light, incident responders face constantly evolving challenges in the response to and investigation of targeted phishing attacks. Mitigating and efficiently resolving a phishing campaign is a complex task; therefore it is extremely important to approach it in a coordinated manner.

A successful investigation of a phishing campaign requires analysis of all of its various phases (especially so where the attack is carried out in multiple stages) and the understanding of how to gather relevant intelligence for further handling.

Given the high frequency with which most organisations are targeted on a daily basis, the vast majority of incident responders focus on immediate mitigation in order to ensure business continuity. A lack of resources in this regard leads to most phishing attempts not being reported to law enforcement. This also means that the likelihood of reporting depends on the type of phishing attack: is the own brand name being abused for a campaign or are there other brand names involved? If the actual brand name of a company is being abused for phishing campaigns, counter measures are more extensive and reporting to authorities is more likely.

In addition to these challenges, sometimes organizations lack a clear, repeatable process that they may use to report suspicious activity directly to the incident response team or to Law Enforcement. Sometimes the activity is directed to a helpdesk, while other times it is sent to a monitored mailbox that is oftentimes overwhelmed with the information flow. In other cases, private companies often simply do not know how and when to report phishing incidents to law enforcement. In order for law enforcement to take on phishing cases, fraud losses must have already happened and the company should have conducted a prior threat assessment, given the lack of resources in many cases.

4.3.2 Implementing Procedures and Methods for Better Incident Handling and Cooperation with Law Enforcement

The first step to improve cooperation with law enforcement is **to improve reporting**. Dutch law enforcement and the private sector, for instance, have created a common incident reporting inbox[40] for victims of phishing campaigns. Through this inbox, companies and clients can report incidents so that law enforcement will assess the incident and open a case for further handling. The sheer amount of phishing emails being sent out on a daily basis make intelligence packages related to incidents and attacks a necessity and should ideally be submitted to the police in order to facilitate any further investigation.

In addition to conducting their own assessment, organisations may also want to work with telecommunications and hosting providers, which gather the data and can help identify threats and patterns of OCGs. Examples of effective collaboration between public and private sector in this regard can be found in the UK (Action Fraud in UK[41]) or the Netherlands (E-Crime Task Force[42]), where law enforcement and the private sector share best practices and information related to phishing campaigns and investigations. While these initiatives have proven to be highly effective, the implementation in different legislative frameworks may need to take in data protection related challenges.

4.3.3 DNS Abuse

The Domain Name System (DNS) underpins the Internet's ability to connect users and devices by translating abstract IP addresses (195.xxx.xxx.xxx) into domain names (example.com) that are recognisable and memorable for humans. While this

[40] Belastingdienst, "*Reporting Malicious and Phishing E-Mails*", https://www.belastingdienst.nl/wps/wcm/connect/bldcontenten/standaard_functies/individuals/contact/phishing-mails/reporting-malicious-phishing-mails, 2019

[41] Action Fraud, *"What is Action Fraud?"*, https://www.actionfraud.police.uk/, 2019

[42] Politie, "*Cybecrime"*, https://www.politie.nl/themas/cybercrime.html, 2019

serves as a critical function for the Internet to operate, the DNS is also frequently abused by cybercriminals.

DNS abuse in this context mainly relates to the registration of domain names for malicious purposes, such as to host a phishing site, on which an entire phishing campaign might depend. This type of abusive domain registration is often related to the infringement of intellectual property rights, where criminals register domain names closely resembling legitimate ones and effectively exploiting insufficient checks from domain registrars.

Threat actors exploit the weak anti-abuse measures implemented by some gTLDs registrars by registering domains with close similarity to the authentic domain. As emails sent from “look-alike” are mostly DMARC compliant, detection becomes more difficult, especially given the high volume email traffic, in which most work places operate.

To curb DNS abuse, registrars and registries should adopt aggressive anti-abuse measures to address DNS-facilitated crime and make their domain names as unattractive to bad actors as possible. These measures range from stronger authentication methods (KYC), including identity checks, to the use of data-based fraud prediction models which combine data registration and infrastructure metrics to identify and predict domain registrations made for harmful purposes. Best practices have been developed and successfully implemented by ccTLD operators[43] – they should now inspire also gTLDs registrars and registries.

4.3.4 The End of WHOIS

In addition to the issues related to efficient incident response and cooperation mechanisms, one of the greatest challenges to the investigation of spear phishing campaigns is the loss of WHOIS data. With the entry into effect of the GDPR in May 2018, the international law enforcement and cybersecurity community lost direct access to personal information on registrants of domain names from the WHOIS database.

Domains are critical for cybercriminals to set up and run phishing campaigns. As such, investigators and cybersecurity professionals alike had long considered the

[43] ICANN, “*DNS Abuse Mitigation. Session 5.1*”, https://gac.icann.org/briefing-materials/public/icann65-gac-briefing-05.1-dns-abuse-mitigation-v1-6jun19.pdf?language_id=1, [direct link to PDF document], 2019

WHOIS database as the key tool and starting point for the vast majority of investigations in this area. With WHOIS information no longer being directly available, investigations are now seriously hampered and delayed as a result. In a recent survey conducted amongst law enforcement authorities, only 33% responded that the WHOIS service still – at least partially – met their investigative needs. This rate indicates a significant decrease from 98% before May 2018.

This problem is further increasing in severity, as existing historical WHOIS records are quickly becoming outdated. WHOIS information no longer being directly available for law enforcement, public safety agencies and cyber security researchers significantly harms the public interest, the rule of law online and undermines efforts to investigate and prevent cybercriminal spear phishing campaigns.

5 Conclusion

Spear phishing is a real threat. It remains the principal attack vector for most cybercrimes and can cause significant harm to an organisation as a result. Given the fact that spear phishing is, by nature, highly targeted, it is critical to ensure that the right mechanisms for dealing with these types of attacks are in place.

Since spear phishing is such a commonly used vehicle for the perpetration of subsequent attacks, it is a threat that affects all industries. Additionally, sophisticated campaigns are often perpetrated by organised criminal groups, which are aiming to exploit this technique to generate large illicit profits.

As such, public-private partnerships, such as the EC3 Advisory Groups, provide an ideal platform to discuss what law enforcement and industry can do jointly to combat this type of threat. This report is the product of a dedicated two-day meeting, summarising guidance and recommendations from some of the leading experts from internet security companies, financial services organisations, telecommunications providers, and cybercrime investigators.

It embodies a truly public-private effort and outlines what an organisation can do to minimise this threat in practice. Ranging from technical solutions, to prevention & awareness campaigns and incident response, this document aims to provide a solid foundation from which a number of basic lessons can be learnt.

While this document is not aimed at being exhaustive, it is a practical overview, each section of which can be followed-up with by a deep-dive of its own. Having laid down this foundation, future reports may examine more closely and focus on a particular aspect of the fight against this type of crime.

In the future, spear phishing is likely to continue being a major attack vector for cybercriminals aiming to infiltrate an organisation. However, with joint efforts from law enforcement and industry, involving technical solutions, operational action, as well as prevention and awareness campaigns, we will continue working towards reducing this threat by bolstering our collective cyber defences.

EC3 would like to once more express sincere gratitude to all private sector partners who attended the joint Advisory Group meeting in March 2019 and who contributed to this report. Only by standing shoulder to should can we effectively tackle cybercrime in the European Union.

6 Use Case: Best Practice Response to Office 365 Phishing Attempt

The following steps are recommended to help secure the Office 365 environment and rectify any potentially impacted accounts:

1. Preserve Tenant activity logs and include the following:
   - Azure Active Directory Logs - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs
   - Unified Audit Logs - https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance
   - Mailbox Audit Logging - https://support.microsoft.com/en-us/help/4021960/how-to-use-mailbox-audit-logs-in-office-365
   - Message Trace Logs - https://docs.microsoft.com/en-us/powershell/module/exchange/mail-flow/get-messagetrace?view=exchange-ps
   - URL Trace Logs - https://docs.microsoft.com/en-us/powershell/module/exchange/advanced-threat-protection/get-urltrace?view=exchange-ps
2. Investigate Office 365 Tenant and other IT infrastructure, including a review of all Tenant settings, user accounts, and the per-user configuration settings for possible modification. Check for indicators of methods of persistence, as well as indicators an intruder may have leveraged an initial foothold to get VPN credentials, or access to other organizational resources.
3. Review delegate permissions and mail forwarding rules for all your mailboxes. The following PowerShell script can help to do this here: http://aka.ms/delegateforwardrules
4. Validate correct information for multi-factor-authentication and self-service password reset here: http://aka.ms/MFAValid
5. Enable multi-factor authentication for all users. Setup instructions can be seen here: http://aka.ms/MFAuth
6. Disable legacy account authentication: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication/
7. For every identified impacted account, automatically perform the following remediation steps by running the script located here: http://aka.ms/remediate

   a.Reset password (this secures the account and kills active sessions).

b. Remove mailbox delegates.

c. Disable mail forwarding rules to external domains.

d. Remove global mail forwarding property on mailbox.

e. Enable MFA on the user's account.

f. Set password complexity on the account to be high.

g. Enable mailbox auditing.

h. Produce Audit Log for the admin to review.

8. As part of your investigation, consider whether you should or must notify government authorities, including law enforcement.

In addition, it is recommended you:

- Read and implement our guidance on addressing unusual activity here: http://aka.ms/fixaccount
- Enable the audit pipeline to help you to analyze the activity on your tenancy here: http://aka.ms/improvesecurity. Once complete, your audit store will start populating with all activity logs and you'll be able to leverage the 'Security and Compliance Center's Search and Investigation' feature seen here: http://aka.ms/sccsearch
- Use the following script to enable mailbox auditing for all your accounts here: http://aka.ms/mailboxaudit1

Deliver or reinforce phishing/cybersecurity training for your employees. Possible resource: www.microsoft.com/safety.

EUROPOL EC3 European Cybercrime Centre

www.europol.europa.eu