Niklas Särökaari

PHISHING ATTACKS AND MITIGATION TACTICS

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2020

ABSTRACT

Särökaari, Niklas
Phishing attacks and mitigation tactics
Jyväskylä: University of Jyväskylä, 2020, 67 p.
Cyber security, Master's Thesis
Supervisor(s): Siponen, Mikko

Social engineering-based attacks, such as phishing and more targeted, spear phishing attacks remains to be one of the most common attack vectors used by threat actors. These attacks are most commonly used to obtain initial access into the target's internal network, for example through compromised endpoint. The access is then further leveraged to move laterally within the network to obtain access to sensitive information.

The public release of offensive security tooling and tactics, techniques and procedures (TTPs), such as disclosure of vulnerabilities with working proof-of-concept exploit code is also actively leveraged by several threat actors in their campaigns. More often advanced persistent threats (APTs) and other sophisticated threat actors are abusing existing functionality or exploiting already known vulnerabilities that have not been patched instead of concentrating time and resources into researching previously unknown vulnerabilities, also known as 0-days.

The research material in this master's thesis is based primarily on secondary sources that has been collected from academic research papers, professional literature and threat intelligence reports. Objective of this master's thesis was to perform a systematic literature review and analysis of observed tactics, techniques and procedures to obtain an understanding of what are the modern techniques that attackers are using to compromise organisations where the primary attack vector is phishing.

This master's thesis analyses some of the common techniques, such as how attackers and phishers are deploying their phishing campaigns. Furthermore, what are some of the most prominent evasion techniques being used as well as how email authentication could help organisations to mitigate some of the most basic impersonation attacks that attackers have been using successfully.

The results of this master's thesis show that attackers are still relying on abusing old functionalities through Microsoft Office documents and one of the most successful attack vectors to compromise an endpoint remains to be delivered through a Microsoft Office document that has malware inside of a Macro. The results of this master's thesis can be used by organisations to develop an understanding of some of the current threats and abilities attackers have and develop mitigations to protect their employees and assets.

Keywords: apt, email security, initial access, malicious attachment, password, phishing, social engineering, username

TIIVISTELMÄ

Särökaari, Niklas
Kalasteluhyökkäykset ja niiden torjuminen
Jyväskylä: Jyväskylän yliopisto, 2020, 67 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

Sosiaalinen hakkerointi, esimerkiksi kalastelu sekä erityisesti kohdennetut kalasteluhyökkäykset ovat edelleen yksi uhkatoimijoiden käytetyimmistä hyökkäystekniikoista. Kohdennetuilla kalasteluhyökkäyksillä hyökkääjä pyrkii saavuttamaan ensimmäisen jalansijan hyökättävän kohteen tietoverkkoon esimerkiksi saastuneen työntekijän työaseman kautta. Tätä pääsyä hyökkääjä käyttää liikkuakseen tietoverkoissa muun muassa saavuttaakseen kampanjansa tavoitteet, joka voi olla valtuuttamattoman pääsyn saaminen arkaluontoiseen tietoon.

Offensiivisten työkalujen sekä taktiikoiden, tekniikoiden ja menetelmien kuten haavoittuvuuksien ja niiden väärinkäyttämiseen tarkoitetun ohjelmakoodin julkaiseminen on myös raportoidusti edesauttanut uhkatoimijoita murtautumaan tietoverkkoihin. Nykyään uhkatoimijoille on tyypillisempää väärinkäyttää olemassa olevaa toiminnallisuutta tai avoimesti julkaistuja offensiivisia työkaluja ja haavoittuvuuksia sen sijaan, että uhkatoimijat käyttäisivät rajoitettuja resurssejaan ennestään tuntemattomien haavoittuvuuksien etsintään.

Lähdemateriaali on pääasiallisesti kerätty toissijaista lähteistä, kuten akateemisista tutkimuspapereista, ammatillisesta lähdekirjallisuudesta sekä uhkatietoraporteista. Tämän pro gradu -tutkielman tavoitteena oli systemaattisesti perehtyä kerättyyn lähdemateriaalin sekä saavuttaa ymmärrys miten nykyaikaiset uhkatoimijat toimivat toteuttaessaan kohdennettuja tietomurtoja, jossa pääasiallinen hyökkäystapa on kalastelukampanja.

Tässä pro gradu -tutkielmassa analysoidaan yleisimpiä tekniikoita liittyen siihen, kuinka uhkatoimijat rakentavat ja toteuttavat kalastelukampanjoita. Tämän lisäksi analysoidaan muutamia tunnettuja tekniikoita, joiden avulla on mahdollista ohittaa olemassa olevia tietoturvakontrolleja. Lopuksi otetaan huomioon se, kuinka organisaatiot voisivat puolustautua tyypillisimpiä hyökkäystekniikoita, esimerkiksi impersonointia vastaan.

Tämän pro gradu -tutkielman perusteella on havaittavissa, että uhkatoimijat luottavat pääasiassa Microsoft Office -dokumenttien väärinkäyttöön osana hyökkäyksiään. Organisaatot voivat hyödyntää tämän pro gradu -tutkielman tuloksia rakentaakseen ymmärrystä moderneista hyökkäystekniikoista ja uhkista, joita he kohtaavat.

Asiasanat: haitallinen liitetiedosto, jalansija, kalastelu, käyttäjätunnus, salasana, sähköposti, tietoturvallisuus, uhkatoimija

FIGURES

CONTENTS

ABSTRACT

“Give a man an 0day and he’ll have access for a day, teach a man to phish and he’ll have access for life.” – the grugq (Grugq, 2015)

1 ABBREVIATIONS

0-day (zero-day) = Vulnerability in a software that is unknown to, or unaddressed to or by the software vendor

2FA = Two-Factor Authentication

APT = Advanced Persistent Threat

APWG = Anti-Phishing Working Group

CTL = Certificate Transparency Log

DBIR = Data Breach Investigation Report

DKIM = Domain Key Identified Mail

DMARC = Domain Message Authentication Reporting

LE = Let's Encrypt

MFA = Multi-Factor Authentication

OST = Offensive Security Tooling

RFC = Request for Comments

SMS = Short Message Service

SPF = Sender Policy Framework

SSL = Secure Sockets Layer

TLS = Transport Layer Security

TTP = Techniques, Tactics and Procedures

VBA = Visual Basic for Applications

2 INTRODUCTION

Phishing involves the use of deceptive emails where cybercriminals and phishers create legitimate looking emails that resembles for example emails from financial institutions to convince their victims to divulge confidential or sensitive information, such as usernames, passwords or credit card information (Nero, Wardman, Copes & Warner, 2011).

Phishing attacks are generally divided into two categories: spear phishing, where attackers are sending individually targeted emails and which is also considered to be more effective than broad phishing messages, which target a wider population (Sanjay, Williams & Dincelli, 2017). Phishing should not be considered to be only a technological issue; it is also a social engineering attack where attackers are targeting and exploiting vulnerabilities in networked systems and are facilitated by users (Chaudhry & Rittenhouse, 2015).

Phishing attacks remains to be one of the most popular and easiest methods to commit cybercrime with an observed daily activity of over 30,000 daily attacks (Lewis, 2018). The Federal Bureau of Investigation estimated that the financial losses caused by phishing attacks, such as business email compromise (BEC) was over 12 billion US dollars in 2018 (FBI, 2018). According to the Anti-Phishing Working Group (APWG) phishing activity trends report (2020), during the 2nd quarter of 2020, financial losses especially originating from business email compromise attacks was increasing. It was also reported that 146,994 unique phishing sites were detected, and that 78 percent of all phishing sites are using SSL protection to encrypt network traffic (APWG, 2020).

Phishing and especially targeted phishing attacks are not just being used by cybercriminals to achieve financial gain. Several advanced persistent threat (APT) groups also utilize phishing techniques for their campaigns (Chen, Kakara & Shoji, 2019; Henderson, Roncone, Jones, Hultquist & Read, 2020). APTs are considered to be "one of the most serious types of cyber attacks" (Ghafir, Prenosil, Hammoudeh, Aparicio-Navarro, Rabie & Jabban, 2018, p.1) where a highly sophisticated threat actor is targeting a specific organization and the attack is carried out through several steps and the most common technique for initial access is spear phishing emails (Ghafir, et al., 2018).

The purpose of this master's thesis is to analyze and evaluate what are the current techniques, tactics and procedures (TTPs) of threat actors. Furthermore, purpose is to understand why these threat actors are continuing to be successful in breaching organisations although security awareness training and technological countermeasures are developed to battle against these types of attacks. The motivation behind this master's thesis is the author's own professional background in security consulting, which also includes designing and implementing targeted attacks to evaluate the overall security posture of organisations and to provide advice how to further protect the critical assets and services from sophisticated cyber-attacks.

2.1 Research objectives

The offensive side of phishing attacks as well as tooling and techniques behind these was chosen as there has not been much academic research being done or an overall overview, besides of threat intelligence reports regarding what offensive techniques and tactics are there and how are these being deployed by adversaries to compromise these organizations. Most of the research published on this matter focuses on the psychological side of persuasion, deployment of phishing as part of security awareness training and framework-based security controls that organizations could adapt and take into use to defend against phishing attacks.

As defenders it is crucial to understand what are the techniques, tactics and procedures that adversaries are using to breach organizations. Having this knowledge allows defenders and organizations to enhance their skills to build more resilient capabilities to prevent, detect and respond to targeted attacks where the initial access method being used is a targeted phishing attack. Objective of this master's thesis is to provide a high-level overview of the attack lifecycle regarding phishing attacks and the methods that adversaries have been using. This is done to provide more centralized insight into some of the most common techniques and tooling that is currently available that can be used to perform these types of attacks that are built and used against employees to obtain sensitive information or breach the external network perimeter.

Most of current offensive research is done by professional security researchers, which is then publicized either in personal or company sponsored blogs, security conferences, or in threat intelligence reports by security companies. These research papers and tooling are commonly published based on the TTPs that have been uncovered during breach investigations to provide defenders the same possibilities as adversaries to protect their organizations. This master's thesis tries to capture some of the most observed TTPs and mechanics behind targeted phishing attacks.

2.2 Research questions

This master's thesis concentrates on the prevalence of targeted phishing campaigns today as well as what are the techniques, tactics and procedures (TTPs) used by adversaries to obtain sensitive information, such as credentials or achieve initial foothold into organizations. This master's thesis tries to answer the following questions:

- Why these attacks are as successful as they are?

- What are the techniques, tactics and procedures commonly implemented in targeted phishing attacks?
- How to defend or mitigate against targeted phishing attacks and its impact?

2.3 Overview of research

The research method chosen for this master's thesis is grounded theory, which is one of qualitative research methods. Grounded theory was originally designed to create theories that were empirically derived from real-world situations (Oktay, 2012). Grounded theory was originally developed by Glaser and Strauss in the 1960s at the University of California (Mills & Birks, 2014). With grounded theory the objective was to develop a more defined and systematic procedure for collecting and analyzing qualitative data (Goulding, 2002).

As described by Goulding (2002) grounded theory has similarities and differences to other qualitative research methods, such as that the sources of data are usually the same. However, with grounded theory the researcher is allowed to include a much wider range of data sets in their research, such as company reports, secondary data and even statistics as long as the information and data collected has relevance and fit to the study. In grounded theory the emphasis is upon theory development and building. Furthermore, one of the essential features of grounded theory methodology is that the developed theory should be true to the data (Goulding, 2002).

In qualitative research there are two sources of data; primary and secondary. Primary sources of data are related to unpublished data that is specifically collected by the original researcher for their research purposes, such as interviews or fieldwork whereas secondary data is collected from existing sources, such as previously published books and journal articles (O'Reilly, Kiyimba, 2015). This master's thesis is solely based on data gathered from secondary sources. One of the critical factors when using secondary data is the validity and credibility of the data that is used in the research. Thus, emphasis while collecting secondary data for this master's thesis was put on ensuring that the data is academic research published in well-known journals and conference papers, professional literature or research published by international consortiums or companies that have done quantitative data analysis in regard to phishing as a phenomenon. The research was also supplemented with published newspaper articles mostly concentrating on analysis of published threat intelligence reports.

The data gathered for this master's thesis was initially divided by the source of the data; academic research paper, professional literature, threat intelligence report, newspaper article or other. Additional coding for the gathered data was performed in the form of initially analyzing the whole text to understand what the main themes of the text are. Once this was finished, additional selective coding was performed to further divide the text into categories such as; phishing, advanced persistent threats, attack lifecycle, email authentication.

As described in Qualitative Research by David Silverman (2016) in grounded theory the research is initiated with the definition of research question, which is then followed by data collection. Once data collection is finished the researcher will perform initial coding where the text is analyzed and summarized. Once initial coding is finished for the data collected the next step is to perform focused, or selective coding where the categories and properties are interpreted followed by theory building (Silverman, 2016).

Grounded theory was chosen as a research method for this master's thesis since the research objective was to perform systematic literature review covering previous academic research, professional literature and articles regarding spear phishing attacks, motivations behind it and what techniques, tactics and procedures are commonly utilized in these attacks. The second part of this master's thesis covers some publicly disclosed tooling and techniques that can be utilized to design and implement targeted phishing attacks against organizations and how to bypass technical security controls in organizations, such as multi-factor authentication.

As part of analyzing what are the common TTPs being used in targeted spear phishing attacks this thesis also includes an analysis of Advanced Persistent Threat (APT) groups as what are their processes of building and performing targeted attacks against organizations. This analysis was done by performing literature review on academic research papers on APTs as well as several threat intelligence reports that dissect and discusses certain groups operations that have been publicly attributed to certain nation-sponsored groups. Through the analysis of APT groups several frameworks have been built around of performing cyber-attacks with one of the most famous ones being termed as the Cyber Kill Chain by Lockheed Martin. During the course of this thesis an in-depth analysis is done regarding the TTPs that are commonly seen to being utilized to obtain initial access into a target environment.

Finally, this thesis will provide some recommendations in both technical and process level as to what should be taken into consideration in organization's security posture to limit the potential attack surface, which a determined attacker could take advantage of and how to limit the potential impact of breach in an organization due to a successful spear phishing attack.

2.3.1 Scope

Scope of this research is to evaluate on a high-level some common techniques and tactics as well as tooling that is available, which can be utilized to perform phishing campaigns. Additionally, this master's thesis will cover how Advanced Persistent Threat (APT) groups commonly operate to achieve initial access during their targeted operations. The objective of this research is to understand the TTPs that are publicly available and that how common these targeted attacks are and what organizations and defenders could do to mitigate against these attacks.

This research will not cover any opportunistic attack scenarios, such as where an adversary has taken control of a publicly accessible web site, which is then used as a watering hole or for drive-by attacks. Also, this thesis does not provide an exhaustive approach to all available techniques and tactics or tooling that is available.

2.3.2 Systematic literature review

This literature review includes analysis based on previous academic research that has been done regarding phishing attacks, especially focusing on the fact that how common these types of attacks are and why attacker's keep on breaching organizations through this attack vector. This literature review first approaches this matter on the reasons behind it why users click on phishing links and also dives into the demographics of phishing attacks where the purpose of the study was to identify are men or women more susceptible to social engineering attacks. These studies provide invaluable information to attackers as well since this information can be used to build better pre-text and target certain individuals that have been distinguished being more vulnerable to these attacks than others.

To provide more in-depth approach into this literature review regarding phishing attacks several threat intelligence and data breach investigation reports is analyzed to obtain first-hand information from business sector to distinguish what are the key motivators, targets and techniques that attackers use to compromise organizations.

All material gathered that has been used in this master's thesis are built upon the analysis of available professional literature regarding cyber security, academic research papers, research done by cyber security companies who analyze the techniques, tactics and procedures of known and unknown threat actors as well as non-profit organization's research based on data collected from private and public sector.

2.3.3 Analysis of Tools, Techniques and Procedures

The analysis of publicly disclosed tooling and techniques regarding phishing attacks and methods to bypass some security controls deployed in organizations to defend against these types of attacks was chosen to obtain understanding of the vast amount of capabilities that are publicly available. In addition to this, this approach was chosen to provide centralized knowledge for defensive teams in organizations regarding how these certain attack techniques and tools work and how organizations could potentially defend and mitigate their environments against these attacks.

The analysis of tools, techniques and procedures (TTPs) are concentrated on the initial phases of the attack lifecycle; reconnaissance, weaponization, delivery and exploitation. These are described in more detail in Section 6 (Attack lifecycle). The analysis will not provide an exhaustive list or in-depth analysis of each technique, but more of a high-level description of some of the most commonly deployed techniques that have been seen deployed by threat actors in the wild in the recent years. This analysis also covers case examples regarding Advanced Persistent Threat (APT) group attacks and their procedures regarding how these groups in general obtain initial foothold into a target organization and what techniques and tactics have been commonly used.

3 PHISHING

Andress (2019) defines phishing as a form of social engineering technique where attacker's objective is to collect target's personal information or install malicious software (malware) on their system. These can be achieved either by convincing the target to click a malicious link within the email that redirects the user into a fake web site that is built with the sole purpose of collecting sensitive information, such as credentials. The fake sites used in phishing typically resemble well-known websites, such as banking, social media or even the targeted organization's own sites. Some of these sites may look obviously fake with poor grammar and completely wrong domain names, while others are extremely difficult to distinguish from the legitimate site. Basic phishing attacks are usually sent as bulk to hundreds, or even thousands of recipients. The success rate in basic phishing attacks may vary a lot. To achieve higher rates of success, attackers may turn to spear phishing, or targeted attacks against specific companies, organizations, or people (Andress, 2019).

Hadnagy and Fincher (2015) defines spear phishing as a more targeted form of a phishing attack. With spear phishing, attackers take the time conduct research by collecting wealth of information about their targets. This information is used to make the attack look as legitimate and relevant as possible to trick the recipient to give out their information or install malicious software on their workstation (Hadnagy & Fincher, 2015). In spear phishing attacks, attackers typically send emails that have the look and feel of a legitimate email, which contains the expected logos, graphics, and signature block. Even the malicious link or attachment can be disguised to look legitimate (Andress, 2019). Because of the high sophistication of the pre-text and design, spear phishing attacks may be extremely difficult for users to detect and defend against.

Hadnagy (2011) defines pre-texting "as the act of creating an invented scenario to persuade a targeted victim to release information or perform some action" that the attacker could take as advantage (Hadnagy, 2011, p. 78). Pretexting gives social engineers an advantage. If the attacker is able to provide enough information within the phishing email that is true and give the target sufficient cause to believe that they've legitimate and reputable source the attacker's chances of success increases substantially (Andress, 2019).

3.1 Stages of a typical phishing attack

There are several types of phishing attacks where attackers can have either a large number of targets or they can only have a few, distinctively selected targets when it is known as a spear phishing attack. However, before attackers can actually initiate any phishing campaigns, they must first setup infrastructure to host and deliver their payloads or phishing sites. Figure 1 describes the high-level stages of a typical phishing attack as described by Oest et al (2020) in their research paper where they analyzed the life cycle and effectiveness of phishing attacks.

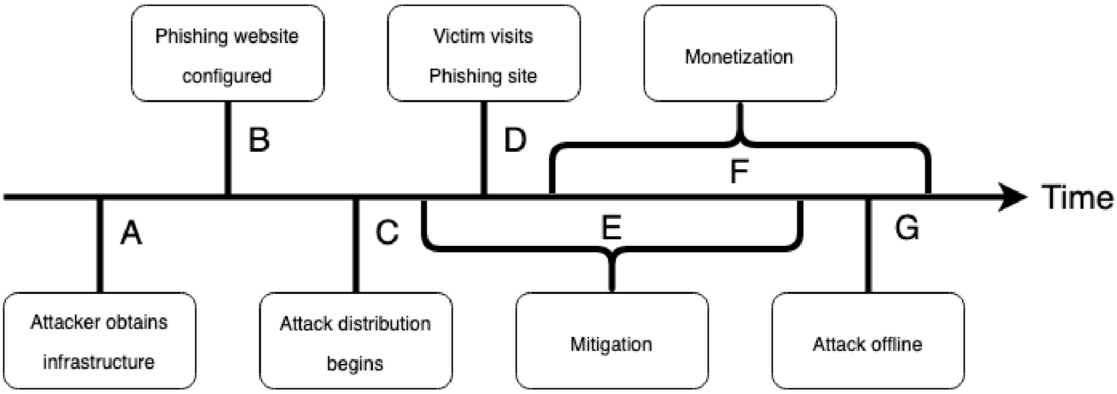

Phishing website configured
Victim visits Phishing site
Monetization
B
D
F
Time
A
C
E
G
Attacker obtains infrastructure
Attack distribution begins
Mitigation
Attack offline

Figure 1 End-to-end life cycle of a phishing attack (Oest et al., 2020, p. 363)

In the overview of the phishing attacks as described by Oest et al (2020) the attacker first obtains infrastructure (A) and configures a phishing website commonly containing a phishing kit that is hosted on this infrastructure (B), which is then used to either harvest credentials or supply malicious software to be downloaded. Once the website is operational, attackers start to distribute it to their victims (C), commonly through email after which victims start to visit the site (D). Depending on the organizations capabilities to detect that a phishing campaign is on-going and targeting their employees, for example through user reports the organization can start to mitigate the attack (E). In an optimal scenario, mitigative actions would occur before (D) when users have not yet visited the phishing site, thus preventing all future victim traffic. However, if this is unsuccessful it creates attackers a timeframe to start monetizing (F) their attack through stolen data or obtaining foothold into the network. The phishing site may go down either due to a take-down or by attackers themselves (G). However, once attackers have obtained data affecting the organization, whether they are credentials or access to the network the monetization still continues even though the initial infrastructure has been taken offline (Oest et al., 2020).

3.2 Previous research on social engineering

Previous research on phishing has been quite extensive ranging from studying the demographics and reasons behind why users are clicking malicious link or opening malicious attachments. Further research has been done also on evaluating the effectiveness of phishing campaigns as part of security awareness training in organizations. Most recent research has been revolving around evaluating the effectiveness of multi-factor authentication and the lifespan of phishing attacks from initial compromise to detection.

Siadatii, Palka, Siegel and McCoy (2017) summarized in their paper that prior research done on evaluating simulated phishing campaigns as part of security awareness training has shown that overall click-through rates and the likelihood that a user will submit their credentials to a phishing site is low. It has also been shown that an effective security awareness training can have a significant effect on decreasing the susceptibility of users falling victim to a phishing campaign. However, this was mostly limited to more persuasive campaigns and that embedded training is not deemed as useful in providing protection for users that are more susceptible to fall victim for a phishing campaign (Siadatii, et al., 2017).

Sheng, Holbrook, Kumaraguru, Cranor and Downs (2010) analyzed the susceptibility in demographics as who are more likely to fall victim of a phishing campaign. On average, women clicked 54,7% of phishing emails compared to 49% for men. It was also discovered that women were more susceptible to give out their personal information, 97 % of the time, to the phishing site compared to men where the amount was only 84 % (Sheng, et al., 2010). Based on the results of the research it was concluded that women are more susceptible than men to fall victim of a phishing campaign.

Research in this area has also been done on identifying the underlying reasons why users click malicious links that originate from a non-existing person. Based on the research done by Benenson, Gassmann and Landwirth (2017) the most common reason why recipients clicked the phishing link was curiosity (34%), the message fit the recipient's expectations (27%) or they though that they might know the sender (16%) even though the message came from a non-existent person. The survey also measured the reasons why some of the recipients did not click the phishing link. The most common reason for not clicking was that the message came from an unknown sender (50%). Secondary reason for not clicking the phishing link was that recipient believed the message to be fraudulent (50%). Another common reason for not clicking the phishing link was that the reception of the message did not fit the recipient's situation (39%) (Benenson, Gassmann & Landwirth, 2017). The findings present an interesting opportunity for attackers to try to impersonate as an employee of the company or organization they are targeting as there is a relevant success criterion where the recipient believe it is a legitimate message. Furthermore, it can be concluded that for attackers it is important to make the pre-text of the phishing message to be relevant for the recipient's job description since 39% of the survey respondents did not react on it as it did not fit for their situation.

Credential harvesting and account takeover are especially affecting organizations in the form of Business Email Compromise (BEC) where attackers have successfully obtained valid credentials and accessed employee's inbox to launch further attacks against the organization (APWG, 2020). Latest research done by Mirian, DeBlasio, Savage, Voelker and Thomas (2019) on the effectiveness of multi-factor authentication on protecting against account takeover found that enabling on-device prompts for multi-factor authentication is capable to prevent over 99% of automated attacks and 90% of targeted attacks.

Whereas SMS-based challenges were discovered to provide the weakest protection by preventing only 96% of attacks involving phishing emails and only 76% of targeted attacks (Mirian, et al., 2019).

3.3 Current state of the phishing

As part of this master's thesis the objective was to evaluate and obtain understanding of what is the current state of phishing campaigns that are designed to target private and public sector. Data gathered to evaluate this was taken from Verizon's Data Breach Investigation Reports (DBIR) covering from 2018 to 2020 and from Anti-Phishing Working Group (APWG), which is an international consortium that publishes quarterly reports about phishing statistics. The APWG Phishing Activity Trends Report is a quarterly publication that collects and performs analysis on phishing attacks and other identity theft techniques that are reported to APWG by its member companies and through its Global Research Partners. Verizon has been publishing its DBIR since 2007 and data gathered and analyzed consists of legitimate incidents covering a wide variety of industries; accommodation and food service, healthcare, financial and insurance, public administration, retail and so on. All incidents that are reported to Verizon are individually reviewed to create a common and anonymous dataset.

Starting from 2018 Verizon (2018) data breach investigation report included over 53,000 incidents and 2,216 confirmed data breaches. The third most common tactic utilized in these incidents and data breaches included social attacks, covering 17% of the data set. In the Verizon DBIR social attacks includes both phishing and pretexting attacks. Phishing and pre-texting covered almost all of the social incidents reported (98%) and breaches (93%). The most common delivery vector was email with 96%. The most notable difference between phishing and pretexting attacks in the 2018 DBIR was that pretexting is almost always financially motivated as 95% of the incidents including pretexting was more about acquiring information directly, such as asking money. Phishing however is almost evenly split between financial (59%) and espionage (41%). Based on the 2018 DBIR: "Phishing is often used as the lead action of an attack and is followed by malware installation and other actions that ultimately lead to exfiltration of data." (Verizon, 2018, p. 12). Another interesting point from the 2018 DBIR was that 70% of breaches associated with sophisticated threat actors, such as nation-state actors involved the use of phishing as an attack vector to achieve initial access. Based on the data set healthcare industry seems to suffer the most from social attacks as 14% of incidents involved either phishing or pretexting (Verizon, 2018).

Moving on to 2019 DBIR there was a definite spike regarding social engineering-based attacks based on Verizon's (2019) analysis. The 2019 DBIR was built upon analysis of 41,686 security incidents, of which 2,013 were confirmed data breaches. Overall, 32% of the confirmed data breaches involved phishing as a tactic. As of 2013 Verizon has reported that social engineering-based attacks have risen 18%. In regard to social action varieties in breaches phishing is the most prevalent one, followed by pretexting and bribery with email being the most common point of entry where the threat actor's objective is to achieve malware installation. Although social engineering-based attacks was on the rise in 2019 compared to 2018 Verizon identified also some positive notes on the data set. Based on the data provided to Verizon by its contributing organizations click rates on sanctioned phishing exercises has been steadily going down since 2012. In 2012, 25% of recipients was observed to click the link in the phishing email and in 2019 the total amount of clicks was only 3% (Verizon, 2019).

In their 2020 DBIR Verizon (2020) analyzed a record total of 157,525 incidents of which 32,002 met their quality standards and of which 3,950 were confirmed data breaches. From this data set 22% of the incidents involved social engineering-based attacks as a tactic and 22% of breaches involved phishing. Although phishing was not as common tactic in 2020 than in 2019 it is argued that attackers are becoming increasingly efficient in utilizing social engineering-based tactics to compromise organizations. When looking at the data from 2019 and 2020, 869 of the confirmed data breaches involved phishing as a tactic as to in 2019 the number was 644 from the amount of total confirmed breaches involving phishing as a tactic. There is however also a positive note also on the 2020 DBIR regarding social engineering-based attacks. In 2019 DBIR it was reported that click rates have steadily been going down and this was a continuing trend in 2020, but also reporting rates regarding phishing attacks have been on the rise. Based on the 2020 DBIR in 2016 only 20% of the phishing test campaigns was reported at least once but in 2019 this number was almost 40%. This is definitely positive news for organizations and shows that overall security awareness has risen which also helps organizations to detect and respond to phishing attacks more effectively (Verizon, 2020).

Analysis from the APWG Phishing Activity Trends Reports (APWG, 2018; APWG, 2020) ranging from 2018 to 2020 shows that phishing is still an effective method and specific industries are especially being targeted. Based on the APWG data set the three most common industry sectors being targeted by phishing campaigns are SaaS and webmail sites, such as Microsoft O365, financial institutions and payment industry. SaaS and webmail sites have been on the lead since 2019 as more and more organizations are moving their on-premise services into the cloud, such as Azure, Google Cloud Platform (GCP) and integrating their on-premise mail services into Microsoft O365 or Google GSuite. In 2019 APWG analyzed that the objective of phishing campaigns is to harvest employee credentials to compromise corporate SaaS accounts, which involves the growing trend of Business Email Compromise (BEC). In BEC the attacker targets employees with access to company finances or other sensitive financial information by sending them a phishing email from fake or compromised email accounts with an objective of tricking them sending money (APWG, 2018; APWG, 2020). BEC attacks have also been actively reported in Finland by the National Cyber Security Centre Finland (2019) as well in their news where organizations have been "subject to phishing with the purpose of obtaining the email credentials of employees.” (Traficom, 2020, p. 3) These compromised accounts have then been used for example to monitor messages, such as payment-related to seek significant financial gain or to acquire business secrets (Traficom, 2020).

Based on APWG first quarterly report (2020) phishing campaigns also seems to follow global trends and disasters as during the COVID-19 pandemic in 2020 where several targeted phishing campaigns were reported to include pretexting covering information related to COVID-19 or targeting video conferencing platforms due to the remote work requirements. These attacks were mainly targeted to obtain valid credentials through fake corporate sites which would have been then used to access other sites and services (APWG, 2020).

As mentioned in the 2020 DBIR analysis that threat actors have become more efficient in regard to phishing can also be seen from the APWG reports. As of 2020 75% of all phishing sites reported to APWG are protected by the HTTPS encryption protocol. The adoption of HTTPS on phishing sites has been steadily risen since 2016 as can be seen on the data provided by APWG on Figure 2 (APWG, 2020).

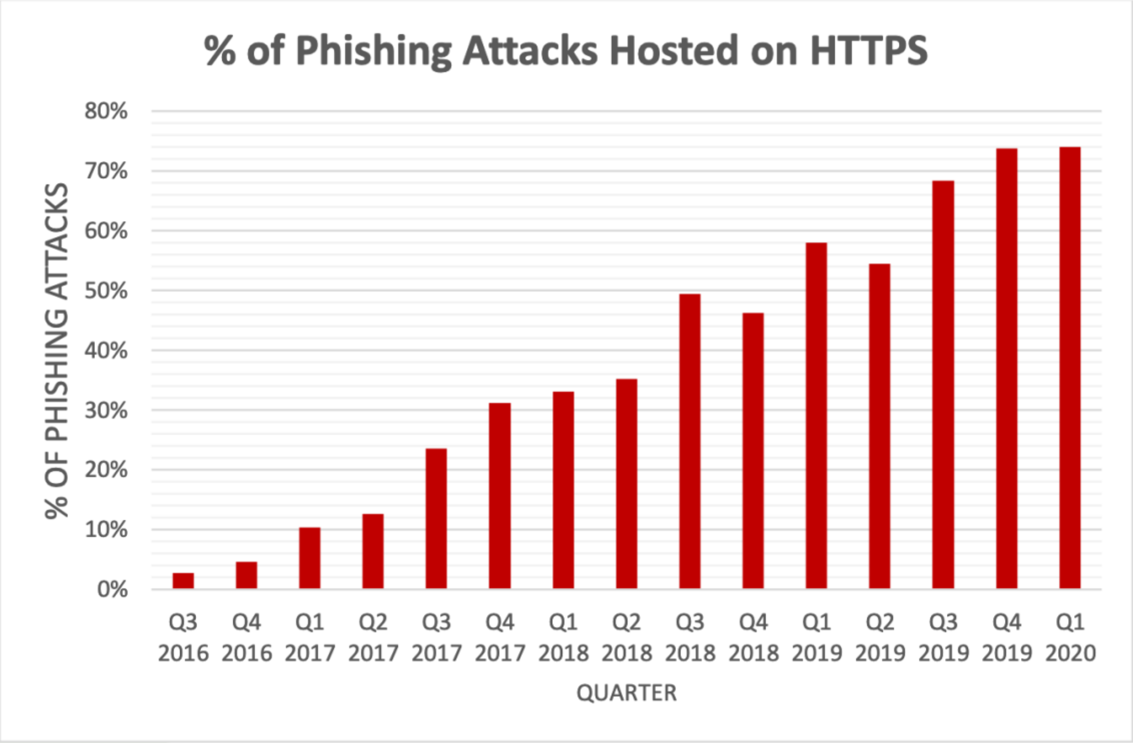


Figure 2 Percentage of Phishing Attacks Hosted on HTTPS (APWG Phishing Activity Trends Report 1st Quarter 2020, p. 12)

The analysis of APWG does not provide any further insight into what has caused the rise of HTTPS adoption in phishing sites. One potential reason behind the growing number of SSL protected phishing sites could be that Let’s Encrypt provides free SSL certificates for 90-days. The beta of Let’s Encrypt ran from September 2015 to April 12, 2016 from which on they started to issue free SSL certificates to anyone (Aas, 2016). When looking at the data provided by APWG we can see clear correlation between these two. Some research has been done in this area regarding Let's Encrypt impact on phishing sites adopting HTTPS encryption. This is discussed more in the Section 7.2.1 (HTTPS).

The GitLab Red Team (2020) performed a phishing campaign where they targeted their employees to measure overall security awareness. During the campaign, the team sent 50 emails from which 17 or 34% of the recipients clicked the link included in the phishing message, which led them to the attacker-controlled web site. From those 17 employees who clicked the link 10 (59%) or 20% of the total test group provided their credentials through the phishing site. Only 6 (12%) reported the phishing attempt to GitLab security team. The Red Team used an open source phishing kit known as GoPhish, which is discussed more in Section 8.2 (Phishing Kits) (The Register, 2020).

Social engineering-based attacks and especially phishing as a tactic seems to be one of the most efficient methods being used by threat actors to compromise organizations. In addition to this, attackers are able to enhance their skillsets and adapt to new trends regarding pretexting and methods as can be seen from the DBIR data sets that the amount of data breaches involving phishing as a tactic has been steadily rising over the years.

4 CASE STUDIES

4.1 Advanced Persistent Threats (APTs)

Defined by Ahmad, Webb, Desouza and Boorman (2019) Advanced Persistent Threats are a threat actor that utilizes sophisticated tactics, techniques and procedures (TTPs) to achieve their objectives. These groups maintain high-level operability by using previously unknown attack vectors, also known as 0-days and that their initial point of intrusion and time are uncertain and unpredictable, which makes it difficult for defenders to detect. Persistence comes from the fact that APT attacks are continuous, and their lifetime is long and once the attack does succeed, they may stay dormant for long periods of time to evade detection (Ahmad, et al., 2019).

As described in TrendMicro's threat intelligence report (2012) APTs are commonly known to utilize social engineering techniques, such as spear phishing campaigns to infiltrate target networks during their operations to gather valuable and sensitive information. The reason behind this is believed to be that spear phishing is an essential tactic to get high-ranking targets to open phishing e-mails, as the targets may be more security aware and thus avoids clicking and opening regular phishing e-mails. Based on the results collected by TrendMicro, 94% of the targeted e-mails used malicious file attachments to achieve code execution to install backdoors into the target network (TrendMicro, 2012).

Ussath, Jaeger, Cheng and Meinel (2016) analyzed APT's techniques and methods from 22 different campaigns to obtain an overview of the most common techniques, tactics and procedures being used by known APT groups. The research focused on three distinct phases: initial compromise, lateral movement and command and control. This thesis will focus explicitly on the analysis of initial compromise, which objective is to obtain access into the target environment. Commonly utilized techniques by APT groups for initial compromise includes spear phishing campaigns. The groups mostly used malicious file attachments or embedded links in e-mail to web servers or websites to compromise the target system as a main technique. The APT groups used mainly PDF files, Flash files, or Microsoft Office documents with or without macros. Only two of these campaigns used previously unknown vulnerabilities to initially compromise the target environment. All others exploited already previously identified and reported vulnerabilities within these file formats (Ussath et al., 2016).

Similar results were made by Li, Huang, Wang, Fan and Li (2016) on their research where they analyzed 89 known public APT cases and their tactics and techniques. From all the cases they analyzed, 73% included either the usage of a malicious file attachment within an e-mail or an embedded link into a malicious site for initial compromise. However, there was an interesting observation regarding the campaigns. Many APT groups commonly used e-mail attachments included pornographic pictures or official documents. Usage of official documents is most likely explained by the fact that APT groups commonly target corporations and national agencies and ministries with an objective of obtaining sensitive and confidential information. Usage of pornographic pictures is a curiosity, and their effectiveness can be debatable. APT groups do not that often use 0-day vulnerabilities in their arsenal to achieve initial access. From the well-known public cases, only 19% used 0-day vulnerabilities compared to the 70%, which exploited publicly known vulnerabilities (Li et al., 2016).

Based on the research of APT groups and their techniques, tactics and procedures, one of the most common initial access vectors seems to be spear phishing campaign utilizing a publicly known vulnerability. There might be several reasons for this why the usage of 0-day vulnerabilities is so low by APT groups. First of all, 0-day research is very time consuming and expensive (Monte, 2015). Also, once a 0-day vulnerability is found, it might not be wise for an APT group to “burn” the vulnerability by using it in an active operation, especially if access can be obtained by using already known vulnerabilities. In addition, nobody really knows how many 0-days each APT group actually has and the research is based only on public, well-known cases, which means that there could be a lot more operations on-going or undiscovered that actually utilizes 0-day vulnerabilities in their attacks (Greenberg, 2020; Metrick, 2020).

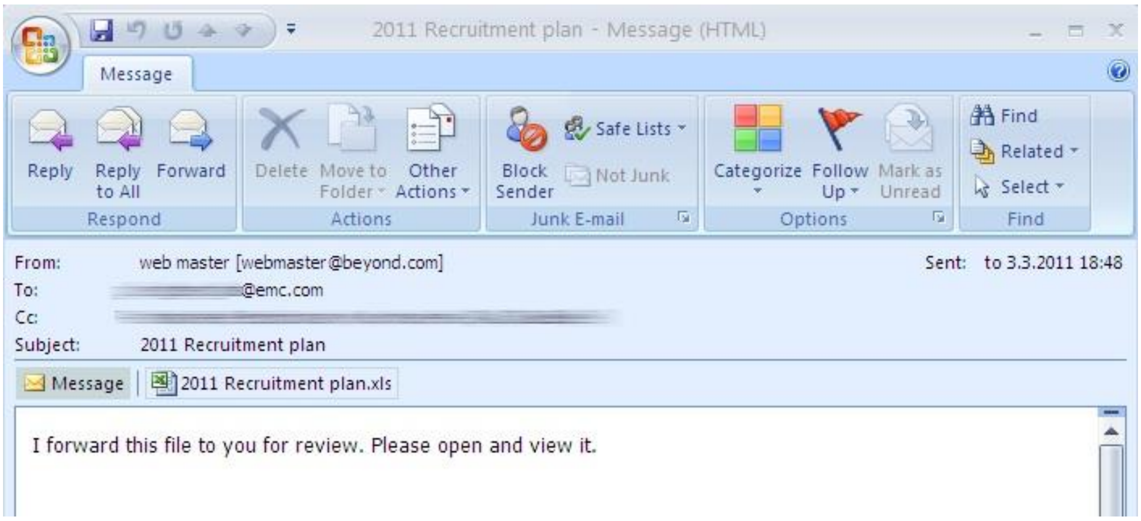
4.2 RSA Breach

It was stated as "one of the biggest hacks in history" when news broke out that RSA, the well-known security company and maker of two-factor authentication tokens - RSA SecurID - was breached by an e-mail containing a malicious attachment (Mikko, 2011).

Based on the analysis done by F-Secure (2011), the current theory is that the real target of the attack was actually Lockheed Martin and Northrop-Grumman with a probable objective of stealing military secrets. However, this had proven difficult to the attackers since the employees of both of these companies were using RSA SecurID tokens for two-factor authentication to access their systems. To achieve their objective, the attackers would need to somehow bypass or break the two-factor authentication being used by these two companies. They decided to target RSA (Mikko, 2011).

The initial phase of the attack was a malicious attachment sent as an e-mail. Uri Rivner, an RSA spokesman, described the attack as the textbook definition of a targeted phishing attack: "The emails were sent to what Rivner said was a small group of RSA employees, at least one of whom pulled the message out of a spam folder, opened it and then opened the malicious attachment.” (Threatpost, 2011)

The attackers sent an e-mail, which contained an attachment named "2011 Recruitment plan.xls" as described in Figure 2. The malicious attachment contained an exploit that took an advantage of previously unknown vulnerability in Adobe Flash (CVE-2011-0609[1]) and installed a backdoor, known as Poison Ivy[2].



From: web master [webmaster@beyond.com] Sent: to 3.3.2011 18:48
To: [redacted]@emc.com
Cc: [redacted]
Subject: 2011 Recruitment plan
2011 Recruitment plan.xls

I forward this file to you for review. Please open and view it.

Figure 3 RSA breach initial spear phishing (F-Secure, 2011)

Once the exploit was triggered the backdoor opened a command and control channel to an attacker-controlled infrastructure and provided remote access to the affected workstation. From this point onwards, the attackers started to perform situational awareness and position themselves in the network to discover and achieve their objectives.

Based on the news article in Wired by Zetter (2011) RSA stated that the intruders did in fact succeed in stealing information related to the SecurID two-factor authentication products. The RSA spokesperson also initially stated that the breach did not pose a risk to their customers, since the attackers would have required more information than they were able to exfiltrate. However, months later after the attack, several of RSA's customers, such as Lockheed Martin discovered attackers trying to breach their network using duplicates of the SecurID tokens, which RSA had issued to the company (Zetter, 2011).

There are several interesting pieces in this campaign. When observing the pre-text of the phishing e-mail and how it has been setup, it is not very advanced or sophisticated. The e-mail and the campaign itself contain several key points that should have been identified as being unsolicited, or malicious. Initially, as also described by Bright (2011) the e-mail was delivered into a spam folder from where the employee had retrieved it and opened the malicious attachment. Secondly, the sender and domain are already quite suspicious as the "*webmaster@beyond.com*" does not seem to have any affiliation with RSA. Also, the e-mail does not contain any signature information or context

[1] https://nvd.nist.gov/vuln/detail/CVE-2011-0609
[2] https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

for the recipient as a reason to open the attachment. In conclusion, a very rudimentary, but successful phishing campaign. Additionally, using publicly available tooling to establish persistence and foothold to perform lateral movement are within the reach of any hacker that has sufficient technical knowledge (Bright, 2011).

4.3 APT28

This case study shortly focuses on publicly available threat intelligence reports to gather a high-level overview of what have been the most commonly employed tactics and techniques by APT28 to achieve initial access against the targeted organizations.

APT28, or better known also as FANCY BEAR or Sofacy is well-known that they actively utilize spear phishing and credential harvesting sites as common techniques to achieve initial access into the target organization (FireEye, 2014). APT28 activities and TTPs has been observed and analyzed by several threat intelligence and security companies.

According to CrowdStrike threat intelligence reports (2019; 2020), APT28 typically employ phishing campaigns and credential harvesting sites using spoofed web sites to gather sensitive information, such as employee's credentials for initial access. In addition to this, APT28 also registers domains that closely resembles domains of the targeted legitimate organizations to make the overall campaign look less suspicious (CrowdStrike, 2019; 2020). This same behavior has been observed also by the National Cyber Security Centre (NCSC) in their Indicators of Compromise for Malware used by APT28 where APT28 has utilized spear phishing to introduce their tooling (ZEBROCY) into the target network (NCSC, 2018).

The threat intelligence reports provided by PaloAlto Networks Unit42 Threat Research Team (2018) describe two different APT28 campaigns where they have employed spear phishing campaigns to target government institutions. Further analysis revealed that in one of these campaigns APT28 was able to spoof an email originating from a well-known supplier of information and market analysis, known as Jane's by IHSMarkit. Being able to spoof emails originating from legitimate organizations make the context of the phishing email more believable and trustworthiness as the recipient has no way of identifying anything anomalous from the email without further analysis of the email's header data. Another interesting fact of the analyzed campaign is that PaloAlto Networks believe that APT28 may have used an open-source tooling to weaponize the documents being used in the attack, known as LuckyStrike. This tool was introduced in a DerbyCon security conference in September 6, 2016. This is based on the analysis performed by PaloAlto Networks researchers who identified several similarities between the APT28 payload, and a document created by LuckyStrike (PaloAlto Networks, 2018). LuckyStrike is a PowerShell based generator of malicious Microsoft Office documents (Lang, 2016).

As uncovered by FireEye in their threat intelligence research they believe that APT28 has also targeted hospitality industry with targeted phishing campaigns that have included a malicious Office Word document to install malware into the target (FireEye, 2017).

Based on the threat intelligence reports and previous research on APT tactics and techniques shows that spear phishing campaigns remains an effective and common method of achieving initial access into their target organizations. What makes these attacks even more successful is the fact that if these APT groups are able to identify misconfigurations - in the target organization's or companies closely related to them - in email infrastructure that would provide means to spoof emails seeming to originate from legitimate source. Another observation between these analyzed campaigns was the heavy usage of Microsoft Office documents being weaponized to introduce malware, such as backdoors into the environment for initial access and persistence (MITRE, 2020). As stated in the research reports APT28, as well as potentially many other APT groups as well, do not shy away of using publicly disclosed offensive security tooling in their operations. This makes it even more crucial for defenders and security researchers alike to have knowledge of what tooling is available to be used to weaponize and deliver exploits into target environments to obtain capabilities and mechanisms to defend against these attacks.

5 EMAIL AUTHENTICATION

Email fraud remains to be prevalent and an effective attack vector, which has caused several billions on financial losses for organisations in recent years (FBI, 2018). Organisations cannot rely on their employees to continuously identify malicious emails and as such, email authentication and sender verification are considered to be the basic security measures that each organization should deploy to protect their email infrastructure to avoid threat actors abusing it to commit fraud or phishing attacks (Derouet, 2016).

These security measures are known as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) (IETF, 2014; IETF, 2011; IETF, 2015). SPF as defined in the latest Request for Comments 7208 from 2014 is designed to verify the sender's domain to ensure that the email originates from a trusted source (IETF, 2014). DKIM as defined in the latest Request for Comments 6376 from 2011 is an email authentication technique designed to detect forged sender addresses in email, which is achieved through a cryptographic signature using a public-key infrastructure model (IETF, 2011). DMARC as defined in the latest Request for Comments 7489 from 2015, is an email authentication, policy and reporting protocol and is built on top of SPF and DKIM (IETF, 2015).

However, deploying SPF and DMARC will not be able to prevent sophisticated and targeted phishing attacks as demonstrated in this thesis. Also, if an attacker is able to gain access to an employee's email account having these countermeasures in place will not provide any protection since the attacker is in a position to impersonate as the compromised user by having access to their email inbox (Petsalis, 2018). Furthermore, adoption of these technical security control measures has been largely voluntary with little penalty for noncompliance (Hatton & John, 2017). The following sections describe these email authentication mechanisms in more detail and how these can be used to protect email infrastructure.

5.1 Sender Policy Framework (SPF)

As stated in Request for Comments 7208 for SPF "email on the Internet can be forged in a number of ways. In particular, existing protocols place no restriction on what a sending host can use as the "MAIL FROM" of a message or the domain given on the SMTP HELO/EHLO commands." (IETF, 2014, p. 1).

Stefan Görling has provided an extensive overview of SPF in his study (2007) where he analyzed SPF as an anti-phishing mechanism. The Sender Policy Framework (SPF) is an open standard that was designed "with transparency and ease of adoption in mind." (Görling, 2007, p. 171). Purpose of SPF was to provide technical methods to prevent sender address forgery. SPF should not be considered as an anti-spam measure but instead of as a mechanism to mitigate problems with fraud and phishing. Purpose of SPF is to "validate that the message was sent by the sender domain specified in the "MAIL FROM:" address of the message envelope." (Görling, 2007, p. 173).

As defined in RFC 7208 (2014) "An SPF record is a DNS record that declares which hosts are, and are not, authorized to use a domain name for the "HELO" and "MAIL FROM" identities." (IETF, 2014, p. 11). The SPF record is expressed in the DNS TXT resource record or as a specific SPF record, which specifies what servers are allowed to send email using the domain provided in the records (IETF, 2014). An example of an SPF record and descriptions of each value is described in below by the RFC 7208:

```
v=spf1 +mx a:colo.example.com/28 -all
```

The policy in this example states that:

- [+mx] mail servers specified in MX records for this domain are authentic.
- [a:colo.example.com/28] if the originating mail server is in this address range, it is also authentic and authorized send email on behalf of the domain.
- [-all] all other mail servers are invalid.

There are four different qualifiers for SPF which describes the action to take when an email is sent for a domain that has a published SPF record:

- [+] Pass
- [-] Fail
- [~] Softfail
- [?] Neutral

Fail effectively means that all received email are suspected to be forged or spam and should be rejected for delivery (Särud, 2016). Softfail means that emails are accepted but are marked with a warning as suspicious or potentially spam. Neutral means that all emails are accepted (Canzoneri, 2014).

5.1.1 Adoption of SPF

Not much research has been done regarding the adoption rate of email authentication mechanisms or SPF in general. There are documented attacks where threat actors have successfully spoofed email addresses during the delivery phase of the attack lifecycle (Lee & Falcone, 2018). This supports the fact that organizations are still struggling with adopting basic security measures on their email infrastructure.

In 2016 a security researcher from a security company known as Detectify did a survey to validate how many Top 500 domains of Alexa, which is the biggest provider of commercial web traffic data and analytics were missing SPF records (Särud, 2016).

In their survey Särud (2016) did a simple DNS lookup to check for domain's SPF and DMARC records to check if the domain was missing or had misconfigured the records. Domain was classified as vulnerable to email spoofing if one of the three combinations were found in the TXT records:

- No SPF at all
- SPF with softfail, only
- SPF with softfail, and DMARC with action none

According to Särud (2016) over 50% of the world's top domains were vulnerable for email spoofing. It was also argued that if half of the Internet's most used domains can be spoofed it is probably even worse for the whole Internet. They also discovered that only 42% of the Top500 Alexa sites uses DMARC meaning that domains that does not have correctly configured DMARC records the organizations would not even be aware of possible abuse of their domain. This is due to the fact that DMARC stands for Domain-based Message Authentication, Reporting and Conformance and it provides visibility for organizations to obtain knowledge by providing information as who is sending email from that organization's domain. Särud also argues that most common reason for so many domains missing these additional security measures are either misinformation or lack of knowledge as to how vulnerable email without authentication can be (Särud, 2016).

5.2 Domain Keys Identified Mail (DKIM) Signatures

Domain Keys Identified Mail (DKIM) permits someone that owns the domain that was used for signing the message to claim some responsibility for a message by associating the domain with the message (IETF, 2011). The idea behind DKIM as described by Leiba and Fenton (2007) in their research paper is that when receiving an email from an entity bearing a valid digital signature, it provides means for the message recipient to verify that the message actually originated from the entity. Although DKIM provides means to verify that the email message originates from the domain it should not be considered as an antispam technique. In its essence, DKIM makes it more difficult for attackers and phishers to spoof legitimate domain names that participate in DKIM signing (Leiba & Fenton, 2007).

There are additional security considerations that should be taken into account with DKIM. The DKIM Request for Comments (2011) lists multiple security issues that affects DKIM that affects confidentiality, integrity as well as availability (IETF, 2011).

The following section describes an example provided by IETF (2011) as to how a composed email that is signed with DKIM looks like. In the following example provided by the RFC 6376, email is signed by the example.com outbound mail server:

```
DKIM-Signature: v=1; a=rsa-sha256; s=brisbane; d=example.com;
```

```
     c=simple/simple; q=dns/txt; i=joe@football.example.com;
     h=Received : From : To : Subject : Date : Message-ID;
     bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
     b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
     4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
     KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
     4bmp/YzhwvcubU4=;
Received: from client1.football.example.com  [192.0.2.1]
     by submitserver.example.com with SUBMISSION;
     Fri, 11 Jul 2003 21:01:54 -0700 (PDT)
From: Joe SixPack <joe@football.example.com>
To: Suzie Q <suzie@shopping.example.net>
Subject: Is dinner ready?
Date: Fri, 11 Jul 2003 21:00:37 -0700 (PDT)
Message-ID: 20030712040037.46341.5F8J@football.example.com


<Message content>
```

As defined in the RFC 6376 (2011) "the signing email server requires access to the private key associated with the "brisbane" selector to generate the signature." (IETF, 2011, p. 65).

5.3 Domain-based Message Authentication, Reporting, and Conformance (DMARC)

The RFC 7489 by Internet Engineering Task Force (2015) defines DMARC as Domain-based Message Authentication, Reporting, and Conformance is an email authentication policy and reporting protocol. It allows mail-originating organizations to express domain-level policies and preferences for message validation, disposition, and reporting from receivers to senders. This can be used to improve and monitor protection of the domain from fraudulent mail. DMARC has two distinct purposes; verify incoming messages by authenticating the sender's domain and define the action to take on suspicious incoming messages. For organizations to deploy DMARC it is required that SPF and DKIM has been set up before configuring DMARC since DMARC uses both SPF and DKIM to verify that messages are authentic (IETF, 2015). An example DMARC record from RFC 7489 has been provided below for example.com domain.

```
"v=DMARC1;p=reject;pct=100;rua=mailto:postmaster@example.com"
```

As with DMARC, the Request for Comments includes additional security considerations that should be taken into account, such as attacks affecting confidentiality and availability (IETF, 2015).

6 ATTACK LIFECYCLE

The attack lifecycle is a model that describes the steps an adversary must take in order to achieve their objectives through a cyber intrusion. This model was initially introduced by Hutchins, Cloppert and Amin from Lockheed Martin in their whitepaper "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusions Kill Chains" (2011). In their whitepaper the researchers define the essence of intrusion where "the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives." (Hutchins, Cloppert & Amin, 2011, p. 4).

Hutchins et al., (2011) have adapted the cyber kill chain that consists of reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objective from the concept of U.S. military targeting doctrine that defines kill chain as "a systematic process to target and engage an adversary to create desired effects." (Hutchins et al., 2011, p. 4). The cyber kill chain is described in Figure 4.

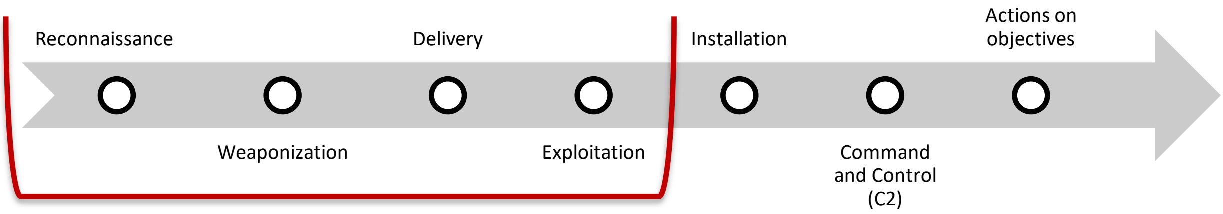


Figure 4 Lockheed Martin's attack lifecycle (Hutchins, Cloppert & Amin, 2011)

This master's thesis will solely focus on the first four steps of the attack lifecycle; reconnaissance, weaponization, delivery and exploitation as these are the key steps in regard of targeted phishing attacks. These four initial steps are defined in by Hutchins et al., (2011) as follows.

- **Reconnaissance** – information gathering from publicly available sources, such as search engines, social media and company web sites to build a target list and identify specific technologies used in the target organization.
- **Weaponization** – Introduction of a remote access trojan into a deliverable payload, such as a Microsoft Office document or PDF.
- **Delivery** – Transmission of the weaponized payload to the target environment. Common mechanisms include, but are not limited to, are email delivery and USB removable media.
- **Exploitation** – After delivery, exploitation triggers the adversary's remote access trojan to establish a command and control channel into the attacker's infrastructure.

As already concluded in the literature review, email is one of the most common delivery mechanisms in phishing attacks, whether it includes a link to a malicious site or contains a weaponized payload designed to install a backdoor into the target organization's internal network. According to the Lockheed Martin Computer Incident Response Team (LM-CIRT) during the years 2004 – 2010, three most common and prevalent delivery vectors for weaponized payloads were email attachments, websites and USB removable media (Hutchins et al., 2011).

The following sections of this master's thesis is built on these observations as how open source intelligence can be used to gather information that is critical for the adversary. This information gathering phase is then followed by weaponization, which is used to design and implement payloads, such as backdoors into documents that are then delivered to the target, for example through email. Once the delivery of the payload has been achieved then follows the execution phase where the payload gets executed on the target to establish a command and control channel for the adversary. Once the threat actor has achieved initial foothold and persistent access into the target environment, for example through a compromised workstation their next step is perform lateral movement to spread their access across the environment by compromising several other workstations and servers. The final phases of the attack are to identify key assets and objectives, such as sensitive data which is then exfiltrated from the target environment. The final stages of the intrusion kill chain are out of scope of this master's thesis as the objective is to concentrate on the initial compromise vectors through targeted phishing attacks.

7 RECONNAISSANCE

As defined by Sanghvi and Dahiya (2013) reconnaissance is the first phase of a cyber-attack where the attacker collects information of the victim. Information gathered during reconnaissance phase can contain network and host related technical information as well as personal or organizational specific information, such as emails, addresses or password complexity requirements. Reconnaissance is divided into two types: active and passive (Sanghvi & Dahiya, 2013).

In their book Sood and Enbody (2014) presents an intelligence gathering, or reconnaissance process as follows:

- *Selection and discovery* – attackers use publicly available resources to collect data about the target.
- *Resource extraction and data mining* – once attackers have identified potential sources to gather data about the target, the process of searching and collecting data for analysis is started.
- *Resource correlation and information processing* – during this phase the attacker's go through the collected data to identify potential associations between the gathered information.
- *Attack modeling* – in the final phase, the attackers start to model an outline of the attack by using the processed information (Sood & Enbody, 2014).

7.1 Active

Active reconnaissance involves actively sending network packets to the targeted organization and is more offensive than passive reconnaissance, or foot printing, since there is more risk that the target may be alerted for possible attack (Sanghvi & Dahiya, 2013). Typical activities related to active reconnaissance is to map any external or internal assets the target might have.

Depending on the objective as described by Chell (2018) when performing targeting or active reconnaissance about a target is to disclose as much version information about the client-side software as possible. This is done to obtain knowledge about the environment to develop targeted payloads to compromise the organization. One tactic is to send a benign phishing email that does not specifically contain any malicious but are engineered to trigger call back through an externally hosted image that is inserted into the phishing email message. This technique can be used to disclose information, such as what operating system is being used in the organization as well as internal domain and hostnames (Chell, 2018).

7.2 Passive

In passive reconnaissance the objective is to minimize interaction with the target (Sanghvi & Dahiya, 2013). Activities during passive reconnaissance would include harvesting email addresses and employee names from social media platforms, such as LinkedIn[3]. Target's external and potentially even internal assets can be passively enumerated using publicly available tools, such as Shodan. Shodan crawls and indexes Internet actively and misconfigured services may expose sensitive information or even critical infrastructure (Tiilikainen & Manner, 2013). Further information that can be gathered using passive reconnaissance techniques is to map the organizations email infrastructure configuration to verify whether the organization has taken necessary steps to prevent email forgery.

[3] https://github.com/initstring/linkedin2username

8 WEAPONIZATION

During weaponization one of the key elements is to also build attacker infrastructure that is used to either host malicious payloads or phishing sites that are used to trick users into submitting their credentials to the attacker-controlled infrastructure. However, this section does not provide deep technological overview of the functionalities and how specifics work in the presented examples provided in this master's thesis.

8.1 Malicious attachments

8.1.1 Microsoft Office Macros

Malicious usage of Microsoft Office Macros, also known as macro viruses, has been known as a concept already since 1989 and initial work by anti-virus researchers regarding this area and initial published work about a working macro virus was done by Joel McNamara in December 1994 (Bontchev, 1996). The evolution of macro viruses and how macros work or are built are out of scope of this master's thesis.

Macro malware has long persisted as a cybersecurity threat as stated by Barden & Lo (2017). Microsoft disabled most of the automatic script execution mechanisms by default, which forced attackers to come up with new ways to achieve code execution through Macros. Now attackers are using innovative social engineering techniques to undermine the user's ability to distinguish between malicious and legitimate documents. The objective is to persuade the user to enable Macros, which would then execute the attacker's payload on the workstation. (Barden & Lo, 2017). These approaches and methods are described in more detail in Section 9.1 (Pretexting).

As discussed later in this master's thesis in the Section 10 (Exploitation), threat actors are actively utilizing Microsoft Office and especially Word-based Macros to compromise their targets using either zero-day or previously known vulnerabilities. Probably one of the most high-profile cases where Microsoft Office Macros has been used as an attack vector is related to the attack on the Ukrainian power grid as documented Lee, Assante and Conway (2016). To compromise the power grid the attackers delivered malicious Office documents via email to employees in the administrative and IT network with a pre-text to encourage users to enable macros in the document. Once the users enabled macros a BlackEnergy 3 type malware was installed on the victim systems and established a command and control channel which was then used to collect information and move laterally in the network (Lee, et al., 2016).

As described in several threat intelligence reports (Kizhakkinan, Wang, Caselden & Eng, 2016; Bohannon & Carr, 2017; Llimos & Pascual, 2019) many threat actors have been actively using Microsoft Office documents with embedded macros that, when enabled, downloads and executes an additional payload that provides initial access for the attackers to the targeted organization. The embedded macros have either been exploiting previously unknown vulnerabilities or taking advantage of unpatched systems and exploiting already publicly known security issues to achieve their initial objective. The usage of macros as a weaponization technique remains to keep one of the most used method for threat actors (Kizhakkinan, Wang, Caselden & Eng, 2016; Bohannon & Carr, 2017; Llimos & Pascual, 2019).

8.1.2 Microsoft Office DDE

Microsoft's Dynamic Data Exchange is a protocol designed to send messages between applications that share data and uses shared memory to exchange data between applications (Microsoft, 2018). Security researchers Etienne Stalmans and Saif El-Sherei discovered means to abuse DDE for malicious purposes by achieving macro-less code execution through Microsoft Word and Excel to bypass macro filtering mail gateways and corporate VBA policies (El-Sherei, 2016; Stalmans & El-Sherei, 2017). In a scenario described by Microsoft:

> an attacker could leverage the DDE protocol by sending a specially crafted file to the user and then convincing the user to open the file, typically by way of an enticement in an email. The attacker would have to convince the user to disable Protected Mode and click through one or more additional prompts. As email attachments are a primary method an attacker could use to spread malware, Microsoft strongly recommends that customers exercise caution when opening suspicious file attachments. (Microsoft, 2017)

The Dynamic Data Exchange (DDE) was actively being used by threat actors to compromise organizations. For example, McAfee Advanced Threat Research analysts identified a campaign leveraging the Microsoft Office Dynamic Data Exchange (DDE) technique while monitoring the activities of APT28 threat group (Sherstobitoff, 2017). Attackers had also actively utilizing DDE to distribute a remote access trojan (RAT) known as DNSMessenger in their campaigns (Brumaghin & Grady, 2017).

Microsoft decided to disable DDE feature in Microsoft Office Word to prevent further malware attacks as it was actively leveraged by several threat actors as reported by Cimpanu (2017). To further prevent the abuse of DDE features in other Office applications, such as Excel and Outlook, Microsoft released further details on how to disable DDE. The timeline shows that threat actors are actively following what is going on in the security industry and that they are capable to quickly adapt and implement newly published techniques into their arsenal (Cimpanu, 2017).

8.1.3 Microsoft Office Excel 4.0 Macros

Security researchers from a company known as Outflank discovered means to abuse Microsoft Office Excel 4.0 Macros for malicious purposes and they presented their findings at the DerbyCon 2018 security conference. As described by Stan Hegt in his blog post (2018) apparently Excel 4.0 macros are still widely supported by Microsoft Office versions, but only by Excel and not by Word or PowerPoint. This could somewhat limit the attackers abuse cases since they are required to create believable pre-texts using Excel spreadsheets to compromise their targets. However, the more interesting point with Excel 4.0 macros is that when compared to Visual Basic for Applications (VBA) the macros are stored completely differently and thus may present problems for security products to identify malicious behavior (Hegt, 2018). Furthermore, Microsoft announced (2018) that their anti-malware interface scanning (AMSI) is capable to scan VBA macros as macro-based threats remains to be prevalent. However, based on research done by Hegt, Microsoft's AMSI is unable detect malicious behavior through Excel 4.0 macros (Hegt, 2018).

The Security researchers Haughom, Singh and Ortolani from VMWare Threat Intelligence Team (2020) analyzed the evolution of Excel 4.0 Macro weaponization. During their research, the researchers discovered that the usage of Excel 4.0 Macros has increased especially in delivering commodity malware and that threat actors have adapted variety of techniques to obfuscate their payloads and evade detection (Haughom, Singh & Ortolani, 2020).

8.2 Malicious links and site cloning

Instead of including a malicious attachment as part of a phishing campaign, attackers may also include links inside the message that redirects the user into a malicious, attacker-controlled web page. These websites are specifically designed to either steal sensitive information or to leverage vulnerabilities in web browsers or their plug-ins (Monte, 2015).

In an article by Hong (2012) where he analyzed the state of phishing attacks and some of the techniques that attackers are using and one of these techniques involved the method of setting up fake websites. When attackers are registering new domains, they are looking names similar to the site they want to impersonate; for example, impersonating exampleorg.com, attackers might register example-org.com to trick their victims. Another commonly used method that has been used by attackers is the use of homograph attacks that exploit the visual similarity of characters; for example attackers could register exampieorg.com to impersonate as exampleorg.com where the lowercase l in the original, legitimate domain has been change to lowercase i (Hong, 2012).

8.2.1 HTTPS

The world wide web has started favoring encrypted communications over HTTPS instead of traditional HTTP (Let's Encrypt, 2019). Let's Encrypt (LE) is an initiative built on the idea to speed up the adoption of HTTPS in the world wide web to provide easy and free way to implement Transport Layer Security (TLS) into web servers to protect user's data from eavesdropping. There were also fears where many believed that LE will be abused by cybercriminals to easily implement TLS into their phishing sites to make it look more legitimate and trustworthy (Aas, 2015). Let's Encrypt has taken actions to prevent the abuse of their ecosystem but it would seem that the actions taken by Let's Encrypt are not sufficient.

In March 2017, Vincent Lynch revealed that the misuse of Let's Encrypt is quite common, for example 96,7% of the over 15,000 security certificates containing the term PayPal were issued for phishing sites (Arghire, 2017). Also, as stated in Section 4.2 (Current state of the phish) phishers has started to widely adopt HTTPS in their phishing campaigns. Based on current research done by Oest, et al., (2020), phishing attacks carried over HTTPS proved to be three times more successful than attacks performed over HTTP. Although some successful phishing attacks still occur over HTTP, these presents a minority of all the investigated attacks (Oest, et al., 2020).

8.3 Defense Evasion

There are several different techniques available for attackers to try to avoid being detected during a phishing campaign. For example, the longer that a phishing website remain online and accessible to lure victims to give out their information or download malicious applications, the more attackers stand to profit (Oest, et al., 2020). This section covers some of the known evasion techniques being used by attackers to obfuscate payloads inside Microsoft Office documents as well as hiding their infrastructure.

8.3.1 VBA Stomping

One of the key elements of a successful spear phishing attack is to bypass the targeted organization's or individual's preventative security controls, such as anti-virus. One of the most common methods used by attackers while performing targeted attacks through email is to embed malicious VBA (Visual Basic for Applications) macros into the attachment files that are designed to compromise the target (Mimura & Ohminami, 2020). A known technique to evade anti-virus detection is known as VBA stomping, originally publicized by Dr. Vesselin Bontchev[4]. VBA macros are stored in a few different forms within a Microsoft Office file document:

- *source code*, original and compressed source code of the macro, which is stored in the end of the module stream,
- *p-code*, compiled pseudo-code, which is stored in a different place in the module stream than source code,

[4] https://github.com/bontchev/pcodedmp

- *execodes,* when p-code has been executed, a further tokenized form is created and stored elsewhere in the document.

As presented by Ogden, Roberts and Sayre at DerbyCon security conference in 2018 (2018) with additional work by Philippe Lagadec at BlackHat Europe security conference in 2019 (2019) purpose of VBA stomping is to manipulate Office documents macro source code, leaving only a compiled version of the macro source code, also known as p-code in the document file. As described in their presentation, when a file containing macros is opened, it actually uses the p-code to execute macros within the document and not the source code. The main observation here is that with VBA stomping it is possible to modify the VBA source code to look benign while the malicious macro source code contained in the p-code may go undetected and effectively evade detection (Ogden, et al., 2018; Lagadec, 2019).

Throughout the beginning of 2020, FireEye observed multiple targeted phishing campaigns that were primarily targeting financial services organisations where the phishing documents were carefully crafted and leveraging the aforementioned VBA stomping technique to avoid detection (Cole, Moore, Stark & Stancill, 2020).

8.3.2 Cloaking

Phishing sites commonly use a technique known as cloaking in an effort to prevent security teams and infrastructure from verifying malicious content that is being hosted on the attacker-controller website (Oest et al., 2020). In their paper Oest et al., analyzed over 2300 real-world phishing kits to analyze some of the common approaches that attackers are taking to evade existing phishing site detection. They discovered that one of the most common method in cloaking is request filtering where each request coming to the web server is first evaluated before content is shown to the user. Using these techniques attackers can verify for example that the users are coming from specific IP-address range that belongs to the targeted organization and denying access to or returning benign content to search engines, security firms, researchers, and denylist crawlers. Successfully blocking especially anti-phishing crawlers decreases the likelihood of timely detection and denylisting of the phishing site (Oest, et al., 2018).

8.3.3 Redirectors

Attackers are commonly using redirection techniques to obfuscate their infrastructure during an attack. During a phishing attack where the victim receives an email containing a link to an attacker-controller website the initially distributed URL might appear benign but redirect to different landing URLs which contain the actual attack (Oest et al., 2020). The initial benign looking domain within the email could be from a legitimate service, such as URL shortening service, or the attackers may have obtained a similar looking domain to trick the recipient victims.

URL shortening services take a long complex URL and shorten it to more convenient and easily sharable. There are several legitimate URL shortening service providers available such as bit.ly, tinyurl.com or goo.gl. Attackers have been starting to abuse these URL shortening services, most likely with an objective of evading network perimeter protections in organizations and "to mask the final destination where the victim will land after clicking on the malicious link" (Le Page, Jourdan, Bochmann, Flood & Onut, 2018, p. 1).

8.4 Spam filtering

Unsolicited email, also known as spam, is an increasing problem, with a big economic impact in society as presented by Sanz, Hidalgo & Pérez (2008). Commonly email is considered as spam if it is unsolicited, which means that the recipient is not interested in receiving the information, the sender is unknown to the recipient or the email has been sent to a large number of recipients (Sanz, Hidalgo & Pérez (2008). The motivation usually behind a spam message is to have information delivered to the recipient that contains a payload, whether it is an advertisement, link to an attacker-controlled web site or malicious attachment (Cormack, 2008).

There are several technical measures that organisations can implement to prevent, or at least reduce the amount of spam. Some of the most common techniques include content-based filtering for the message, usage of allow and deny lists where emails originating from specific IP address, email address or domain name may be filtered and collaborative filtering (Sanz, Hidalgo & Pérez (2008). Deeper technical overview of these technical countermeasures is out of scope of this master's thesis.

Sometimes there are cases when spam filtering is not successful in preventing commodity malware or other unsolicited email getting through. In these cases, it is extremely critical to have additional security controls in place, such as preventative controls on endpoints, like endpoint protection software that can detect and prevent malicious software from executing (Thurman, 2013).

As with any technical countermeasure there usually exists methods that are also publicly disclosed and discussed that can be used to bypass a security control or evade detection. Raulot (2018) studied the effectiveness of existing spam filters against phishing emails to determine what techniques exist that could be used by attackers and phishers to avoid detection and getting flagged as spam. The study concentrated on the most prevalent email service providers: ProtonMail, Office 365 and Gmail. In their study Raulot discovered that just being compliant with email authentication can prove to be an effective method to bypass spam filters. It was also discovered that the age of the domain being used to send spam had no effect as long as the email fulfilled compliance requirements with SPF, DKIM and DMARC (Raulot, 2018).

8.5 Multi-factor authentication

Traditional phishing attack objective is to either achieve code execution on the target user’s workstation or harvest credentials to obtain unauthorized access to some service. To prevent the misuse of harvested credentials, several web-based services started to implement and provide multi-factor authentication (MFA) as an extra layer of security. Two-factor authentication (2FA), which is one form of MFA basically requires two different methods of identity confirmation of the user. For example, once user submits their username and password, they are requested to submit an additional time-based one-time passcode (TOTP), which is validated by the server to make sure the user authenticating is the owner of the account (Arntz, 2017). There are several different and alternative options available to implement 2FA but are out-of-scope of this thesis.

There are several open-sourced offensive tools, such as Evilginx[5], Muraena[6], NecroBrowser[7] to provide means to bypass two-factor authentication (2FA) protection mechanisms when conducting phishing attacks. All these tools use a man-in-the-middle attack to capture login credentials and session tokens to successfully bypass 2FA protection as shown in their presentation at Hack in the Box 2019 security conference in Amsterdam by Orru and Trotta (2019). These specific attack techniques are not new and have been known for a while now. Also, man-in-the-middle attacks have been used previously with great success to eavesdrop network traffic and capture login credentials from unencrypted HTTP sites as well as while performing SSLstripping and DNS poisoning attacks against encrypted HTTPS sites. However, to perform such attacks to bypass 2FA protection has not been previously publicly available, until the release of the aforementioned tools (Orru & Trotta, 2019).

[5] https://github.com/kgretzky/evilginx2
[6] https://github.com/muraenateam/muraena
[7] https://github.com/muraenateam/necrobrowser

These tools work as a proxy between the victim and the service against the victim is authenticating. As the tool sits between the victim and the service, once victim enters their credentials on the fake login site the attack tool seamlessly forwards the traffic between the victim and the site to pass any login credentials and session tokens while logging this information for the attacker. The attack technique is described in the following diagram.

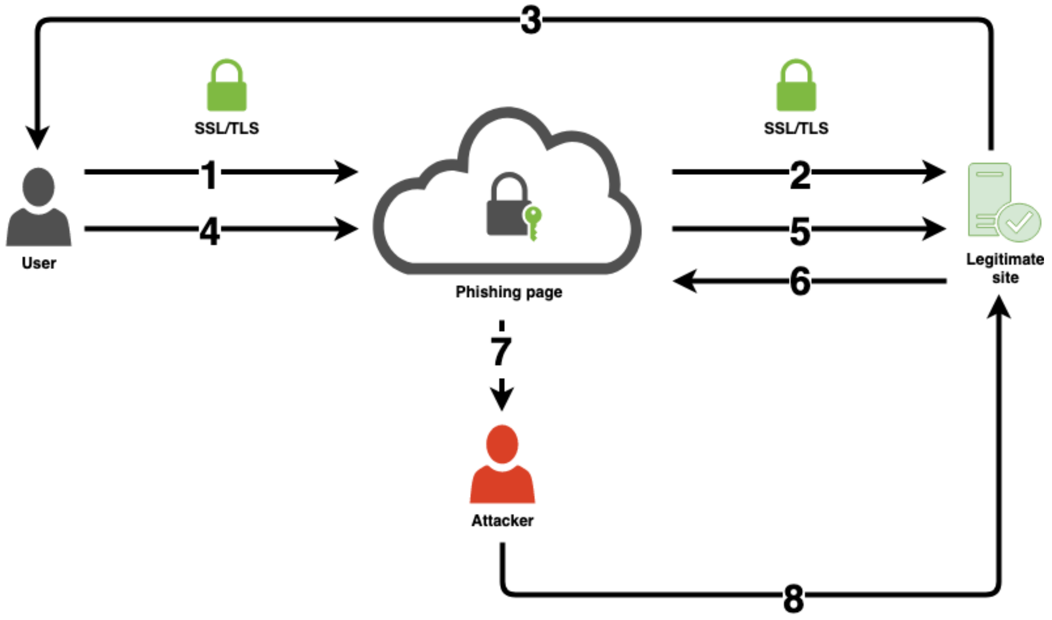


Figure 5 Bypassing multi-factor authentication (MFA)

The attacker has successfully sent a phishing email to the targeted user, which contains a link to a phishing site posing as a legitimate site requiring credentials. In the first step, the user enters their login credentials, username and password to the phishing site, which then forwards the request the legitimate site. Since the user has 2FA enabled the legitimate site sends a SMS or push notification to the user requesting the 2FA token. User submits the 2FA token to the phishing site, which once again forwards the request to the legitimate site. Once the authentication has been successfully completed the server, or legitimate site, returns a valid session token to the user, which is also logged into the attacker's server. Finally, the attacker takes the session token information and can now access the legitimate site posing as the user who has no idea that their credentials and access has been stolen by an unauthorized party.

Although this attack demonstrates that 2FA can be bypassed, it should not be abandoned. Enabling and requiring 2FA for all users will add a layer of security to protect accounts and sensitive information. Without 2FA enabled it is more trivial for attackers to obtain unauthorized access by using the same phishing techniques to harvest credentials or conducting automated password guessing attacks against vulnerable services to discover valid credentials that have poor passwords. There is still one shortcoming for the attacker regarding this attack technique, the phishing campaign must look as legitimate as possible, which can only be achieved by having a similar looking domain as the service that the attacker is targeting. As a user, close attention should be paid on the URL field domain name and certificate information when following any links that are received through e-mail or any other media to avoid submitting sensitive information, such as credentials into a phishing page.

8.5.1 Multi-factor authentication creates friction

A study done by Doerfler, et al (2019) researched the effectiveness of login challenges that are designed to provide an additional layer of security to prevent account takeover. The study also evaluated how these additional layers of security would affect the usability and experience of the users. However, the relationship between usability and security is out of scope of this master's thesis. The objective of the research was to evaluate the effectiveness of different types of multi-factor authentication devices and methods to prevent automated account hijacking performed by automated bots or phishers. The study also included a sample of 1.2 million challenges solved by legitimate users to measure how often these challenges temporarily locked out account holders (Doerfler, et al., 2019).

Another study done by Mirian, et al (2019) explored the current capabilities of attackers that offer account hijacking services. In their study the researchers created fake victim accounts with unique personas to be used as targets. Each victim profile was made look as legitimate as possible with an email address, a strong randomly generated password, and a name. Each fake victim account had a Gmail email account associated with their name to reinforce that the email account was actually owned by the fake victim account. In addition to this, each account had SMS-based two-factor authentication enabled and linked to a unique phone number (Mirian, et al., 2019).

The researchers discovered that most of the hack for hire service providers had problems in bypassing two-factor authentication even though they were successful in obtaining the victim's account password through targeted phishing attack. Most of the service providers used multiple page redirections, for example once the victim entered their credentials, they were redirected to a new screen which asked for the 2FA code. The researchers argue that based on the observed behavior and speed of the attackers being able to use captured credentials to authenticate to the targeted service they were using an automated tool, such as publicly available tool known as Evilginx.

The hypothesis is that two-factor authentication creates friction for attackers as shown by Mirian, et al (2019). Most of the service providers were unable to compromise the tailored victim accounts as they had 2FA enabled. Also, the study done by researchers at New York University and Google shows that knowledge-based challenged, such as recovery email address was the most insecure option as it prevented only over 73% of automated attacks and only 10% of attacks involving phishing emails. On-device prompts, such as push notifications during two-factor authentication proved to be one of the strongest protection methods as they prevented 99% of attacks involving phishing emails and 90% of targeted attacks. SMS-based challenges were considered to provide sufficient protection against automated phishing campaigns by preventing 96% of the attacks, but only 76% of targeted attacks. Risk-aware authentication prevented over 99.99% of automated hijacking attempts and over 92% of attacks involving phishing emails. Risk-aware authentication, which triggers a challenge for the user to provide a second proof of identity, such as proof of access to backup account or security question (Doerfler, et al., 2019; Mirian, et al., 2019).

8.6 Tooling

This section discusses some of the open-source offensive security tooling that has been released that can be used for educational purposes to observe and try out known offensive techniques that has been used by threat actors to compromise organizations. As with any open-source tooling anyone can modify the capabilities and add their own to evade previously built detections and make use of the tooling's capabilities. However, discussion regarding customizing offensive capabilities of specific tooling is out of scope of this paper.

8.6.1 EvilClippy

EvilClippy[8] is a tool developed and published by Stan Hegt from Outflank. It is a cross-platform assistant that can be used to create malicious MS Office documents. Additional features include hiding VBA macros, VBA stomping and techniques to confuse macro analysis tools to make forensic work more difficult (Hegt, 2019). At the time of publication of the tool (March 28, 2019) it was capable to create malicious MS Office documents that were able to bypass most major antivirus products. Since the tool is fully open source the techniques deployed in the tool can be modified by anyone to still achieve similar success.

8.6.2 SharpShooter

SharpShooter[9] was originally developed for internal use by MDSec and is designed for fileless malware payload generation (Chell, 2019). Fileless malware is a type of malicious code execution technique where the payload operates completely in process memory meaning no files are touching the disk, thus making it more difficult for antivirus software to detect and prevent (Kumar, 2020).

[8] https://github.com/outflanknl/EvilClippy

[9] https://github.com/mdsecactivebreach/SharpShooter

SharpShooter can be used to generate multiple types of payloads with different file formats that are commonly used by known threat actors. The payloads generated by SharpShooter can be used by attackers to be delivered either directly as an email attachment or tricking the victim clicking a link within the email to open an attacker-controlled web page where the payload is then served to the user.

For more information in regard to the inner workings of SharpShooter and how to build detections for it can be found from a very comprehensive blog series post by Chung from F-Secure (Chung, 2018).

9 DELIVERY

As stated in Verizon's Data Breach Investigation Reports email is the most common delivery vector when it comes to social engineering attacks (Verizon, 2020). Before attackers launch phishing campaigns one crucial point is to setup infrastructure that is used to host landing pages, email servers that are used for delivery and any other infrastructure that might be required for example to handle command and control traffic. Attacker infrastructure is discussed in more detail in Section 8 (Weaponization).

This section shortly covers the basic principle behind pretexting and how real-world threat actors are using pretexting in delivery phase to entice their victims to open malicious links or attachments which eventually would lead to an account or network compromise. Additionally, a short section is included that contains a summary of some of the publicly available phishing kits that can be used to automate the delivery phase of a phishing campaign.

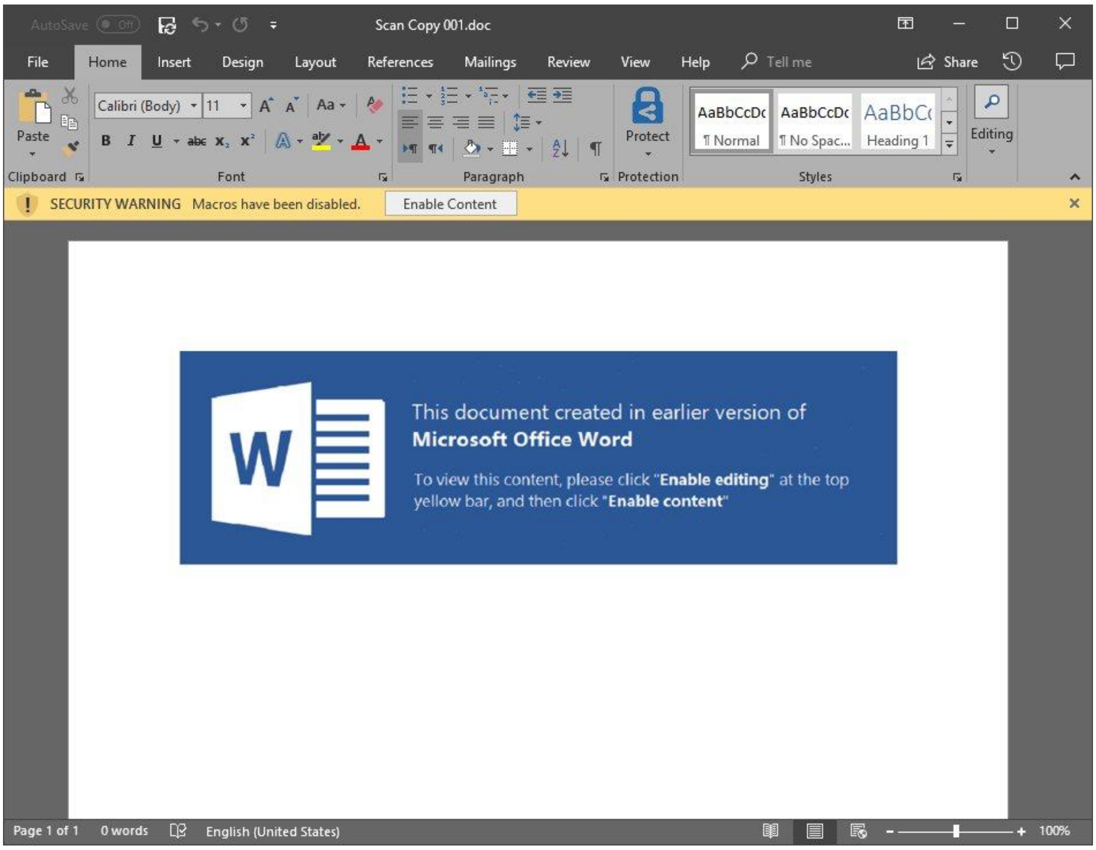
9.1 Pretexting

Pretexting has seen an increase in malicious use since Internet has become more widely adopted and attackers have started performing social engineering-based attacks, such as phishing campaigns as stated by Hadnagy (2015). Pretexting is one of the key factors of delivering and achieving success in social engineering or in a phishing campaign. Pretexting is the background of the story that a social engineer or attacker is using to entice the victim to perform certain actions on the attacker's behalf (Hadnagy, 2015).

An example of a pretexting in phishing campaign would be where an attacker sends a phishing campaign targeting small number of individuals in an organization. The targeted individuals are financial controllers, who's daily job is to handle invoicing. The attacker's objective is to achieve code execution on one of the controller's workstations through a malicious Office document, which contains a backdoor that once triggered established a command and control channel to an attacker-controlled infrastructure. In the described scenario, the pretext would be twofold. First, the attacker must somehow convince the recipients after reading the e-mail to download and open the malicious Office document. Second, since Office documents do not by default enable Macros, which is one of the most common methods to achieve code execution through Office documents as been documented by several threat actors, the attacker must somehow convince the recipient to enable Macros on the document for the attacker's payload to be executed (Kizhakkinan, et al., 2016).

Commonly established methods to convince the recipient to enable Macros is to either blur or "protect" the actual content of the document with a secondary pretext. Several examples have been documented and available online[10][11][12][13] where the pretext is either stating that the document is encrypted and cannot be viewed before the Macros are enabled or that the document has been created with an older version of Office and to view the content the user needs to enable Macros.

The following example in Figure 6 provided by Microsoft Office 365 Threat Research Team (2018) describes a common social engineering method used by attackers to trick their victims to enable and execute macros. The document could contain for example an arbitrary code inside the Word document, which is executed once the user clicks on the "Enable Content" and "Enable Editing" buttons. In the example provided by Microsoft, the document is used to download an additional RTF-file, which contained an embedded malicious Excel spreadsheet file which, if executed, downloads an additional .NET executable that contains a keylogger that is designed to steal sensitive information, such as credentials (Microsoft O365 Threat Research Team, 2018).



SECURITY WARNING Macros have been disabled.

This document created in earlier version of
Microsoft Office Word

To view this content, please click "**Enable editing**" at the top yellow bar, and then click "**Enable content**"

Figure 6 Pre-text for a malicious attachment (Microsoft O365 Threat Research Team, 2018)

[10] https://twitter.com/JohnLaTwC/status/1245852289476096000
[11] https://twitter.com/JohnLaTwC/status/1236403291845611520
[12] https://twitter.com/JohnLaTwC/status/1185723190359646208
[13] https://twitter.com/JohnLaTwC/status/1089572501523378176

9.2 Phishing Kits

This section covers some of the publicly available and open-sourced phishing kits that are available that can be used to setup, weaponize, deliver and collect credentials as part of targeted phishing campaigns. The phishing kits that are covered in master's thesis are initially designed and created by security professionals and organizations with an intent to provide learning opportunities and should not be used for illegal purposes. There are also commercial tools available, such as Rapid7 Metasploit Pro[14] which has an additional social engineering feature that provides phishing awareness management and capabilities to perform spear phishing campaigns.

As discovered by Cova, Kruegel and Vigna (2008) there is an emerging underground market where phishing kits are freely distributed. As described in their research these "tools are available to streamline the operation of creating the initial copy of the target web site, to add the code that collects sensitive information, and to simplify the configuration of the phishing web site." (Cova, Kruegel & Vigna, 2008, p. 1). However, the researchers also discovered that often these freely distributed phishing kits in underground marketplaces contain malicious code that is designed to forward the phished information back to the original authors (Cova, Kruegel & Vigna, 2008).

9.2.1 Social Engineering Toolkit

Social Engineering Toolkit (SET)[15] is developed by David Kennedy who is the founder of the cyber security company TrustedSec. SET includes multiple weaponization and evasion techniques that can be used to develop payloads to perform targeted phishing campaigns against end users. It also has the ability to clone and host a target web site and work as a delivery platform to send phishing emails and to perform credential harvesting. For example, the spear phishing attack vector can be used to send targeted emails with malicious attachments to evaluate organizations technical controls and user awareness to stop targeted attacks.

9.2.2 Gophish

Gophish[16] is an open-source phishing toolkit designed for organizations and security professionals. It can be used to quickly and easily setup and execute phishing engagements and security awareness training. Gophish includes a full HTML editor that can be used to clone and design landing pages for phishing campaigns. It also includes a separate delivery mechanism that can be used to send phishing emails to the targeted organization as well as results tracking that

[14] https://www.rapid7.com/products/metasploit/download/editions/
[15] https://github.com/trustedsec/social-engineer-toolkit
[16] https://github.com/gophish/gophish

allows to see how many users have for example opened the email or submitted their credentials.

Gophish does not include any weaponization or evasion techniques that are bundled with Social Engineering Toolkit. However, Gophish has extensive reporting capabilities which Social Engineering Toolkit does not currently have. The reporting functionality can be used to import the phishing results with a high-level summarization of the phishing campaign results.

9.2.3 King Phisher

King Phisher[17] is a phishing campaign toolkit that can be used to design and launch phishing attacks with the purpose of evaluating security awareness on organizations. King Phisher has multiple features, such as cloning and setting up phishing web sites, delivery mechanism to send phishing emails, support for two-factor authentication bypass and credential harvesting as well as alerting capabilities regarding campaign statuses. As with Gophish, King Phisher does not have weaponization and evasion techniques that are bundled with Social Engineering Toolkit.

9.2.4 Conclusion

The most effective tools available to perform automated and large-scale phishing campaigns are phishing kits (Cova, et al., 2008). As organizations or security professionals are planning to perform large-scale phishing campaigns, they should only use either commercial or publicly available open-sourced phishing kits that has been developed by known security professionals. As previous research has shown the underground market's phishing kits most likely includes backdoors that are designed to send the harvested information to the authors of the kit. As an additional security measure when using open-source toolkits a code review should be performed to ensure that the tool or framework does not perform any illegitimate activities.

[17] https://github.com/rsmusllp/king-phisher

10 EXPLOITATION

> Exploitation is the ability to find and exploit vulnerabilities in software programs, hardware devices, or network configurations. This expertise is required during initial access, persistence, and expansion. Without exploitation expertise, the Attacker cannot perform even the most basic operation (Monte, 2015, p. 38).

10.1 0-days

0-day or zero-day refers to a security vulnerability that is unknown to the software vendor (Sood & Enbody, 2014). Attackers commonly target software that is widely used to identify zero-day vulnerabilities, such as Microsoft Office and Adobe Flash Player as these are widely used and provide large attack surface areas (Virus Bulletin, 2019). For example, Microsoft has been one of the most exploited companies by having numerous zero-day vulnerabilities (Evans & Yuan, 2011).

A threat intelligence report by Kaspersky Lab documents how threat actors have been using previously unknown vulnerabilities in Adobe Flash Player that were delivered through a Microsoft Office document (Kaspersky Lab, 2017). FireEye has also documented a threat actor that leveraged Windows zero-day exploit in payment card data attacks where they sent tailored spear phishing campaign targeting retail, restaurant and hospitality industries (Kizhakkinan, Wang, Caselden, Eng, 2016). Russian cyber-espionage campaigns targeting high-profile organizations, such as NATO and European Union has also extensively leveraged zero-day vulnerabilities and spear phishing to achieve their objectives (Sharwood, 2014).

Zero-day attacks has only a limited lifetime before the vulnerability is disclosed and remediated by vendors (Wang, et al., 2014). However, even though the vulnerability is patched by the software vendor it does not make the attack vector unusable since organizations may not be able to fix or are not aware of the fact that they are affected by that specific vulnerability (Mahrous & Malhotra, 2018).

10.2 Publicly known vulnerabilities

When a zero-day vulnerability is disclosed and patched it becomes a publicly known vulnerability. As previously identified, even sophisticated threat actors mostly use publicly known vulnerabilities to compromise organizations. In 2019 a critical severity vulnerability was disclosed in Pulse Secure VPN software that allowed an unauthenticated user to execute malicious code on vulnerable servers (PulseSecure, 2019). As reported by Tung and Cimpanu in their news articles (2019; 2020), this vulnerability was initially exploited in the wild by nation-state entities and organized crime groups for ransomware attacks. If attackers were able to exploit organizations before they had patched the vulnerability allowed them persistent access into their networks due to disclosure of valid user credentials (CISA, 2020).

FireEye Threat Intelligence identified a spear phishing campaign in August 2015 that targeted Hong Kong media companies using an older vulnerability in Microsoft Office that dated back to 2012 (FireEye Threat Intelligence, 2015). Additionally, some nation state sponsored threat-actors have preferred to use older, known vulnerabilities to compromise their targets instead of investing time and resources in discovering and building new exploits (Scroxton, 2020).

There has been a lot of discussion related to the public release of offensive security tooling and capabilities. One of the continuous discussion topics has been the public release of exploit code when vulnerabilities are being disclosed by software vendors. Andrew Thompson (2019) states that public disclosure of exploitation code lowers the bar and provides unnecessary capabilities for wider audience to abuse the vulnerabilities and compromise organizations. The public disclosure of exploit code of course directly supports adversaries' capabilities to take advantage of unpatched systems since "the time and resources identifying vulnerabilities and developing working exploits are represented as opportunity cost" (Thompson, 2019). As Monte (2015) has stated that without exploitation ability the attacker cannot perform even the most basic operation and publicly disclosing techniques directly supports the attackers modus operandi and may even fast track their progress in achieving their objectives.

The release of offensive capabilities, such as exploit code is a difficult topic and the discussions is more than welcomed. However, the discussion behind the ethics of publicly releasing exploit code is out of scope of this thesis and is welcomed as a future research idea.

11 DISCUSSION AND CONCLUSIONS

This section includes the discussion and overall conclusions of this master's thesis as well as suggestions for future research. As this was the author's first larger academic research project the overall progress during this project has been considerable. Also, completion of this research project supports any future endeavors, whether it is academic research or project-related research where the objective is to identify new techniques or develop technical capabilities in the field of cyber security.

11.1 Research limitations, success and impact

The limitations, success and impact of this research can be considered to be two-fold; practical or theoretical. In practical approach organizations or individuals reviewing this master's thesis can take actionable tasks to improve their overall cyber security resilience by protecting and preparing against phishing campaigns. From theoretical standpoint this master's thesis combines both practical and academic worlds where real-world threat intelligence reports and academic research papers are used to learn and built understanding of attacker's capabilities, tactics, techniques and procedures. It can also be that the results of this master's thesis motivate new academic research on this field and especially regarding the offensive capabilities of modern threat actors as it is mostly concentrated on professional literature and threat intelligence reports.

Limitations of this research are related to the small sample analysis of publicly available offensive security tooling and capabilities. The development lifecycle of offensive security tooling is fast paced and new tooling as well as capabilities are published with an accelerating rate. Offensive security tooling and capabilities are evolving continuously and tooling that was used few years ago actively in several campaigns may be already replaced by another tooling or technique that is more prevalent in achieving the objective by having better capabilities to evade detective and preventative security controls.

Additional limitations are that organizations are vastly different, and the results and findings made in this master's thesis are not applicable to everyone. Also, much of the content that was used in this research are gathered from publicly available threat intelligence and data breach reports. There is not that much of academic research being done related to modern attacker techniques that have been used while compromising organizations, which may impact on the academic quality of this master's thesis. However, during this master's thesis new research was published regarding the impact of using multi-factor authentication to protect against phishing attacks and what are the most critical hours of a phishing campaign for organizations to react.

Success of this research is mostly based on the overall analysis of modern attacker techniques, tactics and procedures that are commonly used by real-world threat actors that were obtained through the literature review. These provide further insight into how adversaries are performing targeted operations and what technical capabilities are there to bypass modern security controls, such as multi-factor authentication. Although this master's thesis discusses different offensive techniques and tooling that are available it also provides means for organizations and defenders to better understand what the current capabilities and techniques are. This is to help them design and implement compensating security controls, detections and response procedures to protect their critical assets and data. Also, results of this master's thesis can be used to design security awareness campaigns where the objective would be to mimic a real-world threat actor's phishing campaign to evaluate employee's capabilities to detect and report targeted phishing attacks. These also support two of the original research questions that was set in the beginning of this research; why phishing campaigns are as successful as they are and how to defend or mitigate targeted phishing attacks.

Results and content of this master's thesis could be used by organizations and defenders to learn more about the techniques, tactics and procedures that are publicly available and commonly used by threat actors. This also provides capabilities for defenders to build their own detections and enhance their response capabilities in case they fall victim of a phishing attack which results a real threat actor obtaining foothold into the network. Additionally, this master's thesis shows that phishing campaigns are evolving technically. Attackers have already widely adopted techniques such as deploying encryption for their phishing sites and categorizing domains to bypass filters and making it look legitimate and trustworthy to trick their victims into supplying sensitive information. This should force organizations to educate their employees and also enforce multi-factor authentication across all external services to protect critical assets and data in case of credentials are compromised.

11.2 Conclusions

Based on the analysis of the collected material for this master's thesis modern threat actors are most commonly relying on phishing techniques for obtaining initial access. Some of the most common means of obtaining the initial access seems to be deploying malware into an Office document, which is then executed once the user enables macros. Attackers are also more increasingly making the use of publicly available offensive security tooling and frameworks in their campaigns. Another method that attackers seems to constantly be using is the abuse of publicly known vulnerabilities as it is much more cost efficient for them instead of allocating time and resources into discovering previously unknown vulnerabilities.

While performing the literature review for this research it was also increasingly evident that new research, tooling and techniques as well as threat intelligence reports were surfacing with information related to new threat actor campaigns as well as into measures of how to identify and mitigate phishing attacks. Constant generation of new research and information also impacted on the overall research project and its scope. This drastically affected especially the amount usage of secondary sources, such as news articles and threat intelligence reports. Although the amount of information available I do believe that this master's thesis was able to capture and answer at least on some level for the presented research questions.

As it may be sometimes believed, adversaries are not that often exploiting previously unknown vulnerabilities when they are compromising organizations. It seems that it is much more common to see that when a new vulnerability has been publicly disclosed it is quickly repurposed by different threat actors to be used in their operations. Based on this finding, all organizations should take into account that keeping systems, especially critical and publicly exposed services, such as virtual private network (VPN) gateways up to date with latest security patches. Furthermore, when adversaries are performing targeted phishing campaigns most of the time the attacks are relying in abusing known vulnerabilities in common software, such as Microsoft Office, Flash or Adobe. However, it should be noted that in most cases obtaining initial foothold into the target environment has not required exploiting any unknown or known vulnerability. Instead, the attackers have just abused functionality, like Microsoft Office macros that are used to entice users to execute arbitrary code on their workstation that provides access to the attacker.

When it comes to the context of offensive security tooling and implications of publishing such capabilities and techniques it has been seen that attackers are also abusing these in their campaigns. Paul Litvak discovered in his research (2020) that adversaries with all types of sophistication levels, ranging from ransomware groups to top government agencies, are making the use of offensive security tooling. What is even more interesting in this scenario is that many of these threat actors have shipped the tools as independent executables and used them as is with few modifications (Litvak, P. 2020). In order to effectively detect and respond to any attack, it is important for an organization and defender to understand the Tools, Techniques and Procedures (TTPs) an attacker is likely to use during their campaign.

The initial research question of this master's thesis was to try to understand and discover reasons behind why phishing attacks, and especially targeted attacks are as successful as they are. Based on the research that was performed it can be concluded that the attacks remain to be successful due to number of reasons. First is that attackers are abusing systems and applications that have not been patched to prevent the exploitation of a known security vulnerability. Second, attackers are using enticing pre-texts to trick the victim into performing actions that eventually lead into completely compromising the workstation. Third is that organizations may have not invested enough in performing highly sophisticated training for their employees to detect and prevent users falling victim for these attacks and do not completely understand that how sophisticated the phishing attacks have become. As a final note it can be concluded that the deployment of multi-factor authentication would create additional friction for the attacker. This means that even though an attacker would be able to compromise the credentials they would not be able to, or at least would require additional level of sophistication to bypass the protection mechanisms that multi-factor authentication provides. Furthermore, when performing security awareness training through phishing campaigns it should concentrate on a wide variety of attack techniques and not just only capturing credentials. For example, if the organizations have widely adopted multi-factor authentication to protect their users then automated phishing campaigns that are designed to capture credentials without capabilities of recording the whole multi-factor authentication process would be useless. Additionally, in more targeted campaigns threat actor's main objective is to compromise the endpoint and establish presence on the target network. There should also be options for organizations to deploy more targeted and sophisticated phishing campaigns as part of their security awareness training to evaluate the capabilities to prevent and detect targeted phishing campaign attacks. These types of campaigns require sophisticated techniques where it is necessary to evade and bypass security controls which has not yet been successfully automated.

The second research question was related as to what are the Techniques, Tactics, and Procedures (TTPs) commonly implemented in targeted phishing attacks. As already discussed in the previous sections the most common techniques are related to abusing functionality and using enticing pre-texts to lure victims into performing actions as designed by the attacker. Even the most sophisticated threat actors are relying on publicly available tooling to achieve their objectives. Based on the literature review of threat intelligence reports, one of the most common methods to achieve initial access in a targeted phishing campaign is the usage of Office macros or exploiting a known vulnerability.

The final research question that was in the scope of this master's thesis was to evaluate how organizations could defend against targeted attacks and mitigate its impact. In my opinion, there is no silver bullet into defending against a sophisticated threat actor but there are ultimately means to mitigate the impact when someone falls victim of such an attack. As already presented, organizations should be aware of their external exposure and make sure that services that are exposed on the public Internet and that could be used to access internals services must be kept updated. In addition to this, performing more sophisticated security awareness training through targeted and carefully planned simulated attacks can the overall awareness and readiness be upgraded. Furthermore, minimizing the potential attack surface on workstations, such as disabling Office macros and keeping software and operating system up to date with latest security patches would cause friction for attackers as they would be required to develop additional evasion techniques. Deployment of multi-factor authentication would in addition to cause friction for attackers when credentials are compromised since the without the access to the employees' device the attacker would not be able access any externally exposed services and again would require them to develop their TTPs further.

In conclusion to all this, there are technological as well as procedural security controls in place for organizations that would allow them to at least make it more difficult for attackers to compromise their environments. Deployment of multi-factor authentication, certificate-based authentication or attack surface reduction configurations, such as application whitelist policies are nowhere near the ultimate answer, but they do provide means to disrupt the attacker's activities and as such provides more time to detect and react to an attack. Based on the research and analysis performed for this master's thesis my suggestion for organizations is to enforce certain security controls that are scientifically proven to decrease attacker's success rate while trying to achieve initial access.

Furthermore, what organizations should take into consideration and ensure is that email authentication is enabled and configured securely. As it has been seen in some of the analyzed threat intelligence reports, threat actors have successfully obtained initial access into an organization since their email was not configured securely and did not have email authentication controls enabled. This basically allowed the attacker to impersonate by sending emails that looked like they were originating from a colleague. This is one of the most effective pre-texts since there already is trust relationship build as the receiver of the email sees that it originates from the same domain making it unnecessary for the receiver to doubt that it would be a phishing campaign.

The public disclosure of vulnerabilities and working exploit code creates a difficult and interesting ethical question in the field of cyber security. As vulnerabilities are released with associated security patches many organizations may not have the capabilities to deploy the necessary security patches to their environment to effectively protect their assets. Once the working exploit code is released to the public it is also quite efficiently repurposed by threat actors and used in their campaigns. This was also discussed by Sood & Enbody (2014) in their book about targeted cyber-attacks:

> Even if a patch is developed to fix vulnerability, many systems remain vulnerable, often for years. Often, a patch can be disruptive to the existing systems causing side effects and instability with damaging consequences. Large institutions can have difficulty finding all dependencies while small institutions and home users may be reluctant to install a patch because of fear of side effects. Therefore, while the value may be diminished, but still known vulnerabilities can be fruitful. (Sood & Enbody, 2014, p. 42)

11.3 Suggestions for future research

As discussed in this master's thesis many security professionals and companies are publishing offensive security tooling that are reportedly being used by real threat-actors as well to compromise organizations. This has also raised a lot of discussions regarding the ethicality and motivations behind releasing offensive security tooling and publishing new tactics and techniques. For example, it is seen that when new tooling, techniques or tactics are released, real-world threat actors will make use of them. Several publicly available attack frameworks, such as PowerShell Empire and PowerSploit has been used by adversaries while performing attacks against organisations (Litvak, 2020).

When it comes to the release of offensive security tooling and capabilities, there are two sides; the ones who support the publication believes that offense informs defense and releasing the knowledge and capabilities allows defenders to build their own detections and capabilities. The other side believes that releasing such tooling and capabilities is actually unnecessary contribution and facilitates network intrusions by actors of all categories and sophistication (Thompson, 2019).

Responsible vulnerability disclosure programs have existed for a long time where security researchers inform software vendors about security vulnerabilities affecting their software and to give sufficient amount of time for the vendor to remediate the vulnerabilities before they are disclosed to the public. This same logic does not apply for offensive security tooling and capabilities. Also, in the recent years the publication of actual public release of exploit code for discovered vulnerabilities has risen. When actual, working code to exploit a vulnerability is released to the public it creates a situation where basically anyone could take the exploit code and run it against a vulnerable asset. This has created situations where organisations who have not reacted and remediated vulnerabilities affecting their services have been compromised since publicly available exploits have existed, or at least it has speeded up the process as was discussed in Section 10.2 (Publicly known vulnerabilities). I believe that future research regarding especially the ethicality behind releasing offensive tooling and capabilities as well as their implications is welcomed.

Secondly, additional research regarding using gamification as a method of raising security awareness in organisations should be studied more. As it was discussed in this master's thesis it was seen that only carefully planned phishing campaigns were able to raise the overall security awareness in organisations. Additionally, gamification of phishing campaigns and security awareness may have a negative impact where employees who are receiving the phishing emails are clicking through them just because they feel like it and want to see the end result. This can easily create a situation where employees through awareness gamification actually fall victim of a real phishing campaign leading into a full compromise of the internal network.

REFERENCES

Aas, J. (2015, 29. October). Let's Encrypt: The CA's Role in Fighting Phishing and Malware. Retrieved from: https://letsencrypt.org/2015/10/29/phishing-and-malware.html

Aas, J. (2016, 12. April). Let's Encrypt News: Leaving Beta, New Sponsors. Retrieved from: https://letsencrypt.org/2016/04/12/leaving-beta-new-sponsors.html

Ahmad, A., Webb, J., Desouza, K. C. & Boorman, J. (2019). Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinfirmation Model of Counterattack. In Computers & Security, Volume 86, 2019, p. 402-418.

Anderss, J. (2019). Foundations of Information Security: A Straightforward Introduction. San Francisco: No Starch Press.

Anti-Phishing Working Group Inc. (2019). Phishing Activity Trends Report: 4th Quarter 2019.

Anti-Phishing Working Group Inc. (2020). Phishing Activity Trends Report: 1st Quarter 2020 plus COVID-19 Coverage.

Anti-Phishing Working Group Inc. (2020). Phishing Activity Trends Report: 2nd Quarter 2020.

Arghire, I. (2017, 27. March). SecurityWeek: Let's Encrypt Issues 15,000 Fraudulent "PayPal" Certificates Used for Cybercrime. Retrieved from: https://www.securityweek.com/lets-encrypt-issues-15000-fraudulent-paypal-certificates-used-cybercrime

Arntz, P. (2017, 20. January). Malwarebytes Labs: Understanding the basics of two-factor authentication. Retrieved from: https://blog.malwarebytes.com/101/2017/01/understanding-the-basics-of-two-factor-authentication/

Benenson, Z., Girard, A., Hintz, N. & Luder, A. (2014). Susceptibility to URL-based Internet attacks: Facebook vs email. In 2014 IEEE International Conference on Pervasive Computing and Communica-tion Workshops (PERCOM WORKSHOPS), Budapest, 2014, pp. 604-609.

Benenson, Z., Gassmann, F. & Landwirth, R. (2017). Unpacking Spear Phishing Susceptibility. In Brenner M. et al. (eds) Financial Cryptography and Data

Security. FC 2017. Lecture Notes in Computer Science, vol 10323. Springer, Cham.

Bohannon, D. & Carr, N, (2017, 30. June). Obfuscation in the Wild: Targeted Attackers Lead the Way in Evasion Techniques. Retrieved from: https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html

Bright, P. (2011, 4. April). Ars Technica: Spearphishing + zero-day: RSA hack not "extremely sophisticated". Retrieved from: https://arstechnica.com/information-technology/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated/

Brumaghin, E. & Grady, C. (2017, 11. October). Spoofed SEC Emails Distribute Evolved DNSMessenger. Retrieved from: https://blog.talosintelligence.com/2017/10/dnsmessenger-sec-campaign.html

Canzoneri, N. (2014, June 12). Postmark blog: Explaining SPF record. Retrieved from: https://postmarkapp.com/blog/explaining-spf

Chaudhry, J.A. & Rittenhouse, G.R. (2015). Phishing: Classification and Countermeasures. In 7th International Conference on Multimedia, Computer Graphics and Broadcast-ing (MulGraB), Jeju, 2015, pp. 28-31.

Chell, D. (2018, March). MDSec blog: Payload Generation using SharpShooter. Retrieved from: https://www.mdsec.co.uk/2018/03/payload-generation-using-sharpshooter/

Chell, D. (2019, March). Macros and More with SharpShooter v2.0. Retrieved from: https://www.mdsec.co.uk/2019/02/macros-and-more-with-sharpshooter-v2-0/

Chen, J., Kakara, H. & Shoji, M. (2019). Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data. TrendMicro.

Chung, W. (2018, 20. August). Analyzing SharpShooter – Part 1. Retrieved from: https://blog.f-secure.com/analyzing-sharpshooter-part-1/

Chung, W. (2018, 12. September). Analyzing SharpShooter – Part 1. Retrieved from: https://blog.f-secure.com/analyzing-sharpshooter-part-2/

Cimpanu, C. (2017, 15. December). Microsoft disables DDE Feature in Word to Prevent Further Malware Attacks. Retrieved from:

https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/

Clabur, T. (2020, 21. May). The Register: To test its security mid-pandemic, GitLab tried phishing its own work-from-home staff. 1 in 5 fell for it. Retrieved from: https://www.theregister.com/2020/05/21/gitlab_phishing_pentest/

Cole, R., Moore, A., Stark, G. & Stancill, B. (2020, 5. February). STOMP 2 DIS: Brilliance in the (Visual) Basic. Retrieved from: https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html

Cormack, G. V. (2008). *Email spam filtering: A systematic review*. Now Publishers Inc.

Cova, M., Kruegel, C. & Vigna, G. (2008). There is no free phish: An analysis of "free" and live phishing kits. In Proceedings of the 2nd Conference on USENIX Workshop on Offensive Technologies

CrowdStrike. (2019, February 12). CrowdStrike blog: Who is FANCY BEAR (APT28)?. Retrieved from: https://www.crowdstrike.com/blog/who-is-fancy-bear/

CrowdStrike. (2020). 2020 Global Threat Report.

Cybersecurity & Infrastructure Security Agency. (2020, 16. April). Continued Threat Actor Exploitation Post Pulse Secure VPN Patching. Retrieved from: https://us-cert.cisa.gov/ncas/alerts/aa20-107a

Death, D. (2018, 5. October). Forbes: The Cyber Kill Chain Explained. Retrieved from: https://www.forbes.com/sites/forbestechcouncil/2018/10/05/the-cyber-kill-chain-explained/

Derouet, E. (2016). Fighting phishing and securing data with email authentication. *Computer fraud & security, 2016*(10), pp. 5-8.

Doerfler, P., Thomas, K., Marincenko, M., Ranieri, J., Jiang, Y., Moscicki, A. & McCoy, D. (2019). Evaluating Login Challenges as a Defense Against Account Takeover. In The World Wide Web Conference, May 2019, pages 372-382.

Evans, N. & Yuan, X. (2011). Observation of recent Microsoft Zero-Day Vulnerabilities. In Proceedings of the 49th Annual Southeast Regional

Conference (ACM-SE ’11). Asso-ciation for Computing Machinery, New York, USA, 328-329.

El-Sherei, S. (2016, 20. May). PowerShell, C-Sharp and DDE The Power Within. Retrieved from: https://sensepost.com/blog/2016/powershell-c-sharp-and-dde-the-power-within/

Falcone, R. (2018, 15. March). Palo Alto Networks Unit42 blog: Sofacy Uses Dealers Choice to Target European Government Agency. Retrieved from: https://unit42.paloaltonetworks.com/unit42-sofacy-uses-dealerschoice-target-european-government-agency/

Federal Bureau of Investigation. (2018, July 12). Business E-mail Compromise The 12 Billion Dollar Scam. Retrieved from: https://www.ic3.gov/Media/Y2018/PSA180712

Finnish Transport and Communications Agency National Cyber Security Centre. (2020, July 21). NCSC News: Protection against Microsoft Office 365 credential phishing and data breaches. Retrieved from: https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/protection-against-microsoft-office-365-credential-phishing-and

FireEye. (2014). APT28: A Window Into Russia’s Cyber Espionage Operations? California: FireEye.

FireEye Threat Intelligence. (2017, 1. December). China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Media Outlets. Retrieved from: https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

Fisher, D. (2011, 2. April). Threatpost: RSA: SecurID Attack Was Phishing Via an Excel Spreadsheet. Retrieved from: https://threatpost.com/rsa-securid-attack-was-phishing-excel-spreadsheet-040111/75099/

Ghafir, I., Prenosil, V., Hammoudeh, M., Aparicio-Navarro, F., Rabie, K. & Jabban, A. (2018). Disguised executable files in spear-phishing emails: detecting the point of entry in advanced persistent threat. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (ICFNDS '18). pp. 1–5.

Goel, S., Williams, K. & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability," Journal of the Association for Information Systems: Vol. 18 : Iss. 1, Article 2.

Goulding, C. (2002). Grounded theory: A practical guide for management, business and market researches.

Greenberg, A. (2020, June 4). Wired: This Map Shows the Global Spread of Zero-Day Hacking Techniques. Retrieved from: https://www.wired.com/story/zero-day-hacking-map-countries/

Grugq, T. E. @thegrugq. (2015, 7. February). *Give a man an 0day a*. Twitter. Retrieved from: https://twitter.com/thegrugq/status/563964286783877121

Görling, S. (2007). An overview of the Sender Policy Framework (SPF) as an anti-phishing mechanism. Internet Research. Vol. 17 No. 2, pp. 169-179.

Hadnagy, C. (2011). Social Engineering: The Art of Human Hacking. Indianapolis: Wiley.

Hadnagy, C., Fincher, M. (2015). Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-Mails. Indianapolis: Wiley.

Hatton, L. & John, A. (2017). Delivering Genuine Emails in an Ocean of Spam. IEEE Software, 34(4), pp. 11-15.

Haughom, J., Singh, B. & Ortolani, S. (2020) Evolution of Excel 4.0 Macro Weaponization. Retrieved from: https://vblocalhost.com/uploads/VB2020-61.pdf

Hegt, S. (2018, 6. October). Old school: evil Excel 4.0 macros (XLM). Retrieved from: https://outflank.nl/blog/2018/10/06/old-school-evil-excel-4-0-macros-xlm/

Hegt, S. (2019, 5. May). Evil Clippy: MS Office maldoc assistant. Retrieved from: https://outflank.nl/blog/2019/05/05/evil-clippy-ms-office-maldoc-assistant/

Henderson, S., Roncone, G., Jones, S., Hultquist, J. & Read, B. (2020, April 22). Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage. Retrieved from: https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html

Hong, J. (2012). The state of phishing attacks. In Communications of the ACM, pp. 74–81.

Hutchins, E., et al. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In the Proceedings of the 6th International Conference on i-Warfare and Security, 2011.

Hyppönen, M. (2011, 26. August). F-Secure Labs blog: How We Found the File That Was Used to Hack RSA. Retrieved from: https://archive.f-secure.com/weblog/archives/00002226.html

Internet Engineering Task Force. (2011). Domain Identified Mail (DKIM) Signatures. (Request For Comments: 6376). Retrieved from: https://tools.ietf.org/html/rfc6376

Internet Engineering Task Force. (2014). Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. (Request For Comments: 7208). Retrieved from: https://tools.ietf.org/html/rfc7208

Kaspersky. (2017, 16. October). BlackOasis APT and new targeted attacks leveraging zero-day exploit. Retrieved from: https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

Kizhakkinan, D., et al. (2016, 11. May). FireEye Threat Research blog: Threat Actor Leverages Windows Zero-day Exploit in Payment Card Data Attacks. Retrieved from: https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html

Kumar, S. (2020). An emerging threat Fileless malware: a survey and research challenges. In Cybersecurity 3, Article 1.

Lagadec, P. (2019, 4 – 5. December). Advanced VBA Macros Attack & Defence. Black Hat Europe security conference. Retrieved from: https://www.decalage.info/files/eu-19-Lagadec-Advanced-VBA-Macros-Attack-And-Defence.pdf

Lang, J. (2016, 23. September). _SHELLNTEL blog: Luckystrike: An Evil Office Docu-ment Generator. Retrieved from: https://www.shellntel.com/blog/2016/9/13/luckystrike-a-database-backed-evil-macro-generator

Lee, B., Falcone, R. (2018, 23. February). Palo Alto Unit42 blog: OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved from:

https://unit42.paloaltonetworks.com/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/

Lee, B. (2018, 28. February). Palo Alto Networks Unit42 blog: Sofacy Attacks Multiple Government Entities. Retrieved from: https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/

Lee, R., Assante, M. & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center & SANS Industrial Control Systems. Retrieved from: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Leiba, B. & Fenton, J. (2007). DomainKeys Identified Mail (DKIM): Using Digital Signatures for Domain Verification. In CEAS.

Le Page, S., Jourdan, G., Bochmann, G. V., Flood, J. & Onut, I. (2018). Using URL shorteners to compare phishing and malware attacks. In 2018 APWG Symposium on Electronic Crime Research (eCrime), San Diego, CA, 2018, pp. 1-13

Let's Encrypt. (2019). Let's Encrypt 2019 Annual Report. Retrieved from: https://www.abetterinternet.org/documents/2019-ISRG-Annual-Report-Desktop.pdf

Lewis, J. (2018). Economic Impact of Cybercrime – No Slowing Down. McAfee.

Li, M., Huang, W., Wag, Y., Fan, W. & Li, J. (2016). The Study of APT Attack Stage Model. In 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, 2016, pp. 1-5

Litvak, P. (2020). The OST Map: Mapping The Use Of Open-Source Offensive Security Libraries in Malware. In The 30th VirusBulletin Conference – VB2020 localhost.

Llimos, N. & Pascual, C. (2019, 12. February). Trickbot Adds Credential-Grabbing Ca-pabilities. Retrieved from: https://www.trendmicro.com/en_us/research/19/b/trickbot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire.html

Metrick, K., Najafi, P. & Semrau, J. (2020, April 6). FireEye Threat Research blog: Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill – Intelligence for Vulner-ability Management, Part One. Retrieved from: https://www.fireeye.com/blog/threat-research/2020/04/zero-day-exploitation-demonstrates-access-to-money-not-skill.html

Microsoft. (2017, 11. October). Microsoft Security Advisory 4053440. Retrieved from: https://docs.microsoft.com/en-us/security-updates/securityadvisories/2017/4053440

Microsoft. (2018, 31. May). About Dynamic Data Exchange. Retrieved from: https://docs.microsoft.com/en-us/windows/win32/dataxchg/about-dynamic-data-exchange

Microsoft. (2018, 11. July). Office 365 Threat Research Team blog: Hawkeye Keylogger – Reborn v8: An in-depth campaign analysis. Retrieved from: https://www.microsoft.com/security/blog/2018/07/11/hawkeye-keylogger-reborn-v8-an-in-depth-campaign-analysis/

Microsoft. (2018, 12. September). Office VBA + AMSI: Parting the veil on malicious macros. Retrieved from: https://www.microsoft.com/security/blog/2018/09/12/office-vba-amsi-parting-the-veil-on-malicious-macros/

Mills, J., & Birks, M. (2014). Qualitative methodology. 55 City Road, London: SAGE Publications, Inc.

Mimura, M. & Ohminami, T. (2020). Using LSI to Detect Unknown Malicious VBA Macros. In Journal of Information Processing, Vol. 28, pp. 493-501.

Mirian, A., et al. (2019). Hack for Hire: Exploring the Emerging Market for Account Hijacking. In The World Wide Web Conference, May 2019, pages 1279-1289.

MITRE. (2020). ATT&CK Matrix for Enterprises: Phishing: Spearphishing Attachment. Retrieved from: https://attack.mitre.org/techniques/T1566/001/

Monte, M. (2015). Network Attacks and Exploitation: A Framework. Indianapolis: Wiley

National Cyber Security Centre. (2018). Indicators of compromise for malware used by APT28. National Cyber Security Centre a part of GCHQ. Crown Copyright 2018.

Nero, P.J., Wardman, B., Copes, H. & Warner, G. (2011). Phishing: Crime that pays. eCrime Researchers Summit, San Diego, CA, 2011, pp. 1-10

O'Reilly, M. & Kiyimba, N. (2015). Advanced Qualitative Research: A guide to Using Theory. SAGE Publications Ltd. London.

Oest, A., Safei, Y., Doupé, A., Ahn, G., Wardman B. & Warner, G. (2018). Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis. In 2018 APWG Symposium on Electronic Crime Research (eCrime), San Diego, CA, 2018, pp. 1-12

Oest, A., Zhang, P., et al. (2020). Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiviness of Phishing Attacks at Scale. In Proceedings of the 29th USENIX Security Symposium, August 12 – 14, 2020.

Ogden, H., Roberts, C. & Sayre, K. (2018). VBA Stomping: Advanced Malicious Document Techniques. DerbyCon security conference. Retrieved from: https://github.com/clr2of8/Presentations/blob/master/DerbyCon2018-VBAstomp-Final-WalmartRedact.pdf

Oktay, J. S. (2012). Grounded Theory. Oxford University Press, USA.

Orru, M & Trotta, G. (2019). Muraena: The Unexpected Phish. In Hack In The Box 2019 Security Conference. Amsterdam.

Petsalis, M. (2018, February 19). IT Pro Portal: Why targeted phishing is the most dangerous fraud businesses face today. Retrieved from: https://www.itproportal.com/features/why-targeted-phishing-is-the-most-dangerous-fraud-businesses-face-today/

PulseSecure. (2019, 24. April). SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX. Retrieved from: https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

Raulot, A. (2019). Bypassing phishing protections with email authentication. *Master Security and Network Engineering*, *5*.

Sanghvi, H. (2013). Cyber Reconnaissance: An Alarm before Cyber Attack. In International Journal of Computer Applications (0975 - 8887), Volume 63 – No. 6, February 2013.

Sanz, E., Hidalgo, J. & Perez, J. (2008). Email Spam Filtering. Advances In Computers, Vol 74, 74, pp. 45-114.

Scroxton, A. (2020, 13. May). Nation state APT groups prefer old, unpatched vulnerabilities. Retrieved from:

https://www.computerweekly.com/news/252483043/Nation-state-APT-groups-prefer-old-unpatched-vulnerabilities

Sharwood, S. (2014, 14. October). Russian hackers exploit 'Sandworm' bug 'to spy on NATO, EU PCs'. Retrieved from: https://www.theregister.com/2014/10/14/isight_microsoft_announce_windows_and_windows_server_0day/

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Sus-ceptibility and Effectiveness of Interventions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10). Association for Computing Machinery, New York, NY, USA, 373-382.

Sherstobitoff, R. (2017, 7. November). Threat Group APT28 Slips Office Malware into Doc Citing NYC Terror Attack. Retrieved from: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/apt28-threat-group-adopts-dde-technique-nyc-attack-theme-in-latest-campaign/

Siadatii, H., Palka, S., Siegel, A. & McCoy, D. (2017). Measuring the effectiveness of embedded phishing exercise. In 10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17), 2017.

Silverman, D. (2016). Qualitative Research. London: SAGE Publications Ltd.

Smith, L. & Read, B. (2017, 11. August). FireEye Threat Research blog: APT28 Targets Hospitality Sector, Presents Threat to Travelers. Retrieved from: https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html

Sood, A. K. & Enbody, R. (2014). *Targeted cyber attacks: Multi-staged attacks driven by exploits and malware.* Amsterdam; Boston: Syngress

Stalmans, E. & El-Sherei, S. (2017, 9. October). Macro-less Code Exec in MSWord. Retrieved from: https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/

Särud, L. (2016, 20. June). Detectify blog: Misconfigured email servers open the door to spoofed emails from top domains. Retrieved from: https://blog.detectify.com/2016/06/20/misconfigured-email-servers-open-the-door-to-spoofed-emails-from-top-domains/

Thompson, A. (2019, 29. November). Misconceptions: Unrestricted Release of Offensive Security Tools. Retrieved from:

https://medium.com/@anthomsec/misconceptions-unrestricted-release-of-offensive-security-tools-789299c72afe

Thurman, M. (2013). Spam makes a comeback: Out of the blue, phishing attacks previously caught in the spam filter are getting through to employee. (Security Manager's Journal). Computerworld, 47(4), p. 35.

Tiilikainen, S., Manner, J. (2013). Suomen automaatioverkkojen haavoittuvuus: Raportti Internetissä julkisesti esillä olevista automaatiolaitteista. Helsinki: Aalto University.

TrendMicro Inc. (2012). TrendLabs APT Research Team: Spear-Phishing Email: Most Favored APT Attack Bait. Retrieved from: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

Ussath, M., Jaeger, D., Cheng, F. & Meinel, C. (2016). Advanced Persistent Threats: Behind the Scenes. In 2016 Annual Conference on Information Science and Systems (CISS). Princeton, NJ, 2016, pp. 181-186.

Verizon Enterprise. (2018). Verizon Data Breach Investigation Report: 2018 Data Breach Investigations Report. Retrieved from: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

Verizon Enterprise. (2019). Verizon Data Breach Investigation Report: 2019 Data Breach Investigations Report. Retrieved from: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Verizon Enterprise. (2020). Verizon Data Breach Investigation Report: 2020 Data Breach Investigations Report. Retrieved from: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Zetter, K. (2011, 26. August). Wired: Researchers Uncover RSA Phishing Attack, Hiding in Plain Sight. Retrieved from: https://www.wired.com/2011/08/how-rsa-got-hacked/