Analysis of Nation-State Phishing Email Attack Vectors

Brian T. Carr

Utica College

Dr. Stephen Pearson

CYB-673

10/20/2019

Abstract

In the past few years crimes carried out within the cyber-domain have increased in sophistication and narrowed to targets providing the greatest return value. (Ghafir & Přenosil, 2015, p. 34) In 2018 alone phishing email attack vectors accounted for 26,379 individuals losing a total of over forty-eight million dollars. That figure does not account for the crimes which go unreported. (Internet Crime Complaint Center, 2019) Phishing email attack vectors and other social engineering attack vectors are among the highest concern for any organizational entity as it exploits the employee. (Sebescen & Vitak, 2017, p. 2238) Phishing emails have been very successful in recent years partially due to favorable technical and economic conditions. (Milletary, 2013, p. 1) Keeping that in mind, it a frightening fact that the presence of malicious phishing campaigns has steadily continued to increase. Some of these malicious phishing campaigns have been tied back to nation-state threat actors including Advanced Persistent Threats (APTs) and malicious e-crime groups. (Verizon, 2016, p. 12) APT actors have been observed implementing phishing email attack vectors in their campaigns. The effectiveness of phishing email attack vectors may explain why the most devious cybercrime organizations choose to employ them.

Table of Contents

Analysis of Nation-State Phishing Email Attack Vectors

In this paper the Author will argue that phishing email attack vectors are highly utilized by APT actors. APT threat actors present some of the most malicious attack vectors in the cyber-domain as they are some of the few groups with the necessary funding and resources to carry out this type of advanced persistent campaigns. Phishing email attack vectors are only a single type of attack vector implemented, although the combination of technical and social engineering aspects can be correlated to increased success. It is very likely that APTs will continue to use phishing email attack vectors, and specifically spear phishing email attack vectors as a method of initial compromise in their campaigns.

Literature Review

Phishing Email Attack Vectors

Phishing is the process of frequently sending communications to an end-user in order to obtain sensitive information from that end-user. Phishing email attack vectors often contain a combination of social engineering and technical attributes to obtain information, distribute malware, and harvest credentials (Graham & Triplett, 2017, pp. 1371-1372) Phishing is a type of cybercrime where the end-user directly divulges sensitive information to the attacker. In addition to emails, phishing can occur in the form of phone calls and text messages. (Shankar , Shetty, & Nath, 2019, p. 2171) Phishing is also defined as the act of stealing personal information within the cyber-domain for malicious purposes. (Milletary, 2013)

The 2018 Verizon Data Breach Investigations Report reveals that ninety-six percent of the encountered attack vectors were phishing emails. The report also explains that there has been an increase in the pretexting of these phishing email attack vectors, which may be correlated to the improved compromise rate. The report goes on to explain that fifty-nine percent

of the encountered phishing emails were aimed towards financial gain, while forty-one percent are attributed to espionage. (Verizon, 2018, p. 12)

Phishing email attack vectors are still proven to be effective at harvesting user credentials and distributing malware by tricking end-users. Some email attack vectors can even lead to ransomware infections. (Boneh, 2017) Phishing emails appear to be highly effective initial compromise vectors which can end in a variety of exploitations. Pelland (2015) describes phishing email attack vectors and spear phishing email attack vectors. Phishing emails are targeted more generally, while spear phishing email may target a specific member or members of an organization. (Pellend, 2015, p. 40) Phishing emails frequently carry their malware payloads as attachments. In the Duqu malware campaign, the initial compromise vector was determined to be an infected Microsoft Office Document. (Moon, Im, Kim, & Park , 2015, p. 2883)

Notable phishing exploitations.

Phishing email attack vectors have been very successful over the past few years, this can be attributed to favorable technical and economic conditions. (Milletary, 2013) The Amazon Prime Day phishing attack involved the information of the customers of Amazon Prime members. All amazon prime members received a fraudulent email which purported to be from Amazon. Once the end-user tried to purchase the items from the email, their credentials and other sensitive information would be harvested. (Shankar , Shetty, & Nath, 2019, p. 2171)

In May of 2007, malicious actors sent out fraudulent invitations to Google user world-wide, requesting that they order a document. Upon clicking the invitation, it led to a third-party application where the malicious actors were able to obtain sensitive user information. (Shankar , Shetty, & Nath, 2019, p. 2171)

In 2011 the security company RSA experienced a breach through a cyber-attack. Further analysis revealed that the initial compromise vector was a spear phishing email. In the same year the email service provided Epsilon experienced a spear phishing exploitation which cost the company roughly $4 billion USD. (Trend Micro, 2012, p. 1)

Phishing mitigation.

Improved digital literacy has been found to significantly affect how an individual responds to encountering a phishing email attack vector. (Graham & Triplett, 2017, p. 1371) Some controls which may help assist in the mitigation of phishing emails are: Provide warning banner for external emails, implement spam filters at gateway appliance, utilize principle of least privilege, and implement Domain-based Message Authentication, Reporting, & Conformance (DMARC) which is able to detect email spoofing by DNS records and additional signatures. (MS-ISAC, 2019)

Advanced Persistent Threat

APTs are often defined differently depending on who is referring to them. Some definitions may focus more heavily on the types of attack vectors the APT produces, and in what manor they are carried out. Other definitions focus on the APT's relationship to a Nation-State. There has yet to be a cybercrime organization without ties to a nation-state. The National Institute of Standards and Technology defines an APT as:

> An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information

> technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. (National Institue of Standards and Technology, 2013, pp. B-1)

While this definition focuses on the type of attacks being produced by the entity, other definitions may focuses on a variety of other characteristics. Definitions like the one provided by Friedberg, Skopik, Settanni, and Fielder (2014) focus on the means in which the APT carries out their campaign. An APT is a slow-moving cyber-attack applied to subliminally compromise interconnected information systems without raising any alarm. (Friedbarg, Skopik, Settanni, & Fiedler, 2015)

Notable Advanced Persistent Threats.

In 2013 researchers at Mandiant published a report on the prolific cybercrime organization known as APT1. APT1 was determine to have direct ties to the Chinese government, and specifically Unit 61398 of the People's Liberation Army. The report revealed that APT1 employs a high number of employees, hundreds and potentially thousands of personnel work for APT1. Individuals in APT1 are required to not only have personal trained in cybersecurity and networking, but also to be proficient in English. (Mandiant, 2013)

APT 28, also known as Fancy Bear is a devious APT with ties to Russia. Fancy Bear has been observed to victimize organizations in multiple nations including the United States. It is

also reported that Fancy Bear's actions are correlated with an Affiliation to the GRU, Russia largest foreign intelligence agency. (CrowdStrike, 2019)

United States Advanced Persistent Threats.

While APTs are primarily discussed in the context of how they victimize United States organizations, it may be surprising to some to discover that the United States utilized an APT at one point in time. In 2015, researchers from Kaspersky Lab's Global Research and Analysis Team (GReAT) released a report regarding a cyber-espionage group known as Equation Group. Equation Group is seen to have many similarities with other APTs, but the main difference is that it is a United States advanced persistent threat.

Advanced Persistent Threats Utilizing Phishing Email Attack Vectors

Spear phishing email attack vectors have been a favored initial compromise vector utilized by many APTs. In a typical scenario, a specially crafted spear phishing email is sent to a specific individual within the targeted organization. Through a combination of social engineering and technical attributed, the end-user is likely tricked in to compliance with a malicious action such as clicking a malicious hyperlink or downloading a malicious attachment. (Trend Micro, 2012, p. 1)

APT1 has been determined to show a common methodology in their campaigns. The campaigns being with highly malicious spear phishing emails. Next, there are typically custom attack vectors deployed. Finally, the data is exfiltrated to a Chinese computer system. APT1 has been attributed to spear phishing observed by the SCADA security company Digital Bond. (Mandiant, 2013)

Researchers from CrowdStrike report that APT28, commonly known as Fancy Bear, employs phishing emails for credential harvesting purposes. These phishing emails typically

contain hyperlinks to malicious webpages hosting the credential harvesting fields. Fancy Bear has been observed to victimize organizations in multiple nations including the United States. It is also reported that Fancy Bear's actions are correlated with an affiliation to the GRU, Russia largest foreign intelligence agency. (CrowdStrike, 2019)

Ghafir and Přenosil (2015) report that APTs typically employ multistep attack scenarios. Spear phishing attacks are observed to a favored means of initial compromise. APT attackers may also target specific individuals within an organization to increase the effectiveness of the phishing email attack vector. (Ghafir & Přenosil, 2015, p. 34)

In the summer of 2016, APT41 was observed sending spear-phishing emails to media organizations with a pro-democracy stance in Hong Kong. APT41 was reported to show a direct trend of attacking groups which are pro-democracy in Hong Kong. APT41 frequently uses popular stories from local news as a means to gain the trust of suspecting users. APT41 has been obverted to target organization in at least 14 different countries, including the United States. APT41 was additionally attributed to the phishing campaigns carried out by the email address, hrsimon59@gmail.com. This email address was responsible for committing acts of cyber espionage against a Taiwanese newspaper, and sending phishing emails to a European bitcoin exchange. (Fireeye, 2019)

Discussion of Findings

Phishing Email Attack Vectors

Graham and Triplett (2017) explain that phishing emails are communications sent via email to a user in order to extract information from that user. That definition covers the majority of cases where phishing email attack vector are employed. The Author would also broaden the definition to include any communications sent via email for a malicious purpose. Phishing email

have gone beyond credential harvesting and social engineering. Malware is frequently distributed via phishing emails, and scare campaigns including sextortion campaign are also observed. Those situations would be considered malicious, but may not directly fixated on the exfiltration of end-user data.

Phishing emails my directly attempt to impersonate a credible source, an unsuspecting user may simply assume that the email is legitimate. Phishing email are often aimed at harvesting end-user credentials, or distributing malware. Phishing emails may contain hyperlinks which lead to malicious webpages containing malware, credential harvesting fields, or other forms of malicious content. Victims who are unbale to distinguish between the malicious site, and site it is mimicking may have their credentials harvested or their systems infected with malware. (Shankar , Shetty, & Nath, 2019, pp. 2171-2172)

Phishing effectiveness.

Even phishing emails that employ low tech and old methodologies are determined to be highly effective in compromising end-users. (Graham & Triplett, 2017, p. 1371) Phishing email attack vectors have persisted for over two-decades in the cyber-domain. Authors of phishing emails are also known to change over time to advert the security controls implemented to defeat the phishing email attack vector. (Gupta, Tewari, Jain, & Agrawal, 2017, p. 3629)

In one study, forty-seven percent of targets divulged private information into a mock phishing webpage. The study determined that there are three primary factors which affect susceptibility to phishing emails: attention payed to the email, how elaborate the pretexting was, and knowledge and experience. (Harrison, Svetieva, & Vishwanath, 2016, p. 265)

Phishing mitigation.

There are numerous solutions which aim to prevent phishing emails from reaching an end-user, although none are perfect. The social engineering portion of any phishing email attack vector may still exploit even the most vigilant end-user. The best way to prevent social engineering attack vectors is to raise the awareness of the affected end-users. By implementing controls with the concept of defense in depth, one may be able to significantly increase organizations defense against this type of attack vector.

Researchers at the Multi-State Information Security Analysis Center recommend: Provide warning banner for external emails, implement spam filters at gateway appliance, utilize principle of least privilege, and implement Domain-based Message Authentication, Reporting, & Conformance (DMARC) which is able to detect email spoofing by DNS records and additional signatures. (MS-ISAC, 2019)

Advanced Persistent Threats

APTs have been seen to wreck-havoc on the behalf of nation-state entities. The actions of APT1 not only correlate with the interests of the Chinese government, but also are directly attributed to PLA Unit 61398. (Mandiant, 2013) The resources obtained by APTs from the nation-state they support allow them to facilitate lengthy and intense cybercrime campaigns. APTs have been observed to commit a variety of crimes, APT41 notably is nicknamed “Double Dragon” for their interest in both cyber-espionage and cybercrime. APT41 has been observed targeting organizations in a variety of nations, including the United States. Many of the organizations victimized by APT41 are directly tied to democratic activists in Hong Kong, further attributing their action to the nation-state of China. (Fireeye, 2019)

Notable Advanced Persistent Threats.

APT 1, formally known as the Unit 61398 of the People's Liberation Army has been observed to employ advanced campaigns in the interest of the Chinese government. The headquarters of APT 1 are additionally observed to be guarded by armed PLA guards. Additionally, the internet connection of APT1 was determined to be a special fiber optic connection provided by a Chinese telecom in the name of national defense. APT1 has been observed to have compromised over 141 companies in over twenty different industries. (Mandiant, 2013)

Advanced Persistent Threats Utilizing Phishing Email Attack Vectors

Spear phishing attack vectors are observed to be commonly employed by APT actors. (Ghafir & Přenosil, 2015, p. 34)Various APTs including APT 1 are known to employ language requirements in their hiring selections. (Mandiant, 2013) One may hypothesize that the language requirement is related to the development of social engineering attack vectors which require pretexting. APT 28, commonly known as Fancy Bear has been observed to implement phishing emails which lead to credential harvesting webpages. APT has been observed to utilize common tools and techniques including the implementation of GETMAIL and MAPIGET, two email compromising tools. (CrowdStrike, 2019)

APT41 has been observed to send phishing emails to their victims. Often their phishing emails contain pretext regarding relevant issues in the news. APT41 carried out one cyberespionage, and one cybercrime campaign from the email, hrsimon59@gmail.com. (Fireeye, 2019)

APT 28 has previously attacked entities all over the globe, but primarily in the United States and Wastern Europe. Fancy Bears targets campaings directly correlate with the interest of

the Russian government and specifically the GRU. Fancy Bear has been linked to the exploitations of Germanies Bunderstag, and a popular French TV station, TV5 Monde. (CrowdStrike, 2019)

Each of these are instances of attacks observed by security researchers, it is to be assumed that there are a variety of phishing campaign occurring which have yet to be located. In addition to new phishing campaigns, new APTs are frequently appearing. While security researches work diligently to track those APT actors, new ones may come into play at any time.

Conclusion

In this paper the Author argued that phishing emails are utilized by APT actors. The Author additionally provided supporting information on the effectiveness of phishing email attack vectors, and instances of APTs utilizing phishing email attack vectors. Various APTs including APT1, APT41, and APT28 have been observed by researchers to implement phishing emails in their cybercrime campaigns. Phishing emails are particularly malicious as they combined technical and social engineering attributes to create a particularly malicious attack vector. To prevent successful phishing compromises, applicable security controls will only help to prevent the technical aspects of the attack vector. Social engineering attacks exploit the human, which the technical controls fail to protect.

References

Boneh, D. (2017). Cybersecurity. *Communications of the ACM*, 20-21.

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

Fireeye. (2019). *APT41.* Retrieved from fireeye.com: https://content.fireeye.com/apt-41/rpt-apt41/

Friedbarg, I., Skopik, F., Settanni, G., & Fiedler, R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. *Comptuers and Security*, 35-57.

Ghafir, I., & Přenosil, V. (2015). Advanced Persistent Threat. *Distance Learning, Simulatin and Communication 2015*, 34-41.

Graham, R., & Triplett, R. (2017). Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior*, 1371-1382.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challanges. *The Natural Comptuer Applications Forum 2016*, 3629-3654.

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. *Online Informiaton Review*, 265-281.

Internet Crime Complaint Center. (2019, April 22). *2018 Internet Crime Report.* Retrieved from ic3.gov: https://pdf.ic3.gov/2018_IC3Report.pdf

Mandiant. (2013, February 19). *APT1 Exposing One of China's Cyber Espionage Units.* Retrieved from fireeye.com: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Milletary, J. (2013, February 6). *Technical Trends in Phishing Attacks.* Retrieved from psu.edu: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.146.836&rep=rep1&type=pdf

Moon, D., Im, H., Kim, I., & Park , J. (2015). DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. *Springer Scienece + Buissness Media*, 2881-2895.

MS-ISAC. (2019). *MS-ISAC Security Primer – Spear Phishing*. Retrieved from cisecurity.org: https://www.cisecurity.org/white-papers/ms-isac-security-primer-spear-phishing/

National Institue of Standards and Technology. (2013, April). *Security aand Privacy Controls for FFederal Information Systems and Organizations.* Retrieved from nist.gov: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Pellend, D. (2015). Email security risks hiding in plain sight. *Financial Executive*, 38-45.

Sebescen, N., & Vitak, J. (2017). Securing the Human: Employee Security Vulnerability Risk in Organizational Settings. *Journal of the Association for Information Science and Technology*, 2237-2247.

Shankar , A., Shetty, R., & Nath, B. K. (2019). A Review on Phishing Attacks. *International Journal of Applied Engineering Research*, 2171-2175.

Trend Micro. (2012). *Spear-Phishing Emial: Most Favored APT Attack Bait.* Retrieved from trendmicro.de: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

Verizon. (2016). *2016 Verizon Data Breach Investigations Report.* Retrieved from verizon.com: https://enterprise.verizon.com/resources/reports/2016/DBIR_2016_Report.pdf

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

ANALYSIS OF NATION STATE PHISHING EMAIL ATTACK VECTORS