PhAttApp: A Phishing Attack Detection Application

Thuy Lam[1,2] and Houssain Kettani[1]

[1]The Beacom College of Computer and Cyber Sciences, Dakota State University, Madison, South Dakota, USA
[2]Orange County Water District, Fountain Valley, California, USA
Thuy.Lam@trojans.dsu.edu, Houssain.Kettani@dsu.edu

ABSTRACT

Technology has grown rapidly since the end of the last century. Thousands of businesses from different major industries are transforming into information organizations and offering online services. The industrial and enterprise of Internet of Things (IoT) is growing at an exponential rate. Incident Command Systems (ICS) and Supervisory Control and Data Acquisition (SCADA), which were once known to be untouchable by malware as they were usually available offline, are now facing security challenges. These systems become more vulnerable as their online availability increases to enable integration with other systems. Technology allows organizations to provide greater value to customers, expand their businesses beyond physical boundaries, and compete with other businesses. However, technology also allows attackers from all over the world to attack organizations and consumers. Ransomware, a type of malware, is a growing cybersecurity threat. It mainly targets home users and businesses for financial gain. Ransomware attacks often start with a delivery phase in which attackers deliver malicious content. Attackers often use multiple threat vectors for ransomware enablement such as emails, instant messages, and drive-by downloads, exploiting the vulnerabilities of a network or application. Among these attack vectors, email is the top threat vector, which most ransomware attackers attempt to use. This study proposes the use of a phishing detector application, PhAttApp. This application offers numerous features to detect and prevent ransomware delivery through phishing channels and thus reduces the risk of ransomware infection.

CCS Concepts

• Security and privacy→Intrusion/anomaly detection and malware mitigation→Malware and its mitigation • Security and privacy→Intrusion/anomaly detection and malware mitigation→Intrusion detection systems • Security and privacy→Software and application security→Web application security

Keywords

Ransomware; scareware; cryptotrojan; cryptoware; cryptoworm; malware; Trojan; phishing; spear phishing; pretexting; malware.

ICISDM 2019, April 6-8, 2019, Houston, TX, USA

ACM ISBN 978-1-4503-6635-9/19/04 …$15.00
https://doi.org/10.1145/3325917.3325927

1. INTRODUCTION

Ransomware continues to be a serious security risk since its inception thirty years ago. Stopping ransomware is almost impossible as the software evolves over time. Moreover, the rapid growth of technology has directly contributed to the growth of ransomware, which has evolved from a simple piece of code in early malware samples to more sophisticated code today. Attackers are coming up with new techniques and tools to avoid detection. They delay the encryption process to provide the malware the opportunity to move laterally and encrypt backup files. Anti-ransomware tools often look for a linear pattern. Therefore, attackers randomize the encryption process to create disorganization and avoid detection by anti-ransomware tools. Attackers also use a polymorphic code, which complicates ransomware detection as the malware code keeps changing. They use a multi-threaded technique to accelerate the encryption process and make their malware exponentially more difficult to stop. Ransomware has not only been changing its predictable nature to avoid anti-ransomware detection, but it has also become a business. It has evolved to a level where amateur attackers can purchase a ransomware kit on a website such as Hall of Ransomware. With increasingly impactful scripts, ransomware was consistently classified in the top fifteen cyber threats in the European Union Agency for Network and Information Security (ENISA) Threat Landscape (ETL) annual report, ranking the seventh in 2017 [5]. While preventing all ransomware attacks is not possible, many researchers have published analyses, investigations, and discussions about preventing ransomware cyber threats.

Ransomware attacks mainly rely on social engineering and sophisticated encryption algorithms. These attacks exploit not only technical vulnerabilities but also human fallibility. The most common attack vector for ransomware is phishing. According to Verizon's 2018 Data Breach Investigations Report, this vector represents 98% of security incidents and 93% of breaches [11]. Despite many manual and automated approaches being introduced, phishing attacks have been continually increasing every year. Cyber attackers are getting smarter and more sophisticated. The margin for human fallibility is also increasing due to the rapid growth of technology. The 2014 IBM's Cyber Security Intelligence Index reported that 95% of security incidents in 2014 were connected to human error. The report also stated that 49% of the total of 53,000 security incidents was related to malicious email attachments, resulting in 13.11% of 1,799 confirmed data breaches [2]. Many successful security attacks are a result of external cybercriminals luring insiders into unintentionally furnishing them with sensitive information or access to organizations' systems.

As the saying goes, prevention is better than cure. It is much better to stop ransomware from entering systems than to battle its encryption or put effort into restoring data after an attack. Since phishing often occurs at the initial stage of a ransomware attack and is the top attack vector of ransomware, we propose an anti-

phishing application that we name PhAttApp. The goal of this application is to reduce human error when dealing with a phishing attack. The strategy is to use attackers' techniques against them. The application adopts an approach that is based on machine learning and behavioral analysis to combat the evolutionary nature of ransomware. It is built to distinguish between normal behavior and the behavior of ransomware. PhAttApp uses information collected from historical ransomware attacks to propose solutions and prevent future ransomware attacks. It also uses machine learning to identify new variations of ransomware.

Unlike other anti-phishing applications such as PhishShield [8] or Detection of Phishing Attacks [9] which focus on partial information in an email, PhAttApp offers a complete model, including recommendations to prevent attacks, by analyzing all parts of a typical email. The PhishShield concentrates only on the URL of the email. The Detection of Phishing Attacks concentrates on the HTML of the email, the domain and sub-domains, the presence of JavaScript and form tag in the email body, the number of links, the URL based image source, and the keywords. PhAttApp is not only able to detect phishing or scamming email from links and sender information, but it is also able to detect phishing email from abnormal email content. It tracks the trend of emails to detect abnormal email. For example, an email is considered as an abnormal email if it belongs to "Call-to-Action" category and being sent from a sender who did not send email with the category "Call-to-Action" in the past. This feature is very effective in detecting business email compromise. In addition, many anti-phishing applications such as Mimecast or Trend-Micro prevent phishing emails by using IP blacklists. They require user interaction to input static list of IP addresses to detect phishing email. This method is less affective in detecting phishing email due to user input error or the data being outdated. PhAttApp does not require user input. Instead, sender information such as IP addresses and domains, are pulled from online sources at runtime to ensure that the information is always up to date.

The application is composed of a Windows Outlook add-in and a virtual file analyzer system. The main function of the Outlook add-in is to detect phishing, pretexting, and spam emails. The add-in analyzes the email's header, subject, attachments, and message to detect scams, spoofing, malicious links, and ransomware enablement. Suspicious attachments are downloaded to the virtual file analyzer system for further analysis. The virtual file analyzer is a sandbox environment built to analyze file headers in order to detect suspicious files. It also prevents unwanted behavior arising from file execution within the system. The goal of the PhAttApp application is to create a non-technical friendly environment and yet, provide users all information they need to make decision about the credibility of the emails and the safety of their email attachments.

2. BACKGROUND AND DEFINITIONS

In this section, we define some terms related to phishing attacks that are useful in understanding the scope of this paper.

- Malware: It is a malicious software designed to perform unwanted actions on computer systems, mobile devices, network systems, tablets, the Internet of Things (IoT) and other devices. It is a general term for spyware, viruses, ransomware, worms, and Trojan horses. Malware is consistently classified in the top fifteen cyber threats in ETL annual report, being on the top since 2014 [5].
- Ransomware: It is a type of malware that intrudes into and encrypts victim's files or systems. It holds the victim's data hostage and demands a monetary ransom for the decryption key. It can come in the form of fake antivirus software that tricks victims into purchasing bogus software or as fake authorized services that trick victims into paying a fine. Ransomware is consistently classified in the top fifteen cyber threats in ETL annual report, ranking the seventh in 2017 [5].
- Phishing: It involves an email message crafted to influence recipients to click on a link or an attachment. The link takes the recipient to a malicious website that asks for the recipient's credentials or downloads malware to the recipient's system. The email attachment often contains malware that is executed once the recipient clicks on it. Attackers exploit psychological vulnerabilities to manipulate people into divulging information or performing actions. Phishing is consistently classified in the top fifteen cyber threats in ETL annual report, ranking the fourth in 2017 [5].
- Spear Phishing: It is a more focused type of phishing in which attackers focus on a specific group of users. The attackers create personalized scam email messages to steal recipients' information or to influence recipients' behavior.
- Business Email Compromise: It is a spoofing attack where attackers first compromise legitimate business email accounts. They then impersonate the business and trick business partners into executing unauthorized fund transfers.
- Email: It is an electronic message which distributed via a network from a sender to one or more recipients. There are ten parts of a standard email as described in Table 1.

Table 1. Parts of a standard email

Part	Description
Header	Contains information concerning email system, sender and recipients.
Subject	A short description of the email's topic.
Date and Time Received	When the email was received.
Sender	The name of email sender which is configured by the sender.
Sender's Email Address	Sender email address is the internet mail address of the sender who send from.
Reply-To	The email address that will become the recipient of reply email.
Recipient	The name of email recipient which configured by the sender.
Recipient's Email Address	The Internet mail address of the recipient where the email was sent to.
Attachments	Files attached to the email.
Body	Contains text or html message that is the actual content

3. PHATTAPP'S OUTLOOK ADD-IN

The main function of this Outlook add-in is to detect phishing and spoofing emails. There is no better way to protect a house than to identify all the doors that provide access to the house and to make

sure that all these doors are closed, blocked, and securely guarded. The built-in logic of PhAttApp's Outlook add-in allows it to make decisions based on information collected from an email's header, subject, message and attachment. The Add-in shows its result after analyzing a email in its summary tab (Figure 1). Details of its findings are displayed in following tabs such as email information, links, trace, category. The trace tab of the Outlook add-in provides all the stops that a particular travel to and from so that users can trace back to the source of any particular email if needed. When this add-in finds a suspicious email, it warns users about the credibility of the email. It will download suspicious email's attachments into the virtual file analyzer system, where the safety of the files is further analyzed.

3.1 The psychology of phishing email attack

Psychology plays a significant role in ransomware attacks. These attacks often start with exploiting human vulnerabilities rather than technical vulnerabilities. They generally start by targeting human behavior and psychology. The targets and attack vectors are often specifically selected by the attackers. Although ransomware has evolved over time; the psychological strategy behind it remains unchanged. The attackers' success depends on their understanding of human nature and ability to anticipate how the victims will behave and react to the bait. The attacks often infect a system by luring users into clicking on a malicious link in an email or a message on social media. Although many online and offline user-training tools and courses are aimed at halting phishing attacks, many users still fall for these phishing emails and become victims of ransomware attacks. There are two main parts in an email which attackers are targeting. These parts are email's subject and email's body.

Users are often more responsive to emails with subject lines that have an authoritative tone or are related to notifications, friends, or the expression of certain interests [7]. PhAttApp offers a model using machine learning technique to differentiate suspicious emails from legitimate emails as shown in Figure 6. An email which has an authoritative tone as subject line must have its body message coordinate with the same organization. If there is any link in the body of the email which is not pointing to the same organization, then it is very possible that the email is not legitimate.

Phishing emails can be classified into two types which are spear phishing and business email phishing. Spear phishing is a sophisticated version of phishing in which attackers target an individual person. They craft a personalized message to encourage a specific target user to provide confidential information or to open malicious content. An example of spear phishing happened in January 2018. A spear phishing campaign was launched against organizations involved in the Pyeongchang Olympics. Attackers used spoofed messages from senders such as info@nctc.go.kr. This email address belongs to the National Counter-Terrorism Center in South Korea; however, the email was sent from an address in Singapore [3]. Attackers attempted to trick victims into opening a malicious document with malware embedded in it as a hypertext application file.

PhAttApp's Outlook add-in analyzes such messages and classifies the message category as depicted in Figure 4. The add-in is based on a set of predefined words and phrases to detect whether the email is suspicious and needs special attention. Phishing emails often employ tactics of appeal, fear, and urgency. Once the add-in detects a suspicious email based on its tone or wording, the add-in warns users about a possible phishing campaign and moves the email to the junk mailbox. Links are usually disabled in the junk mailbox, thus reducing the chance of a user clicking on malicious links or email attachments.

In business email phishing attacks, the attackers impersonate email accounts belonging to senior personnel and encourage target users to perform certain actions, provide confidential information, or open malicious content. The recipient, who recognizes the sender, often clicks on the infected attachment. One of the many ways to detect an authority phishing email is to validate the sender's email address against the email message. The email address must match the original sender's email, who claims to be an authorized party. PhAttApp's Outlook add-in contains the email validation feature to check for the email's domain and the sender's IP address. This add-in uses DNS and domain lookup to verify the sender's address and confirm the sender's identity. Figure 5 is an example where PhAttApp displays sender information from sender's email and sender's IP address.

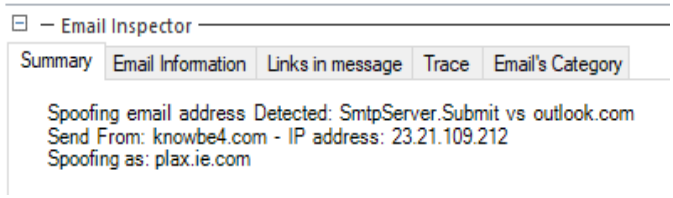

Figure 1. The figure shows summary tag of the PhattApp's Outlook Add-In

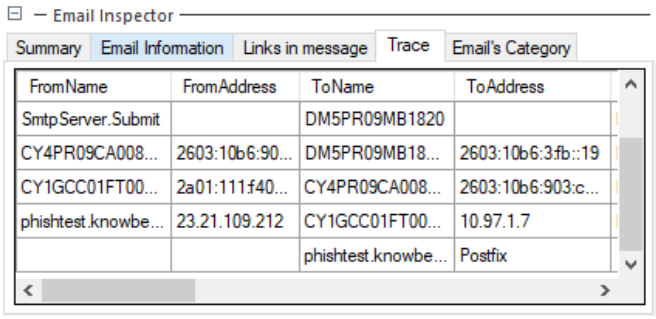

Figure 2. The figure shows the from and to IP addresses and names. This information can be use to trace back to the original source of the email.

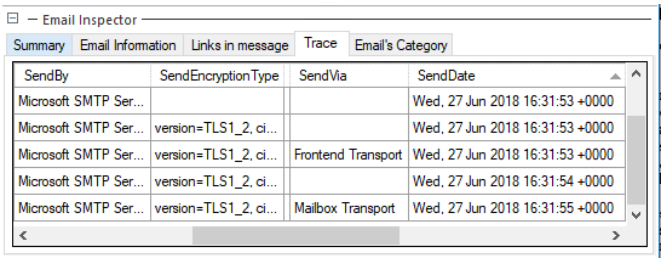

Figure 3. The figure shows the type of email encryption and the email server which were used to transfer this email. This information can use to detect suppicious email sources such as banks or authorzided

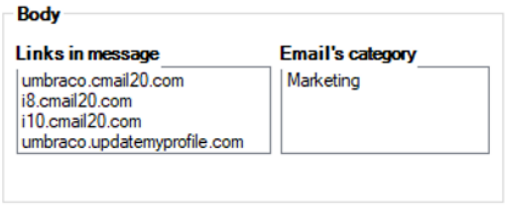

Figure 4. The figure shows the links and type of email detected from email body. The safety of the links are also inspected by the application.

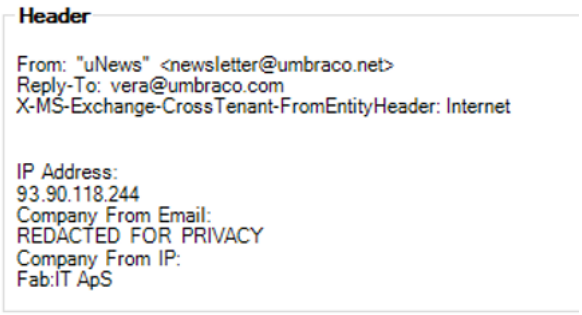

Figure 5.This figure shows the IP and domain lookup to see if they are matching and that those IP and domain are not in blacklists.

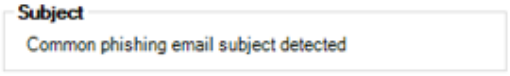

Figure 6. PhAttApp detected that email was sent from fake email address. It also displays some additional information found in email header.

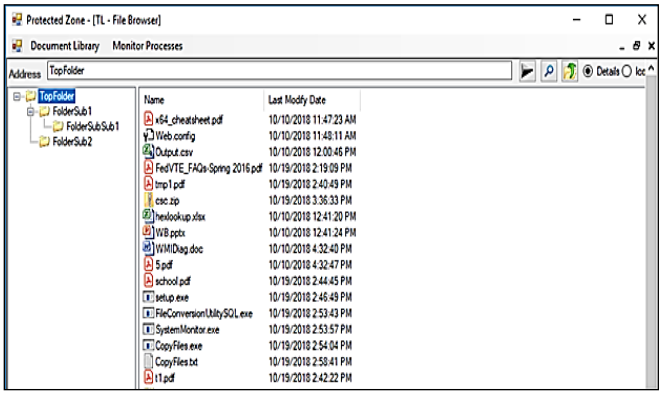

Figure 7. PhAttApp's virtual file analyzer

3.2 The techniques of phishing email attack

Attackers are always looking for more sophisticated ways to evade detection by antivirus software and by users who have received standard anti-phishing training. Homograph attacks are an example of attackers having dramatically improved the design of their phishing scams by using a secure spoofing domain that cannot be distinguished from the real one by the naked eye. This spoofing method is used by attackers to deceive computer users by exploiting the similarities between different characters. Many characters from Greek, Latin, Cyrillic, and Unicode have a similar appearance. Attackers exploit this weakness in scripts to attack users. They lure users into clicking on links where Latin characters are replaced with Greek or Cyrillic characters. Another variation of this type of attack is where attackers replace the "m" character with the "r" and "n" characters. Since "m" and "rn" look similar, attackers may deceive users about the domain to which they are connecting. Names for this type of spoofing attack are script spoofing and homograph spoofing. One of the many ways to detect this type of attack is to force the email message to display in Unicode only. In fact, PhAttApp's Outlook add-in contains a feature to analyze email messages in Unicode, which eliminates any confusion of characters.

4. PHATTAPP'S VIRTUAL FILE ANALYZER

The virtual file analyzer is a ransomware execution safe zone, where files are analyzed, controlled, and stored. A phishing email is often sent with attachments, which are the main source of malware enablement. Attackers, who look for ways to trick users into opening malicious files, rename files with a different extension or embed files inside PDF or Microsoft Office documents. The virtual file analyzer is built to detect such activities and prevent damage to systems as illustrated in Figure 7.

4.1 Files Analyzing

Security training at most organizations suggests that .exe file extensions are not safe but .txt file extensions generally are. Attackers can rename a file from its true extension to some other extension to trick users into clicking on a malicious attachment. Non-technical users cannot identify the actual file extension of the attached file. However, a file often has file headers and magic numbers stored inside it. The virtual file analyzer uses these two identifiers to identify the attached file's actual extension. The system has more than fifty predefined header bytes collected from more than fifty popular file types.

Table 2. File Analyzer detects file type base on file header information

Name	gs922w64.exe	gs922w32.exe
AddressOfEntryPoint32	12,843	12,843
BaseOfCode32	4,096	4,096
BaseOfData32	28,672	28,672
BaseRelocationTable32Size	0	0
BaseRelocationTable32 VirtualAddress	0	0
CertificateTable32Size	6,288	6,288
CertificateTable32 VirtualAddress	17,630,624	17,309,872
Characteristics	271	271
CheckSum32	17,663,208	17,342,376
DllCharacteristics32	34,112	34,112
ExportTable32Size	0	0
FileAlignment32	512	512
IAT32Size	664	664
IAT32VirtualAddress	28,672	28,672
ImageBase32	4,194,304	4,194,304
ImportTable32Size	160	160
ImportTable32 VirtualAddress	29,736	29,736

Furthermore, it has been built to operate with machine learning abilities. It can recognize a new file extension and add it to the mapping lists of known file extensions. Even if attackers rename their malicious files, the file header bytes remain unchanged as seen in Figures 8 and 9. By using the file header bytes, the true file type of any file attachment can be detected.

Results | Messages

	byteString	FileName	headerBytes	FileExtensionShouldBe	containsFiles
1	504B03041400000008...	csc.zip	504B0304	.zip	csc.exe;csc.rsp;

Figure 8. Example showing files inside the zip file

Results | Messages

	byteString	FileName	MatchHeaderBytes	FileExtensionShouldBe
1	4D5A90000300000004...	CopyFiles.txt	4D5A90000	.exe

Figure 9. Example when the file extension is not matching

4.2 Files Controlling

Some organizations must often work with email attachments from vendors, providers, customers, and others. They must accept the risk of possible infection from these email attachments. The virtual file analyzer offers a working environment where such organizations can reduce their risk of being infected by malware. The system is built based on a zero-trust network, where neither external nor internal parties are trusted. Threats are believed to exist on this virtual system at all times; therefore, all files are executed or opened with the lowest guest permission level and are monitored at every step of their execution. Two processes have been created for the execution of every file inside the system. One process opens the file using the lowest permission level. Another process runs with a high permission level and continuously monitors the other process for file creation and register key modifications. The virtual file analyzer utilizes authentication and authorization to control file execution, thus limiting the changes that ransomware can make and controlling the damage a malicious attachment can cause to a system.

4.3 Files storing

The file-storage feature of the virtual file analyzer has been built to allow users to add and organize files that are not email attachments. Users can drag and drop suspicious files that they receive through a non-email delivery method into this system and allow the virtual file analyzer to analyze and control these files.

5. CONCLUDING REMARKS

Many scientists and reports foresaw that phishing attacks would increase due to the rising popularity of Office 365. In June 2016, a variant of Cerber ransomware attacked Office 365 users. They compromise approximately 57% of organizations that use Office 365 [10]. The Checkpoint's report also concludes that they are seeing more cyber criminals are being attracted by Office 365. They are expecting Office 365 to be increasingly targeted for the coming years [1]. As pointed out in [5], between 180 million and 200 million phishing attempts were detected during the second half of 2017 targeting Office 365, making phishing the top threat vector for Office 365 in that period. With Office 365, Microsoft has taken user experience to a new level. Office 365 is offered as a service that mainly focuses on improving the productivity of organizations. It has disrupted traditional communication channels by having all its applications communicate and exchange information seamlessly. While this idea brings many benefits to users, including convenience, time savings, and more control over workflows, it also increases the risk of data leaks. Credentials are sent from Windows to the Web, and then from the Web to Windows. In comparison to Windows, the Web is much more vulnerable as it requires intervention by many third-party vendors in the form of browsers, plug-ins, cookies, and cache. The new trend of cyberattacks will target Office 365, as this is where attackers have a higher chance of obtaining credentials for future attacks. PhAttApp, powered by machine learning, is geared to identify emerging phishing threats that humans may miss. It applies psychological-analysis techniques to automatically detect malicious emails and constantly adapts its understanding as phishing threats mutate. It also responds autonomously to contain threats at the earliest sign of compromise. PhAttApp is part of a larger application that will assist users in defending against ransomware attacks.

6. REFERENCES

[1] Checkpoint. (2018). 2018 security report: Welcome to the future of cyber security. Check Point Research. San Carlos, CA: Check Point Software Technologies Limited. https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf

[2] European Union Agency for Network and Information Security (ENISA). (2018). ENISA threat landscape report 2017: 15 top cyber-threats and trends. Heraklion: ENISA. https://doi.org/10.2824/967192

[3] Hadnagy, C. (2010). Social engineering: The art of human hacking. Indianapolis, IN: John Wiley & Sons.

[4] IBM Security Services. (2014). IBM security services 2014 cyber security intelligence index: Analysis of cyber-attack and incident data from IBM's worldwide security operations (Report No. SE303058-USEN-02). Somers, NY: IBM Corporation.

[5] Tierney, S. (2018, January 8). Protect yourself against the top 3 cyber threats of 2018. Microsoft Industry Blogs – United Kingdom. https://cloudblogs.microsoft.com/industry-blog/en-gb/industry/financial-services/protect-yourself-against-the-top-3-cyber-threats-of-2018/

[6] Pauli, D. (2015, November 9). Cryptowall 4.0: Update makes world's worst ransomware worse still, now you won't even know what files are encrypted. The Register. https://www.theregister.co.uk/2015/11/09/cryptowall_40/

[7] Qi, M., & Zou, C. (2009). A study of anti-phishing strategies based on TRIZ. Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 536-538. https://doi.org/10.1109/NSWCTC.2009.154

[8] Rao, .Srinivasa, & Ali, .T (2015). PhishShield: A Desktop Application to Detect Phishing Webpages through Heuristic Approach. Eleventh International Multi-Conference on Information Processing-2015

[9] Sung A., Basnet, R.,& Mukkamala S. (2008). Detection of Phishing Attacks: A Machine Learning Approach. New Mexico Tech, New Mexico 87801, USA

[10] Toole, S. (2016, June 27). Widespread attack on Office 365 corporate users with zero-day ransomware virus. Avanan. https://www.avanan.com/resources/attack-on-office-365-corporate-users-with-zero-day-ransomware-virus

[11] Verizon. (2018). 2018 data breach investigations report (11th ed.). New York, NY: Verizon. http://www.verizonenterprise.com/DBIR2018