Minimize Phishing Attacks: Securing Spear attacks

Chaitali Parulekar

Department of MCA SEM VI, YMT College of Management, Institutional Area, Sector-4, Kharghar, Navi Mumbai, Maharashtra 410210.

Abstract:- Nowadays, there, there has been a dramatic shift from broad spam attacks which target email-based-phishing campaigns which cause significant financial and operational damage to organizations around the world. Some of the most notorious cyber crimes in recent history — such as the attacks on major banks, media companies and even security firms. There are a few different techniques used to obtain personal information from users. As technology becomes more advanced, the cybercriminals' techniques being used are also more advanced. To prevent Internet phishing, users should have knowledge of how the bad guys do this and they should also be aware of anti-phishing techniques to protect themselves from becoming victims. Phishing is oldest and simple way attacks to steal information from people. In this paper, we will be discussing how to get prevent from such attacks. We will identify the email address because in spear attacks many people get targeted from different emails as a fraud scam mailing. We will show how the security provides by this fraud mails by providing awareness against spear phishing attacks.

Keywords: Cyber Crimes, Phishing, Spear Phishing attacks.

1. Introduction:

Phishing emails are exploratory attacks in which criminals attempt to obtain victims' sensitive data, such as personally identifiable information (PII) or network access credentials.

These attacks open the door for further infiltration into any network the victim can access.

Phishing involves both social engineering and technical trickery to deceive victims into opening attached files, clicking on embedded links and revealing sensitive information. Spear phishing is more targeted.

Cyber criminals who segment their victims with spear-phishing tactics, personalize emails, impersonate specific senders and use other techniques to bypass traditional email defenses. Their goal is to trick targets into clicking a link or opening an attachment.

SPEAR PHISHING EXAMPLES AND CHARACTERISTICS :

A spear-phishing attack shows one or more following characteristics they are as follows: • Blended or multi-vector threat: Spear phishing uses a blend of email spoofing, dynamic URLs and drive-by downloads to bypass traditional defenses. • Use of vulnerabilities of zero-day: Advanced spear-phishing attacks leverage zero-day vulnerabilities in browsers, plugins and desktop applications to compromise systems. • Multi-stage attack.: The initial exploit of systems is the first stage of an APT attack that involves further stages of malware outbound communications, binary downloads and data exfiltration. • Well-crafted email forgeries: Spear phishing email threats are usually targeted to individuals, so don't bear much resemblance to the high-volume, broadcast spam that floods the Internet. This means traditional reputation and spam filters routinely miss these messages, rendering traditional email protections ineffective. Stolen information included sensitive classified intelligence data, financial records, and personally identifiable information.

The use of these kinds of information can be catastrophic, especially when it is made publicly available or sold on the black market.

Some research statistics in regard to the impact of cyber security to businesses, organizations, and individuals include:

Economic Impact of Cybercrime Estimated at $445 billion Worldwide, and between 15 percent and 20 percent of the value created by the Internet.[1]

The estimated damage it caused could exceed $1 billion, according to the report, despite only around $100,000 in bitcoins having so far been paid in ransoms to the perpetrators.[2]

The rest of the paper shows the solution which as follows.

2. SECURITY PROPERTIES

Why is phishing security design complicated? As we discuss in Section 7 and elsewhere[6], many researchers have proposed systems which are intended to prevent ransomware. Here are some features in play: 1. The human capacity is limited. People are not computers for general purposes. Their inherent abilities and technical capabilities limit them. This point is apparent but it implies which security system is designed with a new approach. Suddenly, a usable design needs to take into account what individuals do well and what they are doing, instead of just address a problem based on a traditional cryptography security framework (eg, "What can we secure?").

Browsers often warn users when using an unencrypted connection to submit form information. This warning is so common th at it is overlooked by most users, and some simply turn off the notification. 2. The property of the visuals for general purposes. Further spoofing is possible through operation systems and window platforms that allow general use of graphics. The implications of this property are important: if we build a system designed to resist phishing, we must assume that it is easy to copy uniform graphic models. As we will see in the next section, phishers use this property in establishing many types of attacks to their advantage. 3. The barn door's ownership If a secret is left unprotected, even for a short time, it cannot be guaranteed that an assailant cannot exploit it. This property encourages us to design systems that prioritize the protection of sensitive data by users before it leaves control. Although each of these properties appear self-evident in themselves, in combination they propose a series of tests for anti-phishing software. We argue that these properties need to be taken into account in order to be fully effective, anti-phishing solutions. 4. The golden arches ' property. Organizations invest heavily in reinforcing their brand recognition and evoking consumer confidence in those brands. Just as the phrase "Golden Arches" refers to a particular chain of restaurants, so are different logos used by banks, financial organisations, and other entities that store personal information. Because of massive investment in advertising to strengthen this connection, we have to make extraordinary efforts to prevent the automatic allocation of confidence on the basis of logos alone. The design of security indicators and icons also applies to this principle. For example, users often place their confidence in safety icons implicitly

3. SOLUTION

3.1 Design requirements

Our goal is to develop an authentication scheme that in the context of security features and task analysis does not impose an unfair burden on the user in terms of effort or time. We are committed in particular to minimizing user memory requirements.

- Users must recognize only one image in order to authenticate and remember a low entropy password regardless of how many servers they wish to interact.

- Our interface has the following characteristics.

- To authenticate server content, the user only needs to perform one visual matching operation to compare two images.

- It is difficult for an attacker to spoof successful authentication indicators. We also use this authentication protocol to obtain the following security qualities.

- At the end of an interaction, the server authenticates the user, and the user authenticates the server.

- The network does not send any personally identifiable information. • An attacker cannot mask as a user or a server even after a number of successful authentications has been observed.

3.2THIS TIME IT'S PERSONAL

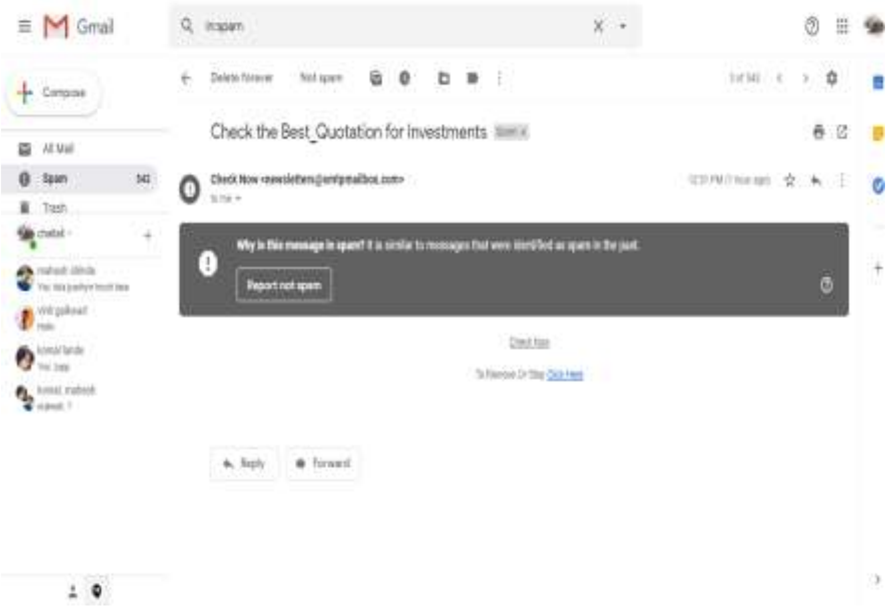
Due to the theft of PII threats from China, the company FireEye has over the past year responded to several targeted attacks. The volume of PII stolen shows that the aim is to collect PII data in large numbers, not that of specific persons.

Mandiant, however, had not seen a trend in the indiscriminate stealing of PII by threatening actors from China before. Mandy experts knew of unique PII theft instances as a by-product of larger data theft operations. Ancyber criminal could, for instance, steal any data from a PII-including file server that the attacker has no particular interest in.

That changed last month when Mandiant investigated several massive violations of PII that threat actors operating in China thought to orchestrate. These violations covered several sectors, including health care, travel, finance and government. Initial suspicion was made by Mandiant that the threat players would target health records and credit card information.

Instead, the client observed threats targeting and stealing data which might be used to verify identities such as social security numbers, names of mothers ' maiden, date of birth, employment history and questions and answers.

3.4 Real Live Example:



Check the Best_Quotation for Investments

Check Now <newsletters@emfpmailbox.com>

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Phishing e-mails are exploratory attacks where criminals attempt to obtain sensitive data for victims, such as PII or access to a network. These attacks open the door of any network the victim could access for further infiltration. Typically Phishing involves social and technical engineering to mislead victims into opening attached files, clicking on integrated links and revealing sensitive information.

Spear is more focused on phishing. Web criminals using spear-phishing tactics segment their victims, customize e-mails, personalize specific senders and use other methods to circumvent traditional email defenses. Their purpose is to click on a link or to open a file. An email addresses may be included in a Phishing campaign, but spear phishing focuses on individuals with a certain mission within specific organisations. By exploiting social networks for personal data on targets, an attacker can write highly accurate and compelling emails.

Once the target clicks on a link or opens a link, the attacker sets the network footprint and completes its unlawful task.

Spear phishing is the most common method of delivery for APT attacks. Cyber criminals and governments today launch APT attacks with sophisticated malware and ongoing, multi-vector and multi-phase campaigns to achieve a particular goal, gaining long-term access to the delicate networks, information and assets of the organization.

How a China-based attacker stole a huge number of PII One assaults has begun with threat actors successfully enticing a worker to use a spear-phishing email to click a malicious link. A backdoor has been downloaded and the attackers have access to the environment of the victim. Once the recognition activity was founded, the main focus was on identification of PII databases with the highest volume.

3.5 BETTER EMAIL SECURITY

Organizations are now in need of an innovative email security solution that detects and blocks automatically advanced targeted campaigns, including spear phishing, collection of credentials or rejection of legitimate senders. FireEye Email Security provides a solution for the protection of e-mail-based cybercrime organizations that is more effective than standard solutions.

Cohesive, integrated solution across threatening vectors Organizations need protection across multiple vectors to be effective in fighting today's cybercrimes. For example, in advanced attacks, email and network vectors are often used together. When a web attack is found in real time, businesses can determine whether there are others in the organization that are being targeted by the attack. The attack is being traced in the original phishing email.

By utilizing the Active Directory information of the victim to identify database administrators and their computers, the attackers were able to access their databases. The threats actors later moved to the systems and collected documents in order to identify database names, database servers and data base credentials. They searched the Active Directory Group Membership for the database keyword.

The attackers showed a strong understanding of Microsoft, Teradata and Oracle database systems and the transaction gateways for accessing them. The threat actors tested authentication and inventoried databases systematically with the database information in hand. They then searched for column names which indicated the stored sensitive information, such as' Social Security Numbers,' and extracted specific fields for each record in the targeted databases once they had found that information of concern. Social security figures, maiden names of mothers, and birth dates were included in the information.

The actors of threat are:

1. Because of the volume of information extracted. Chunks of extracted data (100,000 to 1,000,000 records per day).

2. The information was compressed into split files.

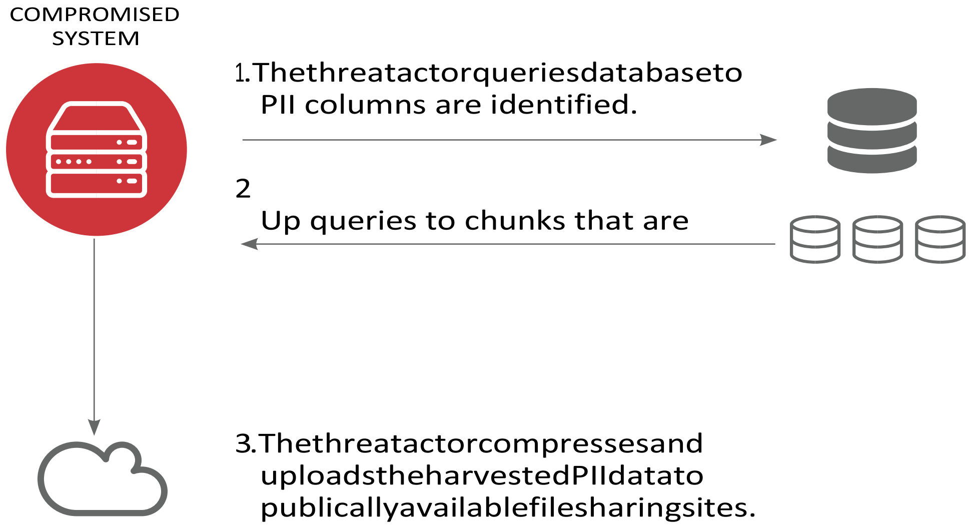

COMPROMISED SYSTEM
1.Thethreatactorqueriesdatabaseto PII columns are identified.
2
Up queries to chunks that are
3.Thethreatactorcompressesand uploadstheharvestedPIIdatato publicallyavailablefilesharingsites.

fig.2 [3]

3. Compressed files with PII have been uploaded to sites of file sharing.

BETTER EMAIL SECURITY

Today, organizations need the innovative solution to detect and block automated advanced, targeted campaigns involving spear phishing, credentials or legit senders ' impersonation. FireEye Email Security provides a more effective email security solution than standard solutions and proactively protects email-based cyber crime organizations.

In order to be effective in combating current cyber criminals, organisations need protection across several vectors. Cohesive, integrated solution across menace vectors For example, in advanced attacks email and network vectors are often used. If a web attack is discovered in real time, companies can determine whether other organizations have also been targeted and track the attack on the

DETECT AND STOP SPEAR PHISHING

Targeted multi-stage multi-vector attacks have been very efficient in penetrating today's networks despite a $20 billion annual investment in IT safety. Most attacks come with an email which is malicious. In specific, socially built messages are the arma of choice since they are effective, such as spear phishing. It is used by criminals if organizations are secure and unable to detect them. To stop advanced targeted attacks, organizations need comprehensive protection toward attacks that protect multiple vectors of threat and address every stage of an attack.

CONCLUSION:

It can be concluded that spear phishing attacks are a specific type of phishing attack. A typical spear attack covers an e-mail and an attachment. The email includes information specific to the end user and a link to the user is genuine. The message design is undertaken to attract the user to perform the desired tasks. Many of these types of attacks involve problems and risks to security. Organizations then need to take appropriate protection measures to mitigate the impact of these attacks. Implementing appropriate security measures will reduce these attacks' likelihood.

References

1. T. Rimo and M. Walth, “McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies”, McAfee, June 9, 2014.

2. A. Cuthbertson. Ransomware attacks have risen 250 percent in 2017, hitting the U.S. hardest. 2017, May 28. Retrieved: September 21, 2018, from http://www.newsweek.com/ransomware-attacks-rise-2502017-us-wannacry-614034.

3. wp-fireeye-how to stop spearfishing attack pdf.