A Review of Various Phishing Attacks & Anti-phishing Techniques

Eze, B. E & Olaiya, O.O.
Department of Computer Engineering
The Federal Polytechnic Ilaro,
Ogun State, Nigeria.
ebereblessing247@gmail.com, yinkakol@gmail.com

ABSTRACT

Phishing is a form of identity theft in which deception is used to trick a user into revealing confidential information with economic value. In recent years, phishing attacks have increased exponentially, targeting every sector of society. Phishing is a significant problem involving fraudulent email and web sites that trick unsuspecting users into revealing private information. Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords. The number of phishing scams is continuously growing, and the cost of the resulting damage is increasing. Among various kind of attack, one of attack is phishing. It is a kind of network attack which theft the identity of user's online and steals some useful information such as password or ATM and financial information. We analyze some of the previously work done to prevent network from phishing attack is described with their merits and demerits and identify that most of them exploit the fact that users are not sufficiently aware of the secure site identification mechanisms in browsers.

Keywords: Phishing, fraud, detection, E-mail, Security

CISDI Journal Reference Format
Eze, B. E & Olaiya, O.O.. (2016): A Review of Various Phishing Attacks & Anti-phishing Techniques.
Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 7 No 4. Pp 159-164
Available online at www.cisdijournal.net

1. INRODUCTION

The term phishing was first used in the Internet literature in 1996 by the hacker group who stole America Online (AOL) accounts' credentials. Phishing is originated from Phreaking which is considered as the science of breaking into phone networks using social engineering. A phishing attack is also based on the concept of social engineering in which users are tricked to open malicious attachments or embedded links in the e-mails [1]. Phishing is the combination of social engineering and technical exploits designed to convince a victim to provide personal information, usually for monetary gains to the attacker (Phisher). Phishing scams can happen when malicious organizations or people (also known as cybercriminals) present themselves as an entity users can trust, then try to trick them into providing personal information. Phishing scams normally occur via emails, websites, text messages and phone calls that can delude recipients' to think that Christmas came early.[3][4]

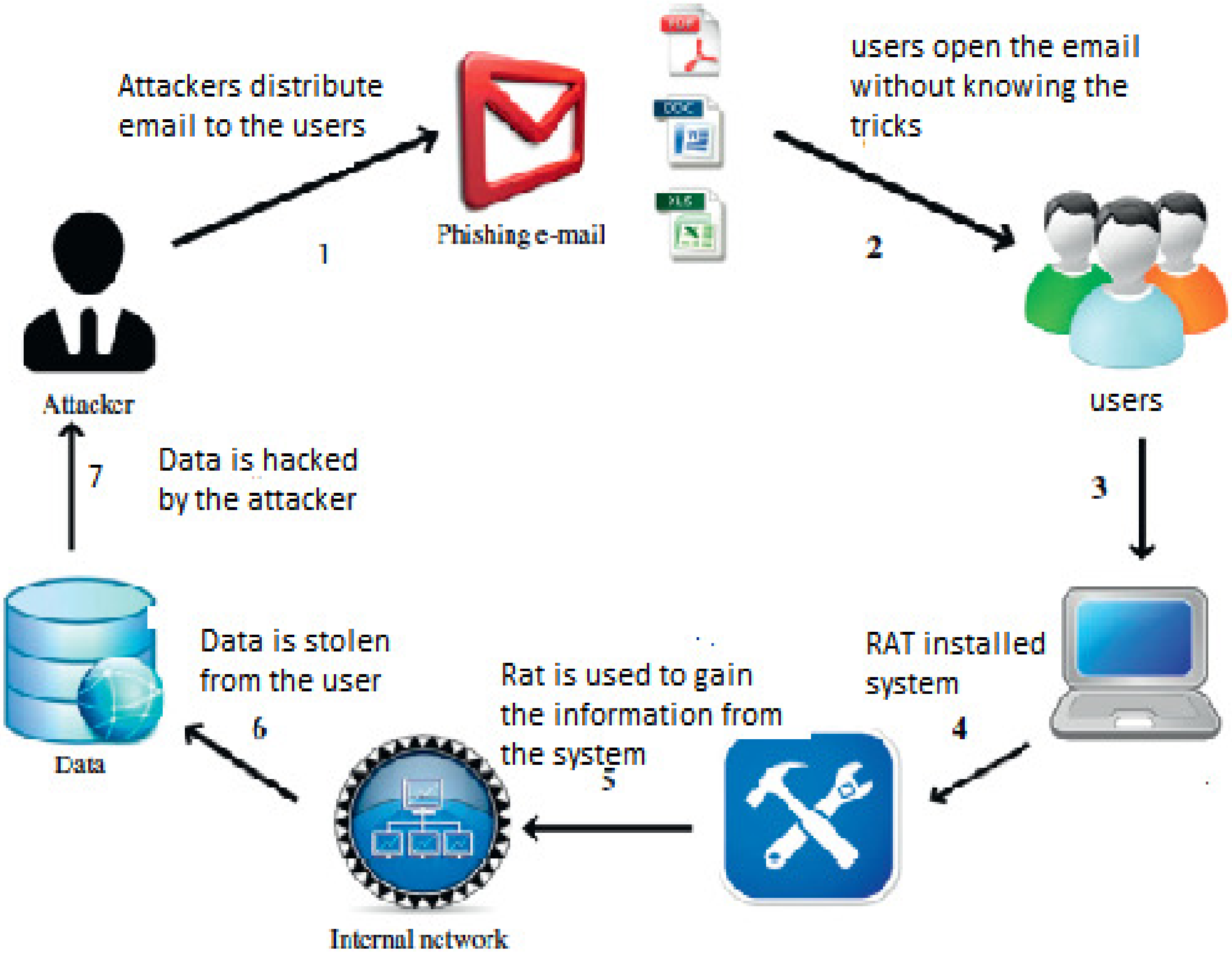
Cybercriminals will often pose as your bank or financial institution, your employer, or any other entity that you normally trust with your information. Only when the email phishing process and characteristics are fully understood can effective measures be designed against phishing attacks. Successful phishing attacks are based on a form of copying, or reengineering, a website's design and layout in order to pass themselves off as a genuine (targeted) website. A malicious website is crafted which looks and feels like the original site, convincing unsuspecting users that they are giving personal information to a trusted organization [2]. Users are frequently drawn to the sites by forged emails designed to look like legitimate correspondence and may even copy the body from real email, but when the user clicks a link to visit the website, they will be directed to the malicious site instead [5][6][8]. The more convincing a phishing attack appears - or rather, the more genuine a malicious website looks - the more success the attack will have in extracting personal information. Some phishing attacks go so far as to create faux websites for which there is no legitimate counterpart; e.g. a page prompting users for personal information the organization wouldn't have otherwise asked for. [9][8]

According to Anti-Phishing Working Group (APWG), phishing activities have been increasing and most phishing websites are hosted in the US. In 2012, an average of over 25,000 unique phishing email reports were reported to the APWG. Plus, the number of unique phishing sites detected exceeded 45,000 per month [3]. With due to rapid increase in the use of internet technology for communication different kind of attacks can be possible on the network such as DOS (denial of service attack), masquerade, replay and phishing etc. It is one of the most serious attacks which steals our personal information or hack the website. [10][11]

The word 'Phishing' originally emerged in 1990s. The early hackers frequently use 'ph' to reinstate 'f' to fabricate new words in the hacker's community, as they typically hack by phones. Phishing is a novel word produced from 'fishing', it refers to the act that the attacker fascinates users to visit a counterfeits website by sending them counterfeit e-mails (or instant messages), and stealthily get victim's personal information such as user name, password, and national security ID, etc. [12][13]

This information then can be used for future target advertisements or even identity theft attacks (e.g., transfer money from victims' bank account). The recurrently used attack process is to send e-mails to prospective victims, which appeared to be sent by banks, online organizations, or ISPs. In these e-mails, they will make up several reasons, e.g. the password of your credit card had been mis-entered for several times, or they are offering upgrading services, to allure you visit their Website to conform or amend your account Number and password through the hyperlink made available in the e-mail [4].[14]

1.1 Steps in Phishing Attack



2. TYPES OF PHISHING ATTACKS

In this section, we give a brief description about the different types of phishing attacks

2. 1 Fruit Sucker

When another attacker breaks into a hacked, vulnerable website with an existing phishing page and changes the email address. Often since the attacker can see where the data is being emailed to he/she will keep the original email addresses intact and merely add his/her own email address in the BCC field. This is a very easy way for an attacker to make extra money. All passwords and account numbers keyed in reach his inbox directly without tipping off the original phishers. If the phishers are rookies and lack automated money transferring scripts, are too lazy to keep a watchful eye on their victims or are situated in a different time zone, then these advantages can help the fruit sucker withdraw a large amount of data (or other assets) from the compromised accounts before they do [6].

2.2 Spear Sucker

An attack against the original crackers. For example, a good guy who breaks into the phishing websites and changes the email address to the NEDBANK's CSO's or CEO's email address. After this he contacts the bank to make them aware of the security breach [6].

2.3 Haxtortionist

When an attacker patches the system, pulls down the phishing page and emails the attackers threatening them that he/she will report the crime and inform NEDBANK of their malicious activity. Reporting such abuse to email servers hosted by Google, Yahoo and similarly large companies in the United States is easy. In this way the attacker may extort a small share of money from the original crackers in return for keeping silent [6].

2.4 Robin-HAT

Here the attacker, after collecting a lot of passwords, changes the recipient's email address for the purpose of redistributing wealth. He/She withdraws money from the accounts and donates a significant portion to charity. Such individuals cannot be called grey hats because they are criminals robbing from other criminals. They are Robin-HATS, those who steal from rich victims and their attackers and redistribute the wealth to the poor and needy [6].

2.5 Server-side exploits

Any discussion of the exploitation of server-side vulnerabilities to assist in a phishing attack quickly transcends phishing and enters the realm of general hacking and cracking; Suffice to say there are numerous techniques for exploiting operating systems, applications and network protocols that a phisher could use if they were determined to comprise a legitimate website in order to conduct a phishing attack. However, two 'non-invasive' techniques of relevance to phishers will be discussed: cross site scripting and preset sessions

- Cross site scripting (CSS or XSS) seeks to inject custom URLs or code into a web-based application data field, and takes advantage of poorly developed systems. Three techniques are typically used
- HTML substitution:http://www.citibank.com/ebanking?URL=fakesite.com/login.htm
  In this example, the standard legitimate website content is rendered, but the web application uses a parameter to identify where to load specific page content (for example the login box); in this case, that content is fetched from fakesite.com (whose URL could be obfuscated using previously described techniques).
- Forced loading of external scripts:
  http://www.citibank.com/ebanking?page=1&response=fakesite.com%21secretScript.js&go=2
  In this example, a script to be executed is passed to the web application.
- Inline embedding of active content:
  http://www.citibank.com/ebanking?page=1&client=<SCRIPT>... </SCRIPT>
  In this example, the script is placed in the URL and executed by the web application.
  Preset sessions use session identifiers. Session identifiers are typically used in HTTP and HTTPS transactions as a mechanism for tracking users through the website and to manage access to restricted resources (i.e. manage state). Session IDs can be implemented in a variety of ways; for example, cookies, hidden HTML fields or URL parameters. Most web applications allow the client to define the session ID. This allows the phisher to embed a session ID within the URL (that refers to the legitimate server) sent as part of the initial email.
  For example, https://mybank.com/ebanking?session=3V1L5e5510N
  Once the email is sent, the phisher polls the legitimate server with the predefined session ID; once the user authenticates against the given session ID, the phisher will have access to all restricted content [6] [7].

2.6 Client-side vulnerabilities

Any discussion of client-side vulnerabilities is similar to that of its server-side counterpart: there are a multitude of vulnerabilities that a smart phisher could take advantage of in order to execute arbitrary code or to manipulate the browser. Given their exposure to the internet, it is not surprising browsers suffer from a significant number of security vulnerabilities.

Most browsers also support a number of plug-ins, each of which carries its own security risks. While patches are typically available in a timely manner, home users are notoriously poor at applying them quickly; therefore, phishers have ample time to exploit most security vulnerabilities, if they choose to do so.

Some past exploits used by phishers include

- Microsoft Internet Explorer URL mishandling: a URL such as:
  The real URL : http://www.citibank.com%01@fakesite.com/phisher.html
  What the User sees: http://www.citibank.com
  Where the browser goes: http://fakesite.com/fakepage.html
  By inserting a %01 string in the username portion of the URL, the location bar displays http://www.citibank.com , while redirecting the user to fakesite.com. Earthlink, Citibank and PayPal were all targeted using this particular flaw.
- Microsoft Internet Explorer and Windows Media Player combination: this vulnerability allowed the execution of a Java JAR archive, disguised as a Windows Media Player skin, which could access local files.
- RealPlayer heap corruption: RealPlayer is available as a plug-in for most browsers, and allows the user to view the proprietary RealMedia format. By creating a malformed RealMedia file, and embedding it in a website to ensure it is automatically played, it is possible to cause a heap corruption, which would allow the execution of arbitrary code.

While malware can often be eliminated with a regularly updated antivirus utility, browser (or any client-side) exploits cannot be defended against until a patch is available and applied [7].

2.7 Malware-Based Phishing

This refers to scams that involve running malicious software on users' PCs. Malware can be as an email attachment, as a downloadable file from a web site for a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.

2.8 Key loggers and Screen loggers

This type of malware tracks the input from the keyboard and the relevant information will be send to the hackers through internet. They go into the users' browsers as a small program and run automatically when the browser is started as well as into system files as device drivers or screen monitors.

2.9 Session Hijacking

This deals with monitoring the activities of the users until they sign in to the account or transaction and create their important information. At that point the infected software will perform unauthorized actions, such as transferring funds, without the user's knowledge.

3. ANALYSIS OF VARIOUS ANTI PHISHING TECHNIQUES

Anti-phishing refers to the method employed in order to detect and prevent phishing attacks. Anti-phishing protects users from phishing. A lot of work has been done on anti-phishing devising various anti-phishing techniques. Some techniques works on emails, some works on attributes of web sites and some on URL of the websites. Many of these techniques focus on enabling clients to recognize & filter various types of phishing attacks. Phishing is a criminal activity that acquires sensitive information about the organization or any individual like the usernames, passwords and details of credit cards. In order to prevent the phishing activity, various techniques can be adopted. Various legislation and technology can be adopted to protect phishing activities.

Gaurav, Madhuresh Mishra, Anurag Jain conclude that most of the anti-phishing techniques focus on contents of web age, URL and email. Character based anti-phishing approach may result in false positive but content based approach never results in false positive. Attribute based approach consider almost all major areas vulnerable to phishing so it can be best anti-phishing approach that can detect known as well as unknown phishing attack. Identity based anti-phishing approach may fails if phisher gets physical access to client's computer [15].

Yue Zhang et al presented the design and evaluation of CANTINA, a novel content-based approach for detecting phishing web sites. CANTINA takes Robust Hyperlinks, an idea for overcoming page not found problems using the well-known Term Frequency / Inverse Document Frequency (TF-IDF) algorithm, and applies it to anti-phishing. We described our implementation of CANTINA, and discussed some simple heuristics that can be applied to reduce false positives. We also presented an evaluation of CANTINA, showing that the pure TF-IDF approach can catch about 97% phishing sites with about 6% false positives, and after combining some simple heuristics we are able to catch about 90% of phishing sites with only 1% false positives [7].

Rani S. K D. Kavitha M. E.presented the work which is based on anti-phishing technique against mobile phishing attack. In this technique, web-to-native phishing attack is developed on iOS mobile platform. The real demonstration of the developed web based attack proved that it has the capability of easily fakes the real apps in iOS. The defense implementation against this web based attack uses keyloggers, alert system and policy whitelist. This defense implementation is effective on iOS built-in keyboard. The major drawback is if any system uses its own implementation of keyboard. The proposed system is ineffective [5].

4. CONCLUDING REMARKS

Organizations have to exercise a constant degree of caution by using tools to alert organizations to suspicious emails, regularly training employees and having logical, robust processes in place. In addition, companies should leverage a cyber cohesive security solution that enables them to detect phishing emails before the messages are delivered to employees. With the right approach, enterprises can prevent their operation from being victims of carefully engineered and targeted attacks. As with all cyber and digital security, a multi layered approach is critical to prevention. Organizations have to exercise a constant degree of caution by using tools to alert organizations to suspicious emails, regularly training employees and having logical, robust processes in place. In addition, companies should leverage a cyber cohesive security solution that enables them to detect phishing emails before the messages are delivered to employees.

With the right approach, enterprises can prevent their operation from being victims of carefully engineered and targeted attacks. As with all cyber and digital security, a multi layered approach is critical to prevention. Once again the key to protecting your organization is educating your staff to be vigilant as well as install proper software to add a digital layer of security to your organization.

REFERENCES

1. Targeted Cyber Attacks. Available at: http://searchsecurity.techtarget.com/feature/Targeted-Cyber-Attacks
2. Approaches to Phishing Identification Using Match and Probabilistic Digital Fingerprint Techniques. Available at: http://www.mcafee.com/us/resources/white-papers/wp- approaches-to-phishing identification.pdf
3. Phishing Attacks and How To Prevent From Being Hooked. Available at: http://www.hongkiat.com/blog/phishing-reports-prevention
4. A Review on Phishing Attacks and Various Anti Phishing Techniques Available at: http://www.ijcaonline.org/research/volume139/number1/suganya-2016-ijca-909084.pdf
5. A Study Of Major Phishing Targets And Their Anti-Phishing Solutions. Available at http://www.ijtra.com/view/a-study-of-major-phishing-targets-and-their-anti-phishing-solutions.pdf
6. Detection Of E-Banking Phishing Websites. Available At http://www.ijmer.com/papers/vol2_issue1/I021046054.pdf
7. CANTINA: A Content-Based Approach to Detecting Phishing Web Sites. Available at http://www2007.org/papers/paper557.pdf
8. Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm Available at http://www.iosrjournals.org/iosr-jce/papers/Vol14-issue3/E01432836.pdf?id=7177
9. A Review on Phishing Attacks and Various Anti Phishing Techniques. Available at: http://www.ijcaonline.org/research/volume139/number1/suganya-2016-ijca-909084.pdf
10. A Review of Various Techniques for Detection and Prevention for Phishing Attack. Available at: http://ijact.org/volume4issue3/IJ0430037.pdf
11. Spear Phishing Explained. Available at: http://senvira.com/spear-phishing-explained
12. Targeted Cyber Attacks. Available at http://searchsecurity.techtarget.com/feature/Targeted-Cyber-Attacks
13. Phishing Activity Trends Report. Available at http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf
14. Apt Group Sends Spear Phishing Emails To Indian Government Officials. Available at https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html
15. Anti-Phishing Techniques: A Review. Available at http://www.ijera.com/papers/Vol2_issue2/BG22350355.pdf