ISSN No:-2456-2165

Phishing Attacks: Identification and Prevention

[1]Abdullah Alnaim, [2]Salem Alturky

Abstract:- Phishing is a major source of insecurity within the internet. This is a kind of fraud in which an individual or a group of individuals aim to get access to valuable data and personal information of an internet user without consent. In this respect, it is extremely necessary to institute detection and preventive measures to protect internet users. This study will describe phishing, address the development of tools and their application in the fight against phishing, explore the provision of education for the detection of phishing with information sourced from past studies in this field and consider possible solutions to the problems related to phishing.

Keywords:- *Phishing, Anti-Phishing, Forensic tools, Hacking, Uniform Resource Locator (URL), Malware, Linkguard.*

I. INTRODUCTION

Phishing is a fraudulent attempt to obtain personal or private information from people or organizations through internet deception methods. The practice is illegal and ranks among other internet crimes such as cyber-crime and hacking [3]. Owing to the negative implications of phishing, this research paper explores the various methods of detection and prevention available for internet users. It seeks to provide information on anti-phishing sites that could help detect and alert users on suspected malicious websites and false emails [5]. Forensic methods of phishing detection and prevention such as computer forensics, network systems, and database forensics among others will be evaluated for efficacy in anti-phishing. In addition, the paper gives some meaningful statistics on the prevalence of phishing practices in the past few years. The concluding remarks address the gravity of the issues in question and possible steps necessary to curb the crime.

II. ATTACKS

A simple definition of Phishing is "he acts of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication." [http://en.wikipedia.org/wiki/Phishing]. Criminals undertaking phishing impersonate real entities and proceed to obtain information by request or malicious coercion from users [4]. Phishing attacks are likely to be successful when one receives a request for information from a person impersonating a friend or other known entity. The five percent of users respond to phishing requests, and a further two million users expose sensitive personal information [1]. Users who gave information to spoofed websites cost banks and financial service providers millions of dollars in losses directly attributable to phishing activities [3].

The significance of phishing is a concern because of the increase in connectivity and access to the internet. Cybercrime is one of the factors preventing the growth of electronic commerce. According to Mohammad and Goudar, the worst hit industries are financial services and health care service providers. The concern banks raise is valid; in a period of two years spanning 2005 to 2007, the top priority among internet risks was viruses and malware. From 2007 onwards, the issue of greatest concern was phishing [3]. In 2016, there were at least 255,065 phishing attacks worldwide in the sense of malicious sites and the average 'uptime', or time the attacks lasted, was nearly 72 hours, which is highly detrimental to business and can have long-lasting and wide-reaching effects [1].

Phishing Statistics	Year 2014	Year 2015	Year 2016
Attacks	247,713	227,471	255,065
Phishing Domain Names	183,222	160,155	195,475
Maliciously Registered Domains	49,932	34,102	95,424

Table 1: Phishing Statistics [1]

The above table shows that phishing attacks increased from 2014 to the end of 2016. It is predictable from the above table that next years may record a massive increase in number of targets from the previous years. This was also the case in the number of phishing domain names recorded in the past three years.

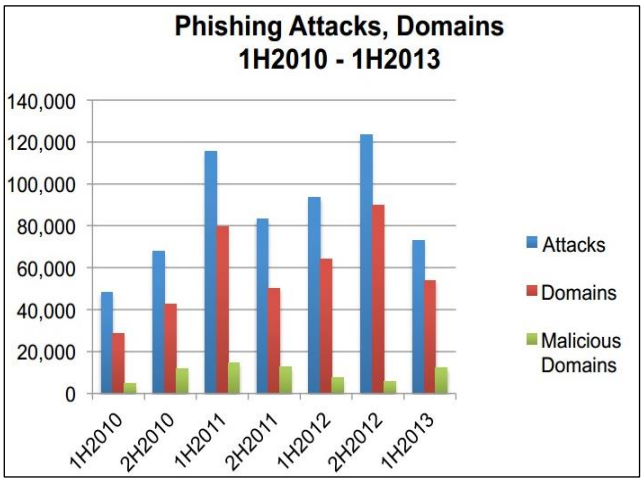

Fig 1: Phishing Attacks, Domains, and Malicious Domains [1]

Figure 1 shows the trend in attacks, maliciously registered phishing domains and phishing domain names, and it shows the number of attacks from 2012 to 2016.

III. IDENTIFICATION

Visual deception is the most common method of phishing on the internet. When one uses a malicious email attachment, it normally contains a link that imitates a real website. The close resemblance to the real website tricks the user into thinking that it is a legitimate site. This gives the innocent user the confidence to submit personal information [3]. The research of Putra and Mallikka (2012), shows that the most effective method works by scaring users into believing that failure to submit the information required would have undesirable consequences. Phishers require users' login details, and often state that a failure to supply them would permanently disable login.

Phishers need to hide from the public eye to be successful. However, phishers also need convincing contact with users in order to carry out attacks. In daily browsing, the simplest method that phishers use is malware downloads. Phishers exploit weaknesses in browsers and deliver malware by this method. Phish Guru is a method of detection that proves to be effective in preventing phishing attacks. To use Phish Guru, one creates a phishing website and then utilises it to train users. When a user falls for the phish, the Phish Guru provides a message that the user is at risk for phishing attacks. The Phish Guru then gives tips to the user to avoid falling for a phishing attack [4].

According to Putra and Mallikka (2012), analysing HTML code on a webpage is one of the most effective tools used by antivirus software to combat phishing. Unfortunately, phishers turned to using images and java applets that are hard to detect. A new anti-phishing method called Linkguard seems to be effective. In this method, the tool analyses the generic attributes of links in attacks. Analyzing the data archive provided by the anti-phishing working group gives the attributes of phishing sites. This tool is effective because it can detect phishing from known as well as unknown sources [4].

IV. PREVENTION USING DIGITAL FORENSIC TOOLS

Digital Forensic Tools are tools used for deriving, preserving, collecting and validating identification, analysis, documentation, interpretation and presentation of digital criminal evidence [2]. These tools are also useful in facilitating the reconstruction of evidence of criminal activity and events while also helping to anticipate unauthorized actions intended to disrupt planned operations [5]. According to Mohammad and Goudar (2013), digital forensic tools are one of the most effective weapons "internet police" can use against phishers and can be used to collect information from a wide array of devices such as CD, DVD, hard drives, flash drives, memory cards and mobile phones. According to Mohammad and Goudar (2013), digital forensic tools can be categorized by the branches of digital forensics to which they belong:

- **Computer Forensics:** "Computer forensics is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media." [http://en.wikipedia.org/wiki/Computer_forensics].
- **Memory Forensics:** "Memory forensics is forensic analysis of a computer's memory dump." [http://en.wikipedia.org/wiki/Memory_forensics].
- **Network Forensics:** "Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection." [http://en.wikipedia.org/wiki/Network_forensics].
- **Mobile Phone Forensics:** "Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions." [http://en.wikipedia.org/wiki /Mobile_ device_forensics].
- **Database Forensics:** "Database Forensics is a branch of digital forensic science relating to the forensic study of databases and their related metadata." [http:// en.wikipedia.org/wiki/Database_forensics].

A. Computer Forensic Tools

Computer forensics is a form of data analysis and examination that is held or retrieved from computer storage media. Information collection should happen in such a way that it is intact and usable as criminal evidence [2]. Computer forensics tools include commercial tools such as FTKImager, X-way and Intella among others. There are also free computer forensic tools such as Helix, Sleuth Kit, Digital Forensic Framework and Open Computer Forensics Architecture (OCFA).

According to Mohammad and Goudar (2013), FTKImager creates a forensic image of a hard disk to ensure that the write-blocking device is in use. Its applications include imaging processes on a Windows platform and is available at [http://accessdata .com/support/product-downloads /ftkdownload-page]. Another tool is X-Way Forensics, which creates a table with full details of the drive formats and media types. It is applicable in free space capturing, slack space and text. It uses the Windows platform and it is available at [http://www.x-ways.net/winhex/ forensics.html] [5].

B. Memory Forensics Tools

Memory forensics collects persistent data, which is usually found on a medium that preserves it when a computer is shut off [5]. Some commercially-available tools include Memoryze, Windows SCOPE and Second Look, while CMAT, Volatility and Volafox are free. Memoryze helps find bugs in live memory and acquire memory images using incident responders. It analyses memory images on live systems and is available on the Windows platform. It is available at [mandiant.com] [5]. Another tool is Windows SCOPE which performs functions such as memory forensics, reverse engineering, computer forensics, and other cyber defence activities. It has network live memory forensics, archiving and incidence response capabilities. It runs on the

Windows platform and is available at [windowsscope.com] [5].

C. Network Forensics Tools

Network forensics is the analysis and monitoring of data activities on a network to gather information on intrusion events or as legal evidence [5]. Examples of tools used in network forensics include TCPDump, Ngrep, WinDump, Airmon-ng, Aireplay-ng, Xplico, Fenris, Honeyd and Flow Tools. For example, WinDump is a network forensic tool that analyses a command line network. It watches, diagnoses and saves the network traffic to disk. It runs on the Windows platform and is available at [winpcap.org/ windump] [5]. TCPdump is also a network forensic tool that can provide privileges on a network device. It displays the TCP/IP and any transmitted packets over the network. It uses the Linux platform and is accessible at [tcpdump.org] [5].

D. Mobile Phone Forensics Tools

Mobile phone forensics tools are tools used to examine SIM cards and handsets, such as PDAs, iPhones or BlackBerrys for information or data presence. Some examples of tools include Radio Tactics, Micro Systemation XRY/XACT, Aceso and Oxygen Forensic Suite [4]. Free tools include NetSleuth, Bitpim and DECAF. Micro Systemation XRY/XACT allows data to be extracted from various mobile devices and is compatible with a wide variety of device operating systems. It runs on the Windows platform and is available at [msab.com] [5]. Another tool is Oxygen Forensic Suite, which uses an extended log for the recording of calls, MMS and email attachments on devices supporting these features. It is compatible with Symbian OS, Apple iPhone, Windows and Android smartphones. It is a Windows application and is available at [oxygen-forensic.com/en] [5].

E. Database Forensics Tools

Database forensics tools are for the analysis, preservation and authentication of data produced by databases [5]. According to Mohammad and Goudar (2013), examples of tools include IDEA, ACL Audit Exchange, Arbutus and SQLite Forensic Reporter. The IDEA forensic tool reads, displays, analyses and manipulates data from different sources, such as a PC, records all file and database exchanges and trails the audit and operations log and imports. It is a Windows application and is available at [caseware.com] [5]. Another database forensic tool is ACL Audit Exchange, which overcomes data access, security and coverage challenges in data. It provides automated data access capabilities in a secure environment. The tool visualizes results on an AX dashboard for audit exchange. It is also a Windows application and is available at [acl.com] [5].

V. PHISHING AND MALWARE DETECTION FOR GOOGLE CHROME

The default setting for Google Chrome enables phishing and malware protection. However, the user can change the settings using the following steps shown in the screenshots below:

From the 'customize and control' button on the right top corner, select settings:

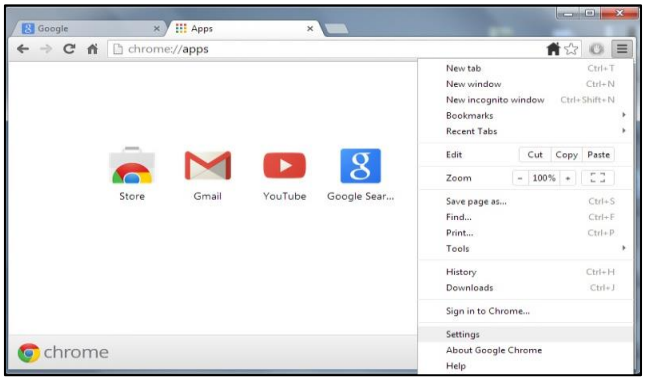

Fig 2: Google Chrome home page

The settings tab appears and provides the privacy settings, which allows the user to enable phishing and malware protection:

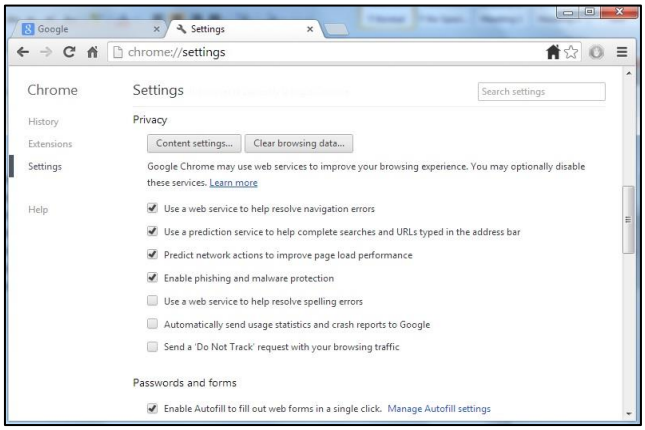

Fig 3: Google Chrome anti-phishing settings

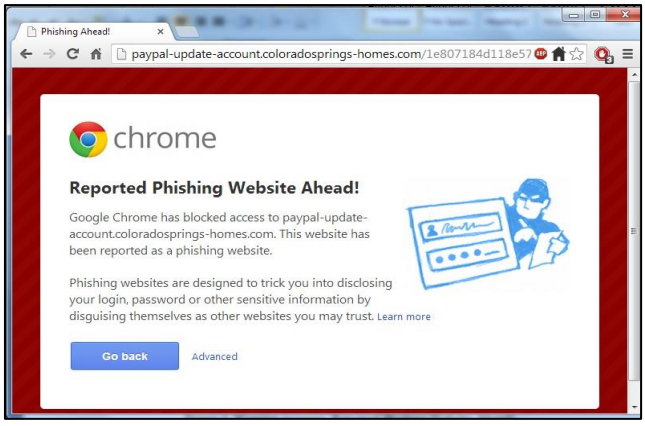

Fig 4: Warning message: Reported Phishing Website Ahead!

VI. CONCLUSION

While some people go phishing for fun and others for profit, the practice has negative implications on internet usage including loss of money and loss of information to the wrong people. This information could thereafter be used to cause malicious damage in various sectors of society. Therefore, stringent measures are necessary to secure internet users from

giving personal and private information to malicious persons. Internet users could employ various countermeasures to detect and prevent malicious retrieval or access to important information from databases and digital internet-enabled devices [4]. Sites such as PhishTank help in detecting and alerting users to malicious internet links that could be used to trick them into giving information to people with bad intentions. However, these sites may not protect databases and other internet access points and therefore professional detection and prevention is important. Use of forensic tools such as computer forensics and mobile phone forensics among others would ensure that the systems are well protected and safe. Future research on anti-phishing methods would help strengthen detection of and protection from malicious web links and emails.

REFERENCES

[1]. Aaron, G. & Rasmussen, R. (2017) Global Phishing Survey: Trends and Domain Name Use. Retrieved from https://docs.apwg.org/reports/APWG_Global. Phishing_Report_2015-2016.pdf

[2]. Alharbi, S., Traore, I., & Weber-Jahnke, J. (2011). The proactive and reactive digital forensics investigation process: A systematic literature review. *International Journal of Security and Its Applications, Volume (5)*, 59-72. Retrieved from http://www.sersc.org/journals/IJSIA/vol5_no4_2011/6. pdf

[3]. Danuvasin, C. (2011). Phishing: A field experiment. *International Journal of Computer Science and Security (IJCSS), Volume (5)*, 277-286. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi =10.1.1.227.6497&rep =rep1&type=pdf

[4]. Mallikka, R., Saleh, A. A., & Putra, S. (2012). Prevention of phishing attacks based on discriminative key point features of WebPages. *International Journal of Computer Science and Security (IJCSS), Volume (6)*, 1-18. Retrieved from http://cscjournals.org/csc/manuscript/Journals/IJCSS/v olume6 /Issue1/IJCSS-562.pdf

[5]. Mohammad, W., Avita, K., & Goudar, R. H. (2013). Hacktivism trends, digital forensic tools, and challenges: A survey. *Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013)*, 138-144. Retrieved from http://ieeexplore.ieee.org.proxy.hil.unb.ca/stamp/stamp. jsp?tp =&arnumber=6558078