Wireless Network: A Study On Phishing Attacks

Saurabh Varma, GITS Gwalior

Abstract: Many of us connect to Wireless Fidelity (Wi-Fi) without knowing what specific threats one is vulnerable. The list of vulnerabilities is large by nature, and most of these ignored by users. Computer networking has made collaboration necessary to both attackers and defenders. Phishing attacks combine technology and social engineering to gain access to restricted information. The most common phishing attacks today send mass email directing the victim to a web site of some perceived authority. This paper is focused on wireless network and phishing attacks.

Keyword: Wireless network, Phishing attacks, web sites, authentication, security.

1. Introduction:

Phishing attacks combine technology and social engineering to gain access to restricted information. The most common phishing attacks today send mass email directing the victim to a web site of some perceived authority. These web sites typically spoof online banks, government agencies, electronic payment firms, and virtual marketplaces. The fraudulent web page collects information from the victim under the guise of "authentication," "security," or "account update." Some of these compromised hosts simply download malware onto clients rather than collect information directly [1].

1.1 Anatomy of an Attack:

Phishing attacks involve three major phases: The first is potential victims getting a phish; the next is the victim captivating the suggested action in the message, usually to go to a fake Web site but can also include installing malware or replying with responsive in order; and the third is the illegal monetizing stolen information.

Fake phishing email, most phishing email messages use social techniques quite than technical actions to fool end users. Assigning necessity is a recognized method used by criminals to misdirect people's consideration [2]; an example is pretending to be a system administrator warning people about a novel assault, urging them to install the attached patch. Another is notifying people there have been several failed logins for their account and they must confirm their account now or danger dire consequences, interesting to people's sense of greed is an ancient procedure now modified to the digital world. One phish the author of this editorial approximate fell for about five years ago was filling out a survey for a bank in return for a small amount of money. The survey seemed inoffensive until it asked for a bank-account number for depositing funds. So-called Nigerian 419 scams, offering "free" money in exchange for helping the dispatcher move big amounts of money, also fall into this group. However, such obvious get-rich-quick scams are morphing to appeal to further emotions. Phishers today strength pretense as a relief agency asking for help with a recent natural disaster or as a random person appealing to prurient interests, as in, say, "sees Britney Spears naked."

2. Review of literature:

One of the first mass attacks on embedded software was performed by the Chernobyl virus in 1999 [28]. The objective of this malware is purely obliteration. It attempts to erase the hard disk and overwrite the BIOS at specified dates. Cell phones have also become targets for worms [29] with the first reports in the wild in 2004, the same author in 2003 predicted infectious malware for the Linksys line of home routers, switches and wireless access points [30]. Adelstein, Stillerman and Kozen identify non destructive malware in Open Firmware boot platforms as a threat. To assure portability, parts of the boot software are written in the stack based language, Forth, and these scripts are executed via an interpreter. They propose a code analyzer the checks for malicious code at load time and prevent aged code from running. Arbaugh, Farber, and Smith implement a cryptographic access control system, AEGIS, to ensure that only sanctioned bootstrapping firmware can be installed on the host platform.

This study explores a variant of email based phishing, where distribution occurs through online market places and hardware is "spoofed" by maliciously compromising its embedded software. Our central example, the malicious home network router, steals information not only by passive eavesdropping, but by Pharming or DNS spoofing.

Browser toolbars at potential phishing web sites using a mixture of link analysis, content analysis, reputation databases, and IP address information. Spoof Guard does two rounds of checks. If either of these tests fails, a second round examines images and form boxes to determine if the page semantically

represents a request for information (e.g. login, credit card, etc.) Another system, PwdHash, generates per site passwords by hashing domain name concatenated to the user password. When the domain names differ, the resulting string does not reveal a usable passphrase. Pharming attacks defeat both of these tactics because they assume correct name resolution. The Net craft toolbar claims defends against Pharming attacks since it reveals the geographic location of the server. While this can raise suspicion, it does not provide a strong defense. Criminal networks have commoditized zombie machines with prices ranging from $0.02 to $0.10 per unit; attackers can choose plausible locations for their hosts if this method ever becomes an effective defense.

3. Phishing attacks and their potential impacts

Phishing is a kind of social-engineering attack in which criminals use spoofed email messages to trick people into sharing sensitive information or installing malware on their computers. Victims perceive these messages as being associated with a trusted brand, while in reality they are only the work of con artists. Rather than directly target the systems people use, phishing attacks target the people using the systems. Phishing cleverly circumvents the vast majority of an organization's or individual's security measures. It doesn't matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organization has if the person behind the keyboard falls for a phish.

The word “phishing” originally comes from the analogy that early Internet criminals used email lures to “phish” for passwords and financial data from sea of Internet users. The use of “ph” in the terminology is partly lost in the annals of time, but most likely linked to popular hacker naming conventions such as “Phreaks” which traces back to early hackers who were involved in “phreaking” – the hacking of telephone systems.
The term was coined in the 1996 timeframe by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users. The popularized first mention on the Internet of phishing was made in alt.2600 hacker newsgroup in January 1996; however the term may have been used even earlier in the popular hacker newsletter “2600”.

Over time, the definition of what constitutes a phishing attack has blurred and expanded. The term Phishing covers not only obtaining user account details, but now includes access to all personal and financial data. What originally entailed tricking users into replying to emails for passwords and credit card details has now expanded into fake websites, installation of Trojan horse key-loggers and screen captures, and man-in-the-middle data proxies – delivered through any electronic communication channel.

Phishing has been classified into web-based phishing and exploit-based phishing [1]. All the attacks which exploit well-known vulnerabilities in popular web browsers to install malware on the victim’s machine come under exploit-based phishing. Visually deceptive phishing can be further classified into using deceptive text, or copying images in the URL [2, 3]. Users can be fooled by making fake websites with a very minor difference in the spelling of the domain name. For example, a difference between the letters “l” and “i” can escape the untrained eye, and “paypal.com”, and “paypai.com” can appear to be the same. Phishers also use non-printing characters and non- ASCII Unicode characters [4].

4. Detection of phishing attacks

Wireless Fidelity connections to the Internetwork have provided near limitless computing convenience for business and private users. These networks are easy to use and have a large variety of devices that can connect. However, wireless connections can be more damaging to network security and user privacy than their fellow wired connections. Although secure wireless connections can limit risk involved when connecting devices to a Wi-Fi network, many of today's Wi-Fi’s are unsecured. Today, Phishers move to wireless connections to trick users' to give their personal information. Wi-Fi networks are vulnerable to a variety of threats including the evil twin attack where an adversary clones a client's preset Set Service Identifier (SSID) for identity theft or any other malicious activity.

4.1 General Methods to Detect Phishing Attacks

A “phish” is a term for a scam website that tries to look like a site that you know might well and visit often. The act of all these sites trying to steal your account information is called *phishing*. While it’s very easy to spot some sites as a phish, others aren’t nearly as easy.

Here are four different anti-phishing methods you can use so that you don’t fall victim to phishing.

1. Use a Custom DNS Service

You need a DNS resolution service so that you can access all the sites that you go to. Your computer doesn't automatically know where Face book is (as far as its Internet address, or IP address, goes), so it needs to ask a DNS resolution service for that IP address. The good thing is, all Internet users have this service, thanks to their internet service provider. The bad news is that's all they do.

The DNS servers at ISPs do nothing else. However, there are some custom and independent DNS companies that do more than just name resolution. They can also filter sites based on content and malware/phishing concerns

2. Use Browser's Phishing List

The browsers check the site visiting against the list to see if it's possibly a phishing site. If it is then browser will start freaking out about it in your face like a good boy. For possible phishing attacks, why *not* throw out a big red page to warn you?

3. Use Sites to Check Links

In case you're presented a link but you're not sure about clicking it, you can copy and check it on a number of different sites. These can tell that whether there's something bad about these sites, including malware and phishing.

4. Use Your Own Ninja Skills

This may sound like useless advice, but using your own skills to detect phishing sites can go a very long way as well, and may even protect you from phishing sites that haven't made it onto any lists that would throw an immediate flag.

Conclusion:

Cybercriminals are continually finding new ways to avoid detection and develop techniques to and manipulate communications and improve the success rates of phishing attack. There are multiple pre cautions already in place such as web browsers taking preventative measures to blacklist compromised websites, although this can also present further concerns for legitimate businesses who are also a victim of cyber fraud. There are many preventative measures and precautions that organizations' can also implement to ensure their websites and networks remain secure. This has now become more vital than ever in ensuring that customer trust is not damaged.

References

1. Tyler Moore, "Cooperative attack and defense in distributed networks" Technical Report, UCAM-CL-TR-718, ISSN 1476-2986
2. Stajano, F. and Wilson, P. Understanding scam victims: Seven principles for systems security. Commun. ACM 54, 3 (Mar. 2011), 70–75.
3. Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. Social phishing. Commun. ACM 50, 10 (Oct. 2007), 94–100.
4. Hong, J. Why have there been so many security breaches recently? Blog@CACM
5. CERT. Incident note IN-99-03.http://www.cert.org/incident notes/IN-99-03.html, April 1999.
6. Ivan Arce. The shellcode generation. IEEE Security & Privacy, September/October 2004.
7. Ivan Arce. The rise of the gadgets. IEEE Security & Privacy, September/October 2003.

