A study of Email date attacks in Network Security

Mr. Kamlesh Lahre
Asst. Professor CSE. Dept.
Dr. C.V. Raman University
Bilaspur(C.G.),India
lahrekamlesh@gmail.com

Rohit Kumar Miri
Asst. Professor CSE. Dept.
Dr. C.V. Raman University
Bilaspur(C.G.),India
rohitmiri@gmail.com

Suraj Prasad keshri
M.Tech Research scholar
Dr. C.V. Raman University
Bilaspur(C.G.),India
suraj.softtech11@gmail.com

Abstract:- phishers have made uses of an increase email of delivery systems handing over confidential and personal information. After 12 years of spoofing attacks publicity, spoofing attacks to the professional whose run them. While spoofed mail developing phisher attack vectors, protect their customer personal data. Business Customer has become way of "officially" e-mail data and question the integrity of the web sites they now connected to as their confidence With various governments and industry groups to preventing any organizations can takes a proactive approach's in combining the email attacks threat. the tool understand and technique use by these professional criminals, and analyze flaw in their own perimeters securities or application, organization can preventing successfully data spoofing attack techniques .These update paper cover the technologies and securities flaw spoofed exploit to conducted their attack, and provide detail vendor advice on what the organization can do to preventing data attack. The information, security professionals and customer can works to protect them selve again the next attack scam to reached their mail inboxes. An office worker clicks on an attachment in email. This infect each Personal computer with malware that components of other machine in each office by snooped password that travel across the MAN. Anthers of the attacks techniques that make sense only in a networks context is web hacking.

Keywords*: Phishing attacks, One Time Password, Authentication, public key , Encryption, Client Identity, e-commerce .*

*****

1. INTRODUCTION

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card detail. The popular social web site, auction site, bank, online payments process or information technology administrator are commonly use to unsuspected public. spoofed email may contained link to website that was infected with malware. Phishing is typical carry put by email spoofing and it usually direct user to enter detail at a fake websites whose look and feel are almost identical. Spoofed mail is an example of social engineering techniques uses to system user and exploits the poor usability to current websites securities technologies. Spoofing is a continue threat that keep growing to these days. The risks grow even largest in social media like that Face book, Twitter etc. Hacker commonly used this website to attacking person using the media site in their work place, i.e home, or public in order to take personal and securities information's that can affects the users and the company. The personals information's like as password, username, securities code, and credit cards number among another thing. Many of the protocol in the TCP/IP suite don't provides mechanism for authenticate the source or destination of a message. IP spoofing and ARP spoofing in particularly may be uses to leverage man-in-the-middle attacks against hosts on a network. Public telephone network usually provides Caller ID information, with includes the caller names and numbers, with each call. However, some technology allowed caller to forge Caller Identity Data information and presents false name and number. Gateway between network that allowed like spoofing and other public network then forward those false information's.

2. TYPES OF EMAIL DATE ATTACKS

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attDatative targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur.

2.1 Passive Data Attack

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.

2.2 Active Data Attack

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

2.3 Distributed Data denial-of-service

A distributed denial-of-service (DDDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

2.4 Insider Data Attack

An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access. Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures.

2.5 Close-in Data Attack

A Close-in attack is a type of attack where the attacker is physically close to the target system. Attacker can the the advantages of being physically close to the target devices.

2.6 Hijacking Data attack

Hijack attack In a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. Hijacking is the exploitation of a valid computer session—sometimes also called a *session key*—to gain unauthorized access to information or services in a computer system.

2.7 Spoofing Data attack

A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread bypass access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this.

2.8 Exploit Data attack

In computing, an exploit is an attack on a computer system, especially one that takes advantage of a particular vulnerability that the system offers to intruders.

2.9 Password Data attack

The purpose of password Data king might be to help a user recover a forgotten password (though installing an entirely new password is less of a security risk, but involves System Administration privileges), to gain unauthorized access to a system, or as a preventive measure by System Administrators to check for easily cDatakable passwords.

3. EMAIL DATA AND ATTACK TECHNIQUES

The Many techniques are developed to conducting Email phishing attacks. The person with novice computer skills can use tools which are available freely on the internet to conduct a phishing attacks. The Basics of Web Hacking introduces you to a tool-driven process to identify the most widespread vulnerabilities in Web applications. Email can be an important communications channel between you and your customers, vendors, and industry peers. This page covers some of the more important issues with effectively using email, including tips for managing hundreds of emails per day.

There are many techniques used in Data Attacks

3.1 An office worker clicks on an attachment in email. This infects her PC with malware that compromises other machines in her office by snooping passwords that travel across the LAN.

3.2 The reason she clicked on the attachment is that the email. The malware had infected her mother’s machine and then sent out a copy of a recent email, with itself attached, to everyone in address book.

3.3 Her mother in turn got infected by an old friend who chose a common password for his ISP account. When there are many machines on a network, the bad guys do not have to be choosy rather than trying to guess the password for a particular account, they just try one password over and over for millions of accounts.

3.4 Another attack technique that makes sense only in a network context is *Google hacking*. Here, the bad guys use search engines to find web servers that are running vulnerable applications.

3.5 The malware writers infect a whole lot of PCs more or less at random using a set of tricks like these. They then look for choice pickings, such as machines in companies from which large numbers of credit card numbers can be stolen, or web servers that can be used to host phishing web pages as well.

3.6 One of the applications is *fast-flux*. This changes the IP address of a web site perhaps once every 20 minutes, so that it’s much more difficult to take down. A different machine in the botnet acts as the host (or as a proxy to the real host) with each change of IP address, so blocking such an address has at most a temporary effect. Fast-flux hosting is used by the better phishing gangs for their bogus bank websites.

4. PROBLEM STATEMENT

There are four basic sources of insider security problems:

4.1 Maliciousness – that results in compromise or destruction of information or disruption of services to other insiders

4.2 Security Practices – that results in compromise or destruction of information or disruption of services to other insiders.

4.3 Carelessness – in the use of an information system and/or the protection of company information

4.4 Ignorance – of security policy, security practices and information system use

5. RELATED WORKS

DATA Attack is a free curriculum and platform for hands-on learning labs related to DATA (cluster database). We believe that the best way to learn about DATA is with a lot of hands-on experience. Cyber crime continue to evolve and refine their attack tactics to evade detection and use techniques that worktop Words Used in data Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data. The report indicates that cybercrime also tend to use finance-related words, such as the names of financial institutions. Data phishing emails are particularly effective as cyber criminals often use information from social networking sites to personalize emails and make them look mostly authentic. Top Words Used in Data Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data s based on data from the Fire Eye .

6. FUTURE WORK

The future of security must reach beyond the capability of an appliance .The malicious attacker will eventually bypass detection based on the fact that there are data hackers out there with a rack of all the latest vendor IPS, Firewalls, etc. in a lab designed to test how effective a piece of malware is against any enterprise security solution. This “already compromised” concept has increase demand for insider threat technology based on reacting to having your network breached. Post compromise data technology is extremely important but obviously not where you want to end up regarding your security posture. The other area of focus growing in popularity besides blocking active data attacks is identifying the ATTACKERS to prevent the initial *attack* aka BEFORE an attack or pre-attack. The concept is simple, why let yourself be attacked from a known malicious source.Why waste defense cycles blocking the same thing over and over again. The “**attacker**” concept can be explained as web sources that may attack you if a connection is capable. This can be accessing malicious websites, hackers attacking you from untrusted networks such as an unregistered IP address. see an attack, which you could prevent with a attack detection tool but you may also get compromised. This is a risky situation.

7. CONCLUSION

This research is centered on a study of Email date attacks in Network Security”. The outcome of the proposed work will likely to yield expected result and fulfill the following objective:

1. Secure email data access.
2. Prevent email data attacks.

REFERENCES

[1] Case Study: Network Clarity, SC Magazine 2014

[2] Cisco. (2011). What is network security?. Retrieved from cisco.com

[3] pcmag.com

[4] Security of the Internet (The Froehlich/Kent Encyclopedia of Telecommunications vol. 15. Marcel Dekker, New York, 1997, pp. 231–255.)

[5] Introduction to Network Security, Matt Curtin.

[6] Security Monitoring with Cisco Security MARS, Gary Halleen/Greg Kellogg, Cisco Press, Jul. 6, 2007.

[7] Self-Defending Networks: The Next Generation of Network Security, Duane DeCapite, Cisco Press, Sep. 8, 2006.

[8] Security Threat Mitigation and Response: Understanding CS-MARS, Dale Tesch/Greg Abelar, Cisco Press, Sep. 26, 2006.

[9] Securing Your Business with Cisco ASA and PIX Firewalls, Greg Abelar, Cisco Press, May 27, 2005.

[10] Deploying Zone-Based Firewalls, Ivan Pepelnjak, Cisco Press, Oct. 5, 2006.

[11] Network Security: PRIVATE Communication in a PUBLIC World, Charlie Kaufman | Radia Perlman | Mike Speciner, Prentice-Hall, 2002. ISBN.

[12] Network Infrastructure Security, Angus Wong and Alan Yeung, Springer, 2009.