Phishing

Author: Sahil Shaikh, Tosib Silawat
Co-Author: Prof. Vivek Dave
Department of MCA, Parul University, Vadodara, India

Abstract: This Document represents review of Interposes Communication methods such as message queue, semaphore and shared memory and discusses their advantages and disadvantages. Through shared memory and a Message Queue method to achieve inter-process communication, to reduce the number of copy times during the message passing procedure. Moreover, this mechanism provides some support to the inter-process communication of multi-processor, improved the efficiency of micro-kernel inter-process communication, to meet the current needs of micro-kernel operating system. I identified the various factors that could affect their performance such as message size. The purpose of this Report is to provide a survey of IPC methods that appeared in the literature over the past decade which was not discussed and also categorize them into meaningful approaches.

I. INTRODUCTION

Phishing is a form of online identity theft that aims to steal sensitive information such as online passwords and credit card information. Phishing attacks use a combination of social engineering and technology spoofing techniques to persuade users into giving away sensitive information that the attacker can used to make financial profit. Normally phishers hijack banks web pages and send emails to the victim in order to trick the victim to visit the malicious site in order to collect the victim bank account information and card number. The information flow is depicted in Fig 1.

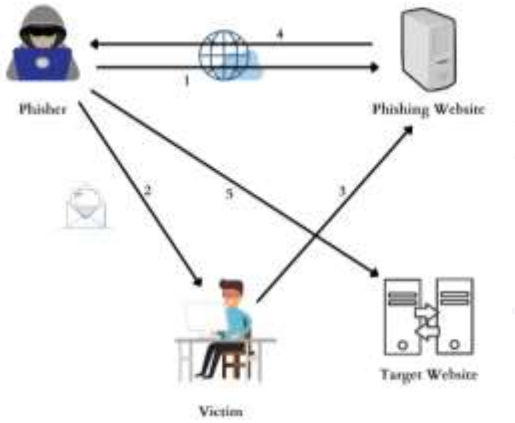


Fig 1: Information Flow in phishing

A complete phishing attack involves the roles of phisher. Firstly, mailers send out large number of fraudulent e-mails which directs uses to fraudulent websites. Secondly collector set up fraudulent websites which actively prompt users to provide confidential information. Finally, cashers use the confidential information to achieve a payout. Goal of this paper is to present on extensive overview of the phishing attacks. The paper is organized as follows. The section II will have an outline of the types of phishing. The section III deals with the theoretical aspects of the phishing techniques. The section IV describes the categories of anti-phishing techniques. Finally, conclusion given in section IV.

II. TYPES OF PHISHING

Phishing has spread beyond e-mail to include VOIP, SMS,Instant messaging, social networking sites and even multiplayer games. Below are some major categories of phishing.

A. Clone phishing

Clone phishing is a type of phishing attack where hacker tries to clone a web site that is victim usually visits. Thecloneweb site usually asks for login credentials, mimickingthe real websites. This will allow the attackers to save thecredentials in a text file, database record on his own server,and then the attacker redirects his victim to the real websites as authenticated user.

Spear phishing targets at specific group. So instead ofcasting out thousands of e-mails randomly spear phisherstarget selected groups of people with something in common. For example, people from same organisation.

C. Phone phishing

This type of phishing refers to messages that claim to beform a bank asking users to dial a phone number regardingproblems with that bank accounts. SMS phishing is avariation for phone phishing. The end-users receiveSMS telling him that he has successfully subscribed to a service.If he wants to unsubscribe the service, he should visit thewebsite now the end users visit the websites and providesensitive information.

D. DNS-Based Phishing (Pharming)

Pharming is an attack aiming to redirect a website traffic to another bogus site. Pharming interferes with the resolutionof domain name to an IP address so that domain name ofgenuine web site is mapped onto IP address of roguewebsite. DNS based phishing is depicted in Fig 2.

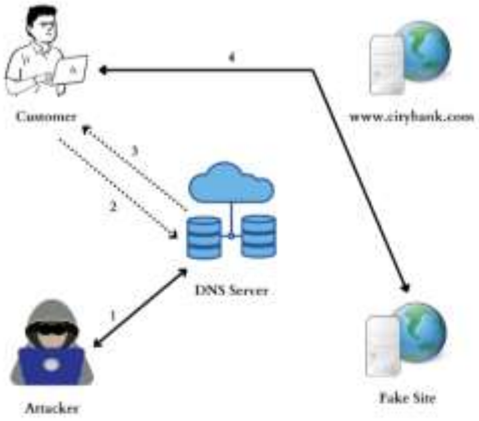


Fig 2: DNS Based phishing

E. Man-in-the-middle-attack

A man-in-the-middle attack often refers to an attack in which an attacker secretly intercepts the electronic messages given between the sender and receiver and then capture, insert and modify message during message transmission. A man-in-the-middle attack uses Trojan horses to intercept personal information.

III. THEORETICAL ASPECTS OF PHISHING TECHNIQUES

Various techniques are developed to conduct phishingattacks. The phishing techniques are described as follows.

A. Email spoofing

Email spoofing is used to make fraudulent emails appearto be from legitimate senders so that recipients are morelikely to believe in the message and take actions according toits instructions. Email spoofing is possible because Simple Mail Transfer Protocol does not include an authenticationmechanism. To send spoofed emails sender inserts command sin headers that will alter messageinformation. It is possible to send a message that appears to be from anyone anywhere saying whatever the sender wants it to say.

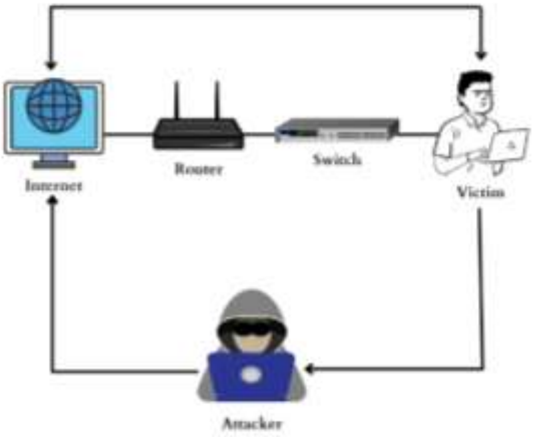


Fig 3: Email Spoofing

B. Web spoofing

A Phisher could forge a website that looks identical to a legitimate website so that the victims may think this is the genuine site and enter the personal information which is collected by the phisher. Web spoofing creates a shadow copy of the World Wide Web. The shadow copy is funnelled through attackers' machine.

Modern web browsers have built in security indicators that can including domain name highlighting and HTTPS indicators as shown in Example They are often neglected by careless users. Modern web browsers display a padlock icon whenvisiting an

HTTPS web site of Hyper Text Transfer Protocol and HTTPS, Transport Layer Security, provides encryption and identification through public key infrastructure. Show Example of redirect to PayPal fake website

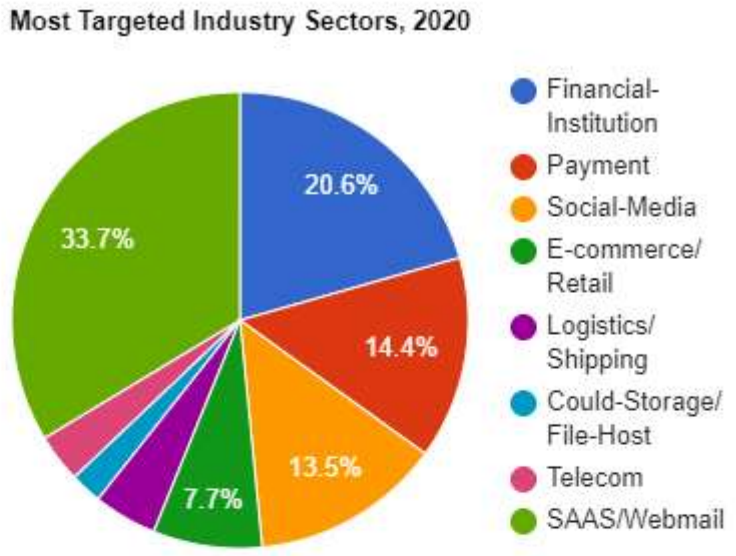
<a href=http://www.paypal.com/
*onclick="this.href = 'http://www.paysite.com/';">**PayPal**</a>*

C. DNS Cache Poisoning

DNS cache poisoning attempts to feed the cache of localDNS resolves with incorrect records. DNS runs over UDP and easy to spoof the source address of the UDP packet.For example, attacker wants his IP address returned for aDNS query, when the resolver asks NS1.google.com forwww.google.com.The attacker could reply first, with its ownIP.

D. Malware

Malware is software used to disrupt computer operation gather sensitive information. It can appear in the form of code, scripts, active content and other software. Malware includes viruses, worms, trojan horses, key loggers, spyware, adware. Client security products are able to detect and remove malware and other potentially unwanted programs. But phishers can make malwareundetectable. Key strokes, screen shots, clipboard contents and program activities can be collected and send this information to phishers by e-mail, ftp server or IRC channel.



IV. CONCLUSION

Phishing attacks are still successful because of many inexperienced and unsophisticated internet users. The last years have brought a dramatic increase in the number and sophistication of such attacks. This paper provides a broad survey of various phishing types which are used by attackers to steal the sensitive information. This study clearly shows that phishing techniques enable the attackers to steal the information efficiently. Our future work is to compare various types of anti-phishing techniques and choose the best one for further research.

V. REFERENCES

Anti-Phishing Working Group
http://www.antiphishing.org
Digital Phishnet
http://www.digitalphishnet.org/
Federal Trade Commission
http://www.consumer.gov/idtheft/
Internet Crime Complaint Centre (a joint project of the FBIand the National Collar Crime Centre)
http://www.ic3.gov