A New Architecture to Perform Phishing via Trojan horse

C.Mounica
Computer Science & Engineering
Karunya University

S.Benson Edwin Raj
Asst.Prof (SG)-CSE
Karunya University

ABSTRACT
Today internet is full of web security threats such as phishing attack, Email bombing, Trojan virus etc., the hackers are increasing in number day by day. They invent new techniques to steal data and confidential information.

Here a hybrid approach to launch a phishing attack is proposed. We use Trojan horse, email bombing, data stealing to perform phishing attack. Such approach is a eye open for all people to have an idea, so that they can prevent and avoid threats.

1. INTRODUCTION

1.1 Trojan horse
A Trojan horse, or Trojan, is software that appears to perform a desirable function for the user prior to run or install, butsteals information or harms the system. [1][7]. It makes the user to believe that it is a legitimate computer application while, in the background, it helps the hacker to spy and steal valuable user information. The virus will begin infecting other files on execution of the infected software. Trojan horses do not reproduce themselves which differentiates them from other computers viruses and worms.

A trojan horse is typically separated into two parts – a server and a client.

It's the client that is cleverly disguised as significant software and positioned in peer-to-peer file sharing networks, or unauthorized download websites. Once the client Trojan executes on your computer, the attacker, i.e. the person running the server, has a high level of control over your computer

Moreover, the Trojan horses should continuously communicate with their originator in order to accomplish their malicious task.[2].

1.1.1 *Different types of Trojan horse*

Trojan horses are almost always designed to do various harmful things, but could be harmless. They are broken down in classification based on how they breach system and the damage they cause. The five main types of Trojan horse[2] they are

1. Remote Access
2. Email Sending
3. Data Destructive
4. Denial-of-service attack (DoS)
5. FTP Trojan (adding or copying data from the infected computer).
6. Proxy Trojans
7. Anti-Protection Trojans.[3][4].

1.2 Email bombing:
In the internet usage, an Email bomb is a form of net abuse consisting of sending huge volumes of Emails to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.[5]

Denial-of-service attack[6]
a type of attack on a netwok by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death* and *Teardrop* attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks.

But, like viruses, new DoS attacks are constantly being dreamed up by hackers.

We use MASS MAILING technique for Email bombing.

The email bombing is of three types

1. Mass Mailing
2. List Linking
3. Zip Bombing

1.2.1 Mass Mailing
Mass mailing consists of sending numerous duplicate mails to the same email address. These types of mail bombs are simple to design but their extreme simplicity means they can be easily detected by spam filters. Email-bombing using mass mailing is also commonly performed as a DDOS attack[1].

1.3.2 List Linking
List linking means signing a particular email address up to several email list subscriptions. The victim then has to unsubscribe from these unwanted services manually. The user's email address gets registered to unwanted spam sites and email address receives junk content from these sites. The mail content will be some discount offers but it actually is a spam content.

1.3.3 Zip Bombing
A ZIP bomb is a variant of mail-bombing. It consists of an enormous text file, containing for example, only the letter z repeated millions of times. Such a file compresses into a relatively small archive, but its unpacking(especially by early versions of mail servers) would use a high amount of processing power, RAM and swap space, which could result in denial of service.

1.3 Phishing attack
In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by

masquerading as a trustworthy entity in an electronic communication.

Phishing is an example of a social engineering techniques used to fool users and exploits the poor usability of current web security technologies.[6]

1.1.1 *Different types of phishing attack*

Numerous different types of phishing attacks[3] have now been identified. Some of the more prevalent are listed below[6].

Deceptive phishing:

The term "phishing" originally referred to account theft using instant messaging but the most common broadcast method to deceptive email message.

Malware-Based Phishing:

This attack refers to scams that involve running malicious software on the users PCs. Malware can be introduced as an email attachment, as a download file from a website.

Key loggers and Screen loggers:

These are particular varieties of malware that track keyboard input and send relevant information to the hacker via the internet. They can embed themselves into user's browsers as small utility program known as helper objects that run automatically when the browser is started as well as into system files as device drivers or screen monitors.

Session hijacking:

This is a kind of attack where users' activities are monitors until they sign in to a target account or transaction and establish their bona fide credentials. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.

Web Trojans:

These Web Trojans popup invisibility when users are attempting to log in. They collect the user's credentials locally and transmit them to the phishers.

Host File Poisoning:

This is a kind of attach where a user types a URL to visit a website it must first be translated into a IP address transmitted, taking the user unwittingly to a fake "look alike" web site their information can be stolen.

System Reconfiguration Attacks:

These attacks modify settings on user's PC for a malicious purpose. For example: URLs in a favorites file might be modifies to direct users to look alike website. For example: a bank website URL may be changes from "bankofabc.com" to "bancofabc.com".

2. RELATED WORKS

2.1 Trojan horse

1. For example, if you access your online bank account, enter your credit card information for online purchases, or transmit other important, confidential information--the keylogger sends it all right to the hacker.
2. This appears to be a very specific virus writer targeting government agencies and, not as (other articles) suggested, targeting only U.K. government agencies," said Dave Cowings, senior business intelligence manager for Symantec.Two programs that fit the profile--identified by Symantec as Trojan.Mdropper.B and Trojan.Riler.C--were among the threats warned about by the NISCC. The Trojan horse programs were attached as documents to e-mail messages. The documents had names that sounded military, including "Nuclear Weapons Technology Proliferation.doc." Others were more generic, such as "Notepad.exe" and "Code Password.doc.".These are definitely virus attacks that attempt to sneak under the radar and are specifically targeted towards government agencies.[6][7]

2.2 Email bombing

1. In the weeks leading up to the five-day 2008 South Ossetia war, a DDoS attack directed at Georgian government sites containing the message: "win+love+in+Rusia" effectively overloaded and shut down multiple Georgian servers. Websites targeted included the Web site of the Georgian president, Mikhail Saakashvili, rendered inoperable for 24 hours, and the National Bank of Georgia. While heavy suspicion was placed on Russia for orchestrating the attack through a proxy, the St. Petersburg-based criminal gang known as the Russian Business Network, or R.B.N, the Russian government denied the allegations, stating that it was possible that individuals in Russia or elsewhere had taken it upon themselves to start the attacks.
2. On December 8, 2010, a group calling themselves Anonymous launched orchestrated DDoS[attacks on organisations such as Mastercard.com, PayPal, Visa.com and PostFinance; as part of the ongoing "Operation Payback" campaign, which originally targeted anti-piracy organisations, in support of the Whistleblowing site Wikileaks.ch and its founder, Julian Assange. The attack brought down the Mastercard, PostFinance, and Visa websites successfully. PostFinance, the bank that had frozen Julian Assange's account, was brought down for more than 16 hours due to the attacks. However, in denial of the fact that it was taken down by a bunch of notorious internet users, the bank issued a statement that the outage was caused by an overload of inquiries.[8]

2.3 Phishing attack

1. For example, 2003 saw the proliferation of a phishing scam[5] in which users received e-mails supposedly from eBay claiming that the users account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking

they were actually being contacted by eBay and were subsequently going to eBay??s site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

fig. 2.3 Email from the trustedbank[5][9]

2. "Phishing" e-mail may look like in the above fig. 2.3. The bank here is fictional, but it is to be assumed that a real phishing attempt would claim to be from an actual bank the customer belongs to. Notice how it tries to establish authenticity by using the bank's logo and providing what appears to be link to a website the customer has been to many times before. This mock-up was created by me on December 2, 2005 and placed in the public domain. Note the effect achieved by not using "i before e, except after c", thus misspelling the word "received".

3.0 PROPOSED ARCHITECTURE

This is an hybrid architecture where we use phishing attack, email bombing, Trojan horse, data stealing techniques. Through these techniques we can steal the data and other confidential information.

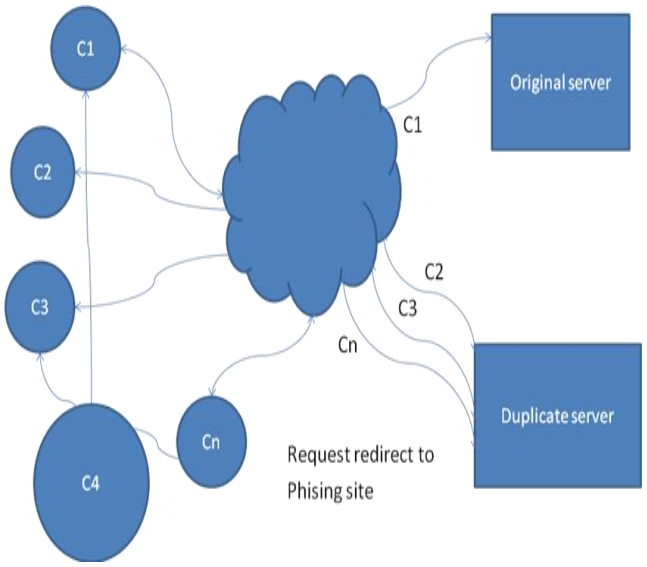

Fig 3.0-proposed architecture

Consider there are nodes (fig 3.0) in the network. For example consider the node C4 which has the contacts of C1, C2, C3, Cn the contact of C2 is not present in the address book of the C4 node.C4 node has the Trojan horse running in it, so the contacts C1, C3, Cn are Email bombed.C2 contact is not a victim of the Trojan horse so it is able to access the original server directly

The email content has the link to launch the phishing attack. When the user clicks on the link he is redirected to the duplicate server instead of original server. Using the details he entered he is redirected back to the original server. In this whole process the victim's account is compromised by stealing the data which the user entered in a fake website.

3.1 Email bombing the Outlook contacts

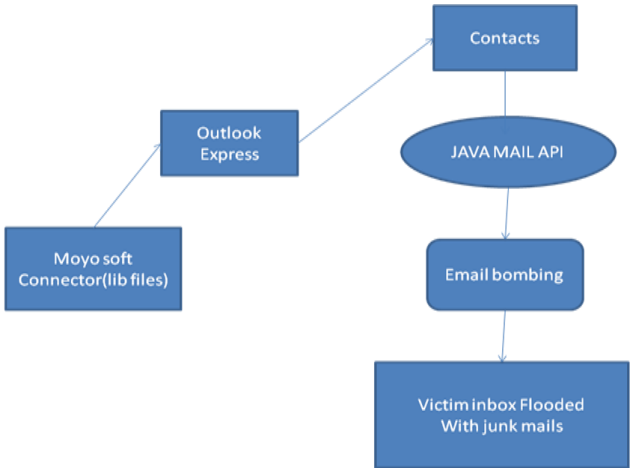

Fig 3.1 Email bombing

To perform the email bombing the client should have Microsoft Outlook Express installed in his system and contacts stored in it. The java program makes use of the MOYOSOFT CONNECTOR which is the library files to access the contacts in the Outlook

Express. Using these library files each of the contact present in the Outlook Express[13] is read and is stored in a variable. Using a standard JAVA MAIL API[11] the contacts are Email bombed with the standard mail message header, text and subject. A numerous number of junk mails are sent to the contacts containing a link to the phishing page. When the user clicks on the link a phishing attack is launched. The entire Email Bombing flow is given in the above diagram fig 3.1.

3.2 Phishing attack for data stealing

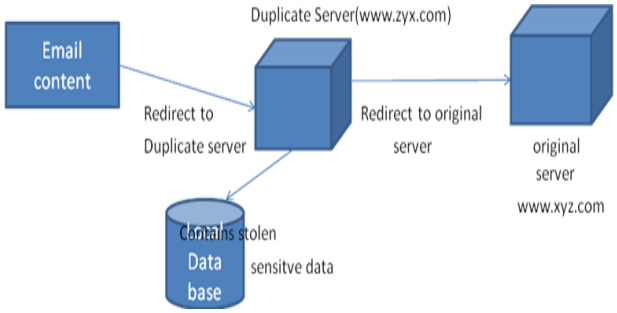

Fig 3.2 Phishing attack for data stealing

To perform a Phishing attack the clients[4] has to click on the link which he received from the Email bomb. When the user clicks on the link it looks like a legitimate link but its internal reference will be to the duplicate server which the user is unaware. When the user clicks on the link he will be redirected to the duplicate server which resembles the original server. The user feels as if he is entering his sensitive information on the legitimate server but he is actually entering the details in a duplicate server. Thus the account details of the victim are compromised. The stolen information is updated on both the application server. Above fig 3.2 shows how a phishing attack is done

3.3 Exe-Binding

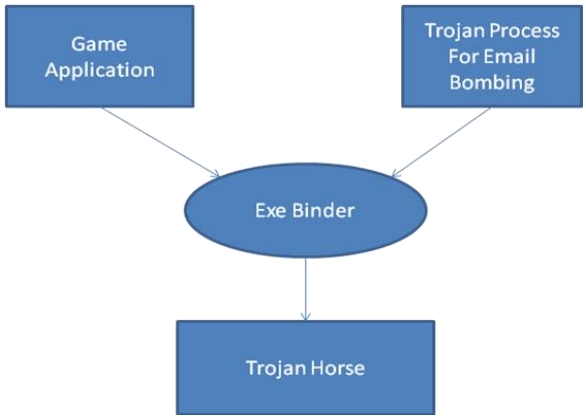

Fig 3.3 Exe-binding

Binding is the process of combining the two executable into single executable so that the two executables execute at the same time. We use exe binder like one-exe-maker which is third party software tool used to generate the combined exe. In this tool we first executable as the attractive game application and we set its parameter as a normal executable. Next we have the executable which does the actual Email bombing. This executable is given the attribute as hidden. This executable works as a hidden process and does the actual work of a Trojan horse. These two combined executable form single executable which will be the generated Trojan horse. Above figure shows an EXE BINDING is done.

3.4 Creation and prevention tool for the designed Trojan

A prevention tool will be designed for a specific purpose. In this case the prevention tool should be able to detect the Trojan process which is performing the Email bombing and stop the execution of that process.

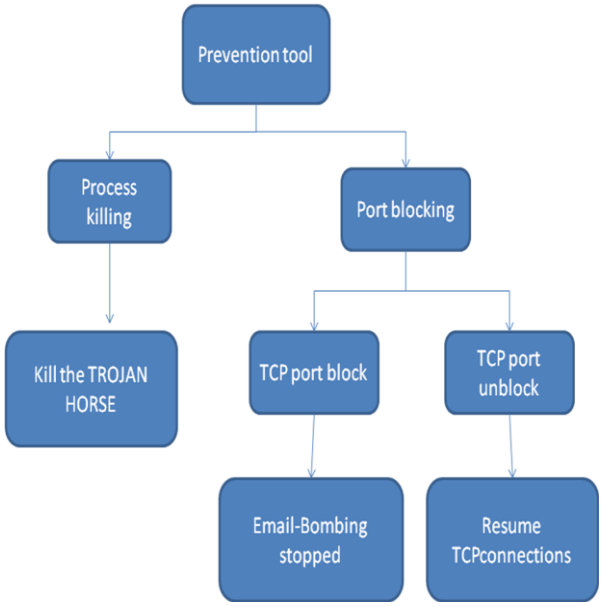

Fig 3.4 Prevention tool

There are two ways in which the removal tool can be implemented

Process Killing.

Port blocking.

Process killing:

Each application associated to the particular process, the Trojan horses also associated with a process. To implement the process killing the removal tool has to identify the Trojan process and kill it. To kill the process the removal tool uses windows utility tool TASK KILL . Sign task kill we can set rules that can kill process which satisfy the rule

Port blocking:

Port blocking refers to blocking the ports on the client side. Each network application runs on a particular port. The Trojan horse opens a port on a client side above 1024, it communicates through port 25 on remote server. We cannot manipulate the port

on server side so all the manipulation regarding the ports should be done on client side.

4. IMPLEMENTATION

Implementation is a process that means converting a new system in to operation. Proper implementation is essential to provide a reliable system to meet the requirements. The various features provided in the system were discussed during implementation

4.1. Email Bombing

To do Email bombing of the Outlook Express contacts we need library files like mail authenticator to check the correct email address. This java program needs Microsoft Outlook Connector called the MOYOSOFT OUTLOOK CONNECTOR[12]. The java program uses the library files of javax.mail.*. For implanting the concept of email bombing we require

- Operating system - Windows XP or higher
- Development tools - Netbeans IDE 6.7.1
- Development Environment - JDK 1.6 or above
- Other software - Microsoft Outlook Express.

4.2 Phishing Attack

To implement a phishing attack we use java server pages to create web pages. Phishing attack[3] is done by creating two application servers. We use Glassfish server v2.1. one server is legitimate server and other is duplicate server[4].

Operating system - Windows XP or higher

- Development tools - Netbeans IDE 6.7.1
- Development Environment - JDK 1.6 or above
- Application server - Glassfish v2.1

Host file acts as a local DNS on Windows operating system.

4.3 EXE Binding and Trojan Generation

To create a Trojan horse we need to bind the Trojan process with the game application. Using this tool we can combine both the game and Trojan process. The following tools are required for implementation of exe binding.

- Operating system - Windows XP or higher
- EXE Generator - Jar-to exe Wizard 1.8
- Binding Tools - Senna Spy One EXE Maker 2000

4.4 Prevention Tool

4.4.1 Process Killing

To implement this process killing the prevention tool has to identify the Trojan process and kill it. To kill the process the prevention tool uses window's utility tool TASK KILL[13]. Using task kill we can set rules that can kill the process which can satisfy.

4.4.2 P*ort Blocking*.

The concept of port blocking is done through the IPSECCMD. This IPSECCMD is a part of the support tools from windows update. This IPSECCMD[15] is used as a firewall. Using this command line we can configure the traffic on the client system. Using this command we can block the port and unblock the port.

4.5 General security measures of Trojan horse

(1) CLEAN RE-INSTALLATION

Back up entire hard disk, format disk, re-install the operating system and all your application from original CDs

(2) ANTI-VIRUS SOFTWARE

Anti-virus software is always going to be playing catch up with active virus on the system and update it regularly .Always it's likely to have auto update option ON

(3) ANTI-TROJAN PROGRAMS

These programs are most effective against Trojan horse attacks, because they specialize in Trojans instead of general viruses.

(4) AVOID USING PEER TO PEER

P2P sharing networks like kazaa[14], Lime wire Ares , or Gnutella have to be avoided because they are generally unprotected. Safe to stop downloading files claim to be "rare" songs, books, movies.

4.6 Methods of Infection

By visiting a rogue websites

- Using Microsoft Outlook[12] that has Internet Explorer
- Open ports: Computers with their own servers

4.7 How to avoid infecting in the future

- NEVER download blindly from people or sites which are not 100% sure about[8].
- Must be sure what the file is before opening
- Never use features in your programs that get or preview files
- NEVER blindly type commands that strangers tell you to type.

4.8 Experimental result

Thus TROJAN HORSE [1] created in an Ethical way to know about how the Trojan horse works and how a Phishing Attack is launched by hackers to compromise some victims account. Phishing Attack[3] is not done in the real world but is done in Local Area Network with two application servers. The prevention tool is designed in such a way that he Trojan horse will be stopped thereby stopping the Email bombing.

5. CONCLUSION

There are so many ways to trap the user and steal data or personal information. Hackers are smart enough to choose any kind of techniques and any number of techniques. We had highlighted 4 techinques and created a Trojan horse for data stealing in this paper. There needs to be a more general awareness of hacker attacks to secure privacy. User should have an idea of the real threat of hacking and the problems encountered because of it. He must take precautionary actions and must in fact search for a permanent solution.

6. REFERENCES

[1] Jamie Crapanzano (2003): "Deconstructing SubSeven, the Trojan Horse of Choice", SANS Institute

[2] Carnegie Mellon University (1999): "CERT Advisory CA-1999-02 Trojan Horses".

[3] Gonsalves, Antone (April 25, 2006). "Phishers Snare Victims With VoIP". Techweb

[4] Ponnurangam Kumaraguru, Yong Woo Rhee, Alessandro Acquisti, Lorrie Cranor, Jason Hong and Elizabeth Nunge (November 2006). "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System" (PDF). Technical Report CMU-CyLab-06-017, CyLab, Carnegie Mellon University.

[5] Maher Aburrous , M.A. Hossain , Keshav Dahal , Fadi Thabtah, "An Intelligent phishing detection system for e-banking using fuzzy data mining", Expert Systems with Applications 37 (2010) 7913–7921

[6] William stallings, cryptography and network security, Third edition, Prentice Hall the principles and practice of cryptography and network security, 2009

[7] Charles P. Pfleeger " about trojans, malwares and security of systems" , Security in computing, Prentice-Hall, inc. Upper Saddle River, NJ,2007

[8] Kirda and C. Kruegel, ―Protecting Users against PhishingAttacks with AntiPhish, 29th Annual International Computer Software and Applications Conference, ACM PressWashington, USA, 2005, Vol. 01, pp. 517-524.

[9] Debra L. Cook1, Vijay K. Gurbani1, Michael Daniluk2 "Phishwish: A Stateless phishing filter," Proc. Symp. Usable Privacy and Security, 2005.

[10] Maher Aburrous , M.A. Hossain , Keshav Dahal , Fadi Thabtah, "An Intelligent phishing detection system for e-banking using fuzzy data mining", Expert Systems with Applications, (2010) 7913–792

[11] Elliotte Rusty Harold –"Java network programming",edition 2, "how an mail is sent to client and about java mail API", published by O'Reilly (2000,2001).

[12] Gantam Prabhu-"Ms Outlook Express Guide (e-book)2001.

[13] Thomas, Robert M- " DOS 6 instant reference", all commands used in command prompt, 1993

[14] Andrew S. Tanenbaum-"computer networks", edition4, "working of networks and new technologies", published by Pearson Education,Inc.

[15] Pete Loshin –"Big Book of IPsec RFCs: IP Security Architecture", IP security , (2000)