ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

An Integrated Framework for Detecting and prevention of Trojan Horse (BINGHE) in a Client-Server Network

Ahmed Aliyu[1], Sani Danjuma[2], Bo Dai [3], Usman Waziri[4], Abubakar Ado[5]

Lecturer, Mathematical Sciences, Bauchi State University, Gadau, Bauchi State, Nigeria [1]

Lecturer, Computer Science, Sa'adatu Rimi College of Education, Kumbotso, Kano State, Nigeria [2]

Professor, Electrical/Electronics, Liaoning University of Technology, Jinzhou, Liaoning Province, China[3]

Lecturer, Mathematical Sciences, Bauchi State University, Gadau, Bauchi State, Nigeria [4]

Student, Computer Science and, Liaoning University of Technology, Jinzhou, Liaoning Province, China[5]

Abstract: Due to the advancement of malware which gains privileges to the operating system and drops a malicious code, and allowing unauthorized access to the target computer networks. One of this malware includes a Trojan horse which has access to computer or network with the aid of a user, whether knowingly or unknowingly. This paper presents a frame work of detecting a Trojan horse in network environment (client/server) so as to tackle present kind of Trojan horses (BINGHE). The result of the experiment shows a great potential of the method in allowing the detection and analysing different behaviour and attack of Trojan horse malware in computer and client/server network.

Keywords: Trojan horse, Malware, network, client server

I. INTRODUCTION

A Trojan horse is a non-self-replicating type of malware which gains privileged access to the operating system while appearing to perform a desirable function but instead drops a malicious payload, often including a backdoor allowing unauthorized access to the target's computer [1]. These backdoors tend to be invisible to average users. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems [2]. Trojans may use drive-by download or install via online games or internet-driven applications in order to reach target computers. The term is derived from the Trojan Horse story in Greek mythology because Trojan horses employ a form of "social engineering," presenting themselves as harmless, useful gifts, in order to persuade victims to install them on their computers [3][4][5][6][7]. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses into your computer [8].

Trojan horses in this way may require interaction with a hacker to fulfil their purpose, though the hacker does not have to be the individual responsible for distributing the Trojan horse. It is possible for individual hackers to scan computers on a network using a port scanner in the hope of finding one with a malicious Trojan horse installed, which the hacker can then use to control the target computer [9]. A Trojan may give a hacker remote access to a targeted computer system. Operations that could be performed by a hacker on a targeted computer system may include:

- ✓ Use of the machine as part of a botnet (e.g. to perform automated spamming or to distribute Denial-of-service attacks)
- ✓ Crashing the computer
- ✓ Blue screen of death
- ✓ Electronic money theft and disabling all internet traffic on the host [7]
- ✓ Data theft (e.g. retrieving passwords or credit card information)
- ✓ Installation of software, including third-party malware and ransom ware
- ✓ Downloading or uploading of files on the user's computer
- ✓ Modification or deletion of files
- ✓ Keystroke logging
- ✓ Watching the user's screen
- ✓ Viewing the user's webcam

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

- ✓ Controlling the computer system remotely
- ✓ Anonymizing remote third-party internet viewing

A recent innovation in Trojan horse code takes advantage of a security flaw in older versions of Internet Explorer and Google Chrome to use the host computer as an anonymizer proxy to effectively hide internet usage [10]. A hacker is able to view internet sites while the tracking cookies, internet history, and any IP logging are maintained on the host computer. The host's computer may or may not show the internet history of the sites viewed using the computer as a proxy. The first generation of anonymizer Trojan horses tended to leave their tracks in the page view histories of the host computer. Newer generations of the Trojan horse tend to "cover" their tracks more efficiently. Several versions of Sub7 have been widely circulated in the US and Europe, Asia and are the most widely distributed examples of this type of Trojan horse [9].

II. AN OVERVIEW

Due to the popularity of botnets among hackers and the availability of advertising services that permit authors to violate their users' privacy, Trojan horses are becoming more common. According to a survey conducted by Bit Defender from January to June 2009, "Trojan-type malware is on the rise, accounting for 83-percent of the global malware detected in the world." This virus has a relationship with worms as it spreads with the help given by worms and travel across the internet with them. Their main purpose is to make its host system open to access through the internet. Bit Defender also states that approximately 15% of computers are members of a botnet - usually an effect of a Trojan infection [11][12].

2.1 Classification of Trojan Horses

Trojan horses are classified based on how they breach systems and the damage they cause. The seven main classified types of Trojan horses are [8]:

I. Remote Access Trojan

Abbreviated as RATs, a Remote Access Trojan is one of seven major types of Trojan horse designed to provide the attacker with complete control of the victim's system. Attackers usually hide these Trojan horses in games and other small programs that unsuspecting users then execute on their PCs

II. Data Sending Trojan

A type of a Trojan Horses that is designed to provide the attacker with sensitive data such as passwords, credit card information, log files, e-mail address or IM contact lists. These Trojans can look for specific pre-defined data (e.g., just credit card information or passwords), or they could install a key logger and send all recorded keystrokes back to the attacker.

III. Destructive Trojan

This type is designed to destroy and delete files, and is more like a virus than any other Trojan. It can often go undetected by antivirus software.

IV. Proxy Trojan

A type of Trojan horse designed to use the victim's computer as a proxy server. This gives the attacker the opportunity to do everything from your computer, including the possibility of conducting credit card fraud and other illegal activities, or even to use your system to launch malicious attacks against other networks.

V. FTP Trojan

Is designed to open port 21 (the port for FTP transfer) and lets the attacker connect to your computer using File Transfer Protocol (FTP).

VI. Denial of Service Attack (DoS)

This is a type of attack on a network that is designed to bring the network to its knees 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, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

VII. Security Software disabler Trojan
A type of Trojan horse designed to stop or kill security programs such as an antivirus program or firewall without the user knowing. This Trojan type is normally combined with another type of Trojan as a payload.

2.2 Common Types of Trojan Horses

- ✓ Kryptik (Win32/Kryptik)
- ✓ Netbus (by Carl-Fredrik Neikter)
- ✓ Subseven or Sub7(by Mobman)
- ✓ Back Orifice (Sir Dystic)
- ✓ The Blackhole exploit kit.
- ✓ Flashback Trojan (Trojan BackDoor.Flashback)
- ✓ ProRat
- ✓ Zero Access

2.3 Effect of Trojan Horses Attacks in Some Countries
Cyber attack in China launched from bases overseas surged in 2011, rising to 8.9 million computers affected from 5 million the previous year, according to a network security report.Japan was the source of most attacks (22.8percent) to follow closely by the United States (20.4 percent) and the Republic of Korea (7.1 percent). The report released by China's National Computer Network Emergency Response Technical Team and Coordination Centre, found that 11,851 Internet protocol address based overseas had controlled 10,593 Chinese websites last year. "This shows that Chinese websites still face a serious problem from being maliciously attacked by foreign hackers or IP addresses" Wang Minghua, deputy director of the team operation department said at a news conference. These attacks include destroying servers, distorting website content and stealing personal data from Chinese web users [14]. Overseas hackers altered the content of 1,116 Chinese websites, including 404 run by government agencies, Wang told China Daily, adding that they may have been responsible for many more, as the address and names they are use are often difficult to trace.Although it was discovered that many hackers used Trojan Horse style programs simply to steal personal data.

2.4. Drive-by downloads attacks
Drive-by download attacks make users access the websites that have been compromised by malicious third parties, and infect the users with malware. This method is effective for attackers since they can exploit a number of vulnerabilities at the same time and they can attack a number of users. We will examine the status. Detection of malware from drive-by download attacks Our FNC Secure Web-Net Management Service logs customers' Internet web browsing history using virus check servers. Figure 1 shows monthly history of malware detected by the virus check server in 2012 (April 2012 to March 2013). Malware is categorized into Trojan horse, Exploit, Backdoor, and others. Trojan horse is programs that operate maliciously while the users are unaware. Exploit is programs or methods that attack vulnerabilities of computers and servers. Backdoor is software that is used to allow the attackers to remotely operate the target device. While Trojan horse occupies the majority of detected malware, Exploit is detected at a certain rate every month. This indicates that the attacks on software vulnerabilities are continuously carried out. [15]

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

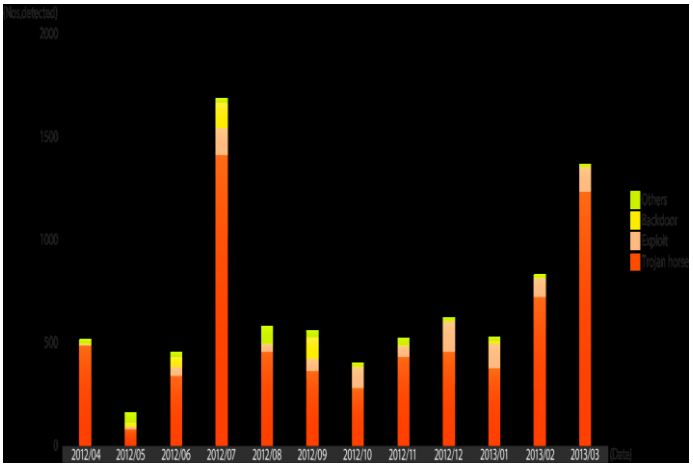

Figure 1: Monthly history of malware detected by virus check servers

Focusing on Trojan horse, the most common attacks. Figure 2 shows a further breakdown of Trojan horse into iframe/redirector, JavaScript, other scripts, and others, and their monthly detection history. "iframe/ redirector" uses inline frame embedding and redirect codes with JavaScript. "JavaScript" indicates other malicious JavaScript codes. "Other scripts" indicates script codes other than JavaScript that are used in Internet Explorer such as VBScript. Any other malicious codes that are not applicable to any of these are in "Others".

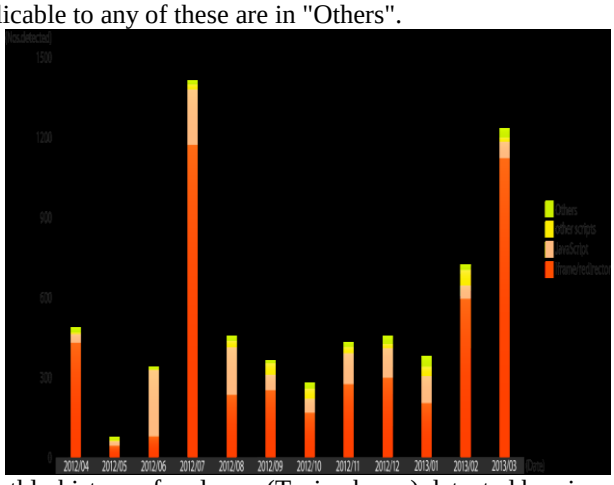

Figure 2: Monthly history of malware (Trojan horse) detected by virus check servers

"iframe/redirector" was in the majority throughout 2012. Together with "JavaScript", the most of malicious codes were written in JavaScript. The number of detected malicious codes used for drive-by downloads attacks such as "iframe/redirector" had a sudden increase in July 2012 and January 2013 onwards. Drive-by download attacks lead users to malicious sites and make them download or execute malware. The attackers falsify legitimate websites by embedding inline frames with malicious contents using JavaScript, or redirect users to malicious sites, to make the user execute codes that exploits vulnerabilities of web browsers or plug-ins. "Iframe/redirector" inserts inline frame codes in to HTML using JavaScript, or redirects users to malicious sites, to make users execute malicious contents. Attackers can make users download malicious contents while the users are unaware because inline frames can be hidden.

2.5. Using Computer Forensic Methods for Privacy-Invasive Software

Boldt and Carlson [16] present a notion of privacy-invasive software (PIS). Adware and spyware are the primary types of privacy-invasive software. Often times, PIS is obtained as a part of file sharing software. Boldt and Carlson use the Forensic Tool Kit (FTK) to help identify the PIS. The basic approach consists of initially creating a system free of PIS, a "clean" system. A snapshot of the clean system is considered the baseline of the system. The snapshot depicts the file

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

system of the target host. Once the baseline is recorded, some action is performed to potentially release PIS on the target host. The action could be, for example, surfing the World Wide Web. A snapshot would be taken at regular intervals. Ad-Aware was the most popular PIS removal tool, and so the authors chose to assess Ad-Aware using forensic and static analysis techniques. Through using their technique, Boldt and Carlson found that Ad-Aware produced false positives as well as false negatives.

2.6. Short Sequences of System Calls

Hofmeyr et al [17]. Propose a technique that monitors system call sequences in order to detect maliciousness. First, profiles must be developed that represent the normal behaviour of the system's services. "Normal" in this technique is defined in terms of short sequences of system calls. Although intrusions may be based on other parameters, these other parameters are ignored. Hamming distance is used to determine how closely a system call sequence resembles another. A threshold must be set to determine whether a process is anomalous. Typically, processes showing large Hamming distance values are anomalous. Hofmeyr et al.'s method was able to find intrusions that attempted to exploit various UNIX programs like sendmail, lpr, and ftpd.

III. METHOD DESCRIPTION

This section starts first with what Binghe is and it technology, experiment carried-out and the result obtained, followed by the description of the detection method, characteristics and some of the limitation of present Trojan detection method.

3.1 Binghe backdoor

Binghe is a backdoor program which or gives attacker a privilege to penetrate into a computer system using a tcp port connection. Backdoor Binghe is a backdoor Trojan horse program that allows unauthorized access to a compromised computer. The back door has key logging and the ability to run programs, as well as spy capabilities.

Figure 3:1Binghe application scanning interface.

3.2 Binghe Experimentation

Due to the experiment conducted using a local area network setup, we are able to detect that the Binghe uses a Tcp port 7626 for connection and we also detect that the registry key was manipulated from it default settings. Which enable hacker to connect to a computer system and manipulate the computer system on the network. As how it often happens in a networked environment, an attacker can send an unsolicited email containing an attachment of Binghe application (Trojan horse) which has a picture of a lady like a toy, which can attract an unaware user to download and click on the application thinking that is an ordinary picture. Binghe does not require long installation steps, what a user needs to do are just to click on the application and then Binghe setup.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

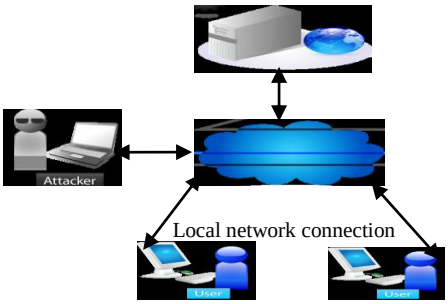

Figure 4:2 An attacker send Binghe.

This create a TCP port connection, which opens port 7626 that gives the attacker a connection after scanning the network for the IP addresses of those computer on the network. The attacker now uses this ip address to connect to a particular computer, and perform the following operation on the compromised computer system; key logging, Sending/copying of message, screen watching (spying) and even full system control.

$$S_N = \{B: |C_N \cap C_M/N\} \geq \alpha \qquad (1)$$

The Binghe uses technology of backdoor application, a backdoor opens a network tcp port for attacker to connect. It uses a client server communication mode; where the compromised (attacked computer) is made to be the server while the attacker is the client. Because a server always listen to a connection from other computers (clients).

3.2 Binghe detection algorithm

1. A Binghe has a relation B = ($N^* \cap E^*$, N_c) consists of set of network connection.
2. $\forall(N^*, E^* \in N_c) \exists N_c$ that control and then $B \rightarrow -1$ on N_c
3. Check the registry value of DWORD
4. If (B==-1)then DWORD=”default” else DWORD==DWORD

IV. A GENERATIVE MODEL

We develop an integrated framework to tackle the behavior and effect of binghe Trojan attack with the ability to detect it malicious act in the network environment, this approach looks into a specific nodes in the network as shown in figure 3.1 which Binghe is trying to have access. In view, of this we construct a standard algorithm system which is specifically designed to detect the point of precision as shown in figure 3.2. The action identify the kind of behavior introduce by Trojan. Equation (1) show that in a given set of network S_N if there is an absolute attack by Trojan in the network in one of the system there should be a tendency of affecting any other node in the network, which as a result could harm the network.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

```
Input-range of port
Output-current_status/Action
Declaration – I, s, t, p as integers
BingheNode=0  //current_status of affected node α(b)
Begin
    for  each (i=1 to n-1)      // number of nodes to scan
        for  each (N* in Nc)
            for each (α(b) to Nc)
                if (α(b)='-1' ) then Nc(i)='-1'
                        if  Nc(i)='-1' then
            While p="open"
                If  t='7626' then
                Close t;
                Close p;
                Endif
            Endwhile
                Endif
            Endfor
        Endfor
    Endfor
Return current_status
```

Figure 3.2 (Binghe detection pseudo code)

V. CONCLUSION AND FUTUREWORK

The work in this paper has provide a frame work for detection of Binghe Trojan malware which gains privileged access to the operating system while appearing to perform a desirable function but instead drops a malicious payload, often including a backdoor allowing unauthorized access to the target's computer, Through an extensive set of and experiments, we have demonstrated that using this framework increase the Trojan detection sensitivity. To improve the sensitivity further, the frame work only work for Trojan horse, which has a fixed TCP port, further research work, is required to tackle dynamic port issues and also the work does not cover Trojan horse which can attack a source code of a program.

REFERENCES

[1] Symantec Corporation "What is the difference between viruses, worms, and Trojans?" http://www.symantec.com/docs/TECH98539 Retrieved 2009- 01- 10.
[2] Michigan Information and Analysis Center Monthly Cyber Security Tips, NEWSLETTER. "Prevention and Responding to identity theft" volume 1, Issue 7, pp. 2, 2006
[3] Landwehr, C. E; A. R Bull, J. P McDermott, W. S Choi (1993). "A taxonomy of computer program security flaws, with examples". DTIC Document. Retrieved 2012-04-05.
[4] Thompson, Ken. 1984. *Reflections on Trusting Trust*. Communication of the ACM, Vol. 27,No. 8, pp. 761-763.
[5] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," in *Proceedings of ACM SIGCOMM/USENIX Internet Measurement Conference (IMC)*, pp. 41-52, 2006.
[6] Hardware Trojan horse detection using gate-level characterization Design Automation Conference, 2009. DAC '09. 46th ACM/IEEE pp. 688 – 693 26-31 July 2009.
[7] Bontchev, V. (1996). 'Possible macro virus attacks and how to prevent them'. *Computers & Security* 15(1996):595-626.
[8] Adrian Spalka, Armin B. Cremers and Hanno Langweg, "Trojan Horse Attacks on Software for Electronic Signatures" vol. Informatica **26** (2002) pp. 191-203
[9] Jamie Crapanzano (2003): "Deconstructing SubSeven, the Trojan Horse of Choice", SANS Institute, Retrieved on 2009-06-11
[10] Vincentas, "Trojan Horse in SpyWareLoop.com". Spyware Loop. Retrieved 28 July 2013.
[11] Bitdefender, "BitDefender malware and spam survey finds e-threats adapting to online behavioural trends *Published: 6 August 2009 pp. 1*
[12] Datta, Ganesh. "What are Trojans?" SecuredAid survey 30 Nov., 2011
[13] Burt, Jeffrey and Ziff Davis "HP Fewer but more Dangerous Software Security Vulnerability" eWeek.com Retrieved 2012-04-20
[14] www.bjreview.com.cn/THIS_WEEK/2012-03-23/Content_441986.htm

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

[15] Cyber Security Trend - Annual Review 2013 - Better response to cyber attacks and triaging gray events - Writing and data preparation Tomohiro Nakashima et.al by NRI Secure Technologies, Ltd. Pp. 26-27
[16] M. Boldt and B. Carlsson. "Analysing privacy-invasive software using computer forensic methods". PhD in computer science at Blekinge Institute of Technology. Pp. 1-14. January 2006.
[17] S. Hofmeyr, S. Forrest, and A. Somayaji. Intrusion detection using sequences of system calls. Journal of Computer Security, pp. 151 – 180, 1998.

BIOGRAPHY

Ahmed Aliyu is a Graduate Assistant at Department of mathematical Sciences, Bauchi State University Gadau, Itas-Gadau Local Government, Bauchi State of Nigeria. And attended Abubuakar Tafawa Balewa University Bauchi State Nigeria, for his first degree in computer science and currently pursuing a master's degree in Computer science at Liaoning University of technology, Jinzhou china

Sani Dajuma: is working with Sa'adatu Rimi College of education, Kumbotso Kano state Nigeria. He did his first degree in computer science and currently, he is undergoing a master's degree program in Computer Science and Technology at Liaoning University of Technology, Jinzhou China. He is also a member of IEEE, he has written many papers among them is the paper titled "A critical Simulation of CPU Scheduling Algorithms using Exponential Distribution; An analysis for security in web applications; Using SQL for testing database application; Design Analysis and Implementation of Semantic Web Application.etc

Bo Dai: is lecturer in School of electrical/Electronic Engineering Liaoning University of Technology he is currently an Associate Professor, his Research area include: Network Security, Intrusion Detection system, Grid Computing and Neural Network.

Usman Waziri Ahmad Aliyu is a Graduate Assistant at Department of Mathematical Sciences, Bauchi State University Gadau, Itas-Gadau Local Government, Bauchi State of Nigeria. And attended Bayero University, Kano, Nigeria, for his first degree in Mathematics and currently pursuing a master's degree in computer science at Liaoning University of technology, Jinzhou china.

Abubakar Ado Rogo: is a student in Department of Electrical/Electronic Engineering, and attended Abubuakar Tafawa Balewa University Bauchi State Nigeria, for his first degree in computer science and currently pursuing a master's degree in Computer science at Liaoning University of technology, Jinzhou, China. His research interest include: Database and information system.