International Journal of Pure and Applied Mathematics
Volume 116 No. 8 2017, 315-320
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

STUDIES ON MALICIOUS SOFTWARE

[1]G.Michael, [2]R.Karthikeyan
[1,2]Assistant Professor Dept of CSE, BIST, BIHER, Bharath University, Chennai-73
[1]micheal.cse@bharathunive.ac.in, [2]karthikeyan.cse@bharathunive.ac.in

Abstract: Malicious software, commonly known as malware, is any software package that can harm to a computer system. Malware is the type of worms, viruses, trojans, spyware, adware and root kits, etc., that steal protected data, delete the documents or add software not approved by a user. Malware is software system designed to cause damage to a pc and user. Some types of malware "spy" on user internet traffic. Examples include spyware and adware. Spyware monitors a user's location and if enabled, it will capture sensitive data, e.g., master card numbers, promoting identity theft. Adware also acquires user data,that is shared with advertisers and then integrated with unwanted, triggered pop-up ads. Worms and viruses behave differently, as they'll quickly proliferate and undermine an entire computing system. They additionally could perform unsavory activities from a user's pc while not the user's knowledge. in the wake of a virus or worm, a computing system will experience significant damage.

Keywords: Virus, Worm, Logic bomb, Trojan horse, Backdoor (trapdoor), Key loggers.

1. Introduction

Malicious software is also typically referred to as Malware. "Malicious software consists of pc viruses, worms, and trojan horses". other professionals consist of spyware, dishonest adware, crime ware, rootkits, and different unwanted software program. Malware is a collective time period for any malicious software{21-11] which enters gadget without authorization of client of the appliance. The time period is constructed from uniting the phrases 'malicious' and 'software program'. Malware is a completely massive hazard in today's computing world. It keeps to develop in capability and strengthen in complexity. Most of the malware enters the machine at the same time as downloading documents over net. Once the malicious software program finds its way into the device,[20-12] it scans for vulnerabilities of operating device and perform unintentional actions at the system ultimately deceleration down the performance of the device. Malware has capacity to infect different executable code, statistics/gadget files, boot walls of drives, and create abnormal web site guests on community main to denial of service. when user executes the inflamed document; it becomes resident in memory and infect each other record accomplished afterwards. If working device has a vulnerability, malware can also take manage of device and infect other structures on community. Such malicious packages (virus is greater popular time period) are also known as parasites and adversely have an effect on the performance of device commonly resulting in sluggish-down. Some malware is very easy to notice and defer via antivirus software.

1.1 Virus

A computer virus is a computer program which can propagate (replicate) itself without the user's consent. It spread atgeometric rate, eventually infecting the entire system and spreading to other connected system. Usually, it has malicious intent, e.g.[17-3] The virus which affects the performance of the system. Virus can be categorized as transient or resident**[1]**

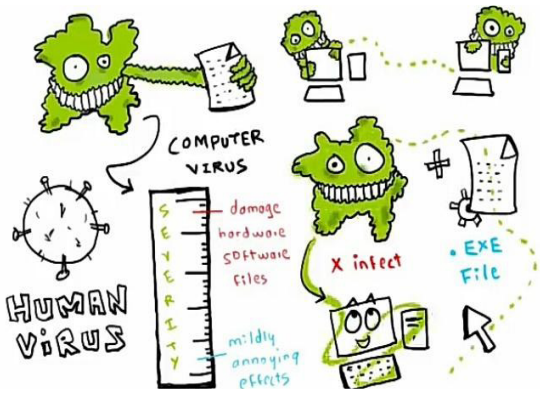

Figure 1. Computer virus

1.2 The Nature of Viruses

A virus is a bit of software which could "infect" different packages by way of modifying them; the change includes a replica of the virus program,[16-4] which could then move directly to infect other programs. Biological viruses are tiny scraps of genetic code DNA or RNA that can take over the machinery of a residing mobile and trick it into making lots of perfect replicas of the original virus. Like its organic counterpart, a laptop virus carries in its instructional code the recipe for making perfect copies of itself.[15-5] The usual virus will become embedded in a program on a computer. Then, on every occasion the infected laptop comes into contact with an uninfected piece of software, a clean copy of the virus passes into the new software. Thus, the contamination can be un fold from computer to laptop by using unsuspecting users who both swap disks or ship applications to each other over a community.[14-6] In a community surroundings, the ability to get entry to packages and gadget offerings on different computer systems affords a great lifestyle for the unfold of a virulent disease. A virus can do something that other programs do. The handiest difference is that it attaches itself to some other software and executes secretly whilst the host program is administered. Once a virus is executing, it can perform any function, inclusive of erasing files and programs.

1.3 Virus structure

A virus can be prepended or postpended to an executable program, or it can be embedded in some other fashion. The key to its operation is that the infected program, when invoked,[13-7] will first execute the virus code and then execute the original code of the program.

A very general depiction of virus structure is shown in a simple virus as Figure 19.1. In this case, the virus code, V, is prepended to infected programs, and it is assumed that the entry point to the program, when invoked, is the first line of the program.

1.4 Simple virus

Simple virus replicates itself. It is the easiest to detect. If a user launches an infected program, the virus gain control of the computer and attaches a copy of itself to another program file. After attachinga copy of itself to another program file,[12-8] virus transfers its control back to the host program, which runs normally.

The following pseudo-program shows how a virus might be written in a pseudo-computer language and affects the computer program. The ":=" symbol is used for definition, the ":" symbol labels a statement, the ";" separates statements, the "=" symbol is used for assignment comparison, the "~" symbol stands for not, the "{" and "}" symbols group sequences of statements together, and the "..." symbol is used to indicate that an irrelevant portion of code has been left implicit.**[2]**

Figure 2. Executable virus

Program

```
program virus:= {1234567;
 subroutine infect-executable:=
{ loop:file = get-random-executable-file;
if first-line-of-file = 1234567 then goto loop;
prepend virus to file;}
subroutine do-damage:=
{whatever damage is to be done}

subroutine trigger-pulled:=
{return true if some condition holds}
main-program:=
{infect-executable;
if trigger-pulled then do-damage;
goto next;}
next:}
```

1.5 Worms

Computer worms are malicious programs that replicate, execute and spread across network connection independent without human interaction. Most worms are created only to replicate and spread across a network. Consuming available computing resources. However, some worms carry a payload to damage the host system.

Network worm programs are use network connections to spread from system to system.[10-9] Once active within the system, a network worms can behave like a computer virus or it could implant Trojan horse programs or perform any number of disruptive or destructive actions.

To replicate itself, a network worm use some sort of network vehicle. Examples include the following:

- Electronic mail facility: A worm mails a copy of itself to other systems.
- Remote execution capability: A worm executes a copy of itself on another system.
- Remote login capability: A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other.

1.6 Attacks of Worms

- Deleting system files and other malicious attacks on a computer systems.
- Communicate information back to attacker e.g., passwords, other proprietary information.
- Causing a disturbance normal operation of system, thus denial of service attack (DoS) – due to re-infecting infected system.
- Worms may carry viruses with them and it can spread into many action.

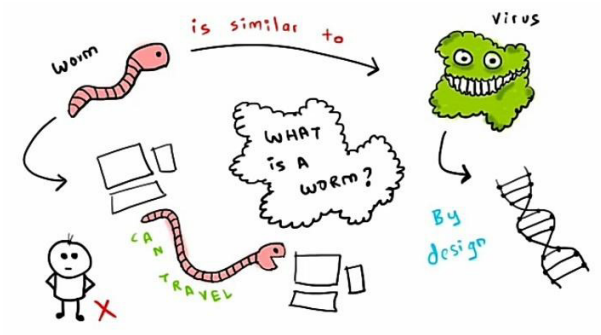

Figure 3. Worms

1.6 Logic Bomb

One of the oldest kinds of application threat, predating viruses and worms, is the logic bomb. The good judgment bomb is code embedded in a few valid programs that is set to "explode" when positive conditions are met. Examples of situations that may be used as triggers for a good judgment bomb are the presence or absence of certain files, a specific day of the week or date, or a specific consumer walking the utility. Once triggered, a bomb may additionally modify or delete records or whole files, purpose a gadget halt, or do a little other damage. A placing instance of how good judgment bombs can be hired become the case of Tim Lloyd, who was convicted of putting a good judgment bomb that value his company, Omega Engineering, extra than $10 million, derailed its company increase method, and subsequently caused the layoff of eighty people. Ultimately, Lloyd was sentenced to 41 months in jail and ordered to pay $2 million in restitution.

1.7 Trojan Horses

In computing, Trojan horse, or Trojan, is any malicious computer application that's used to hack right into a pc with the aid of deceptive users of its genuine rationale. The time period is derived from the Ancient Greek tale of the wood horse that become used to assist Greek troops invade the metropolis of Troy by means of stealth.

Trojans are typically spread by some form of social engineering, for instance where a user is duped into executing an email attachment disguised to be unsuspicious, (e.g., a recurring form to be stuffed in), or with the aid of pressure-via down load or from junk mail hyperlinks and fake pop up & Advertisement. Although their payload can be whatever, many contemporary bureaucracy act as a backdoor, contacting a controller that may then have unauthorized get admission to the affected pc.This contamination allows an attacker to access users' private statistics including banking information, passwords, or personal identity (IP address). Trojan looks for your personal information and sends it to the Trojan writer (hacker). It can also allow the hacker to take full control of your system**. [3]**

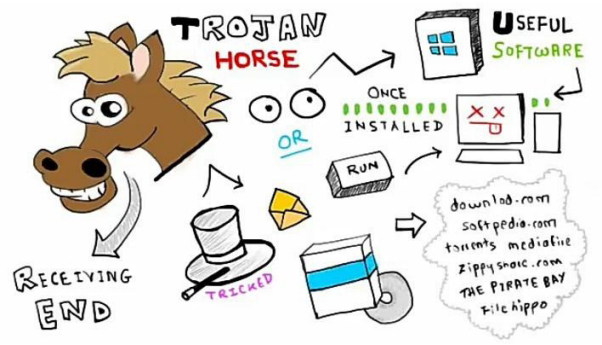

Figure 4. Trojan Horse

1.7 Different types of Trojan Horses

1. Remote access Trojan:takes full control of your system and passes it to the hacker.
2. The data-sending Trojan: sends data back to the hacker by means of e-mail.
3. e.g., Key-loggers – log and transmit each keystroke.
4. The destructive Trojan: has only one purpose: to destroy and delete files. Unlikely to be detected by anti-virus software.
5. The denial-of-service (DOS) attack Trojans: combines computing power of all computers/systems it infects to launch an attack on another computer system. Floods the system with traffic, hence it crashes.

6. The proxy Trojans: allows a hacker to turn user's computer into HIS (Host Integration Server) server – to make purchases with stolen credit cards and run other organized criminal enterprises in particular user's name.
7. The FTP Trojan: opens port 21 (the port for FTP transfer) and lets the attacker connect to your computer using File Transfer Protocol (FTP).

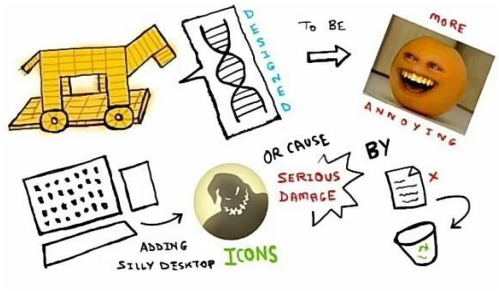

Figure 5. Trojan Attack

1.8 Zombie

A zombie could be a program that secretly takes over another Internet-attached pc then uses that computer to launch attacks that are troublesome to trace to the zombie's creator. Zombies are used in denial of service attacks, generally against targeted websites. The zombie is planted on many computers belonging presence of danger to third parties, then used to overwhelm the target internet sites by launching an overwhelming destructive attack of web traffic. Discusses zombies within the context of denial of service attacks**. [4]**

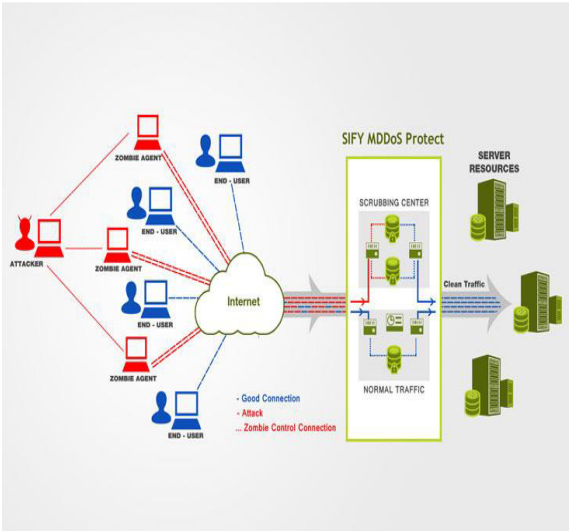

Figure 6. Zombie Attack

1.9 Backdoor

A backdoor, also known as a trapdoor, is a mystery access point right into a program that allows a person that is privy to the backdoor to benefit get right of entry to without going via the standard safety get entry to procedures. Programmers have used backdoors legitimately for many years to debug and check programs. This commonly is completed when the programmer is developing a software that has an authentication technique, or a lengthy setup, requiring the person to enter many extraordinary values to run the utility. To debug the application, the developer may additionally desire to gain unique privileges or to keep away from all the important setup and authentication. The programmer might also need to ensure that there's a technique of activating the software must something be incorrect with the authentication process this is being constructed into the software. The backdoor is code that acknowledges some unique collection of enter or is caused by means of being run from a positive person ID or by means of not likely sequence of occasions.

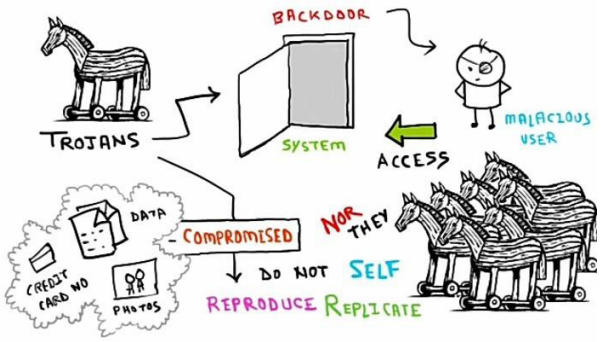

Figure 7. Backdoor(trapdoor)

1.10 Counter measures

Although the malicious software program to be had today has accelerated in sophistication and volume, the technology placed in shielding measures has additionally elevated. Today, absolutely everyone from the largest software program organizations to the smallest home networks have access to numerous anti-virus packages, updates and patches, removal equipment, and community protection.

As indicated earlier, companies such as Symantec and McAfee annually release anti-virus software in order to combat the ever-changing and increasingly "intelligent" threats. Presently, Bit defender is Anti-Virus stands as the number-one selling anti-virus protection program in the world, boasting the ability to remove viruses, worms, and Trojan horses automatically,

detecting spyware and other non-viral threats, as well as blocking more sophisticated codes even before they can enter a computer system. **[5]**Anti-virus software such as this are also regularly updated to identify and fix the newest loopholes and flaws which malicious code strive to exploit. These updates may be with no trouble downloaded by the quit person through a customizable automatic down load device located inside the program.

2. Conclusion

As software and computing continues to evolve and play an increasingly-predominant role in society, the quality and potential destructiveness of malicious code will also continue to increase. While malicious code developers continue to produce intelligent software to exploit the weaknesses of companies like Microsoft, these companies will continue to place enormous amounts of money into development of countermeasures. Whoever can stay "ahead" of the other in this game of cat and mouse will determine how the rest of society is affected. Software is indeed now commonplace amongst society's ever-increasing technological identity, being the driving force behind many routine applications and services. Unfortunately, the presence of malicious code will continually cast a darkish shadow over

References

[1]Ritstein Charles (1992), EXECUTIVE GUIDE TO COMPUTER VIRUSES, National computer security association.

[2] D.Rakesh, L.Padmalatha, PATTERN MATCHING ALGORITHM USING FILTER ENGINE AND EXACT MACHING ENGINE, International journal engineering and research Technology(IJERT) VOL.1 issue7, september-2012.

[3] Webopedia.com. Trojan Horse. Retrieved Nov 8, 2003 from website: http://www.webopedia.com/TERM/T/Trojan_horse.html

[4]"Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A
Tutorial." IEEE Communications Magazine, October 2002.

[5] "The World's Most Trusted Antivirus Solution." (no date given), Symantec Website. Retrieved March 27, 2005 from the World Wide Web: http://www.symantec.com/nav/nav_9xnt/.

[6]Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[7]Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.

[8]Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.

[9]Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.