International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 4, Number 1 (2012), pp. 9-18

http://www.irphouse.com

Analysis of Various Types of Viruses and their Remedies

Sandeep Kaur and Gaurav Pushkarna

Dept of Computer Science,
Lovely Professional University, Phagwara, India
E-mail: sandeep.khullar40@yahoo.com, gaurav.pushkarna@lpu.co.in

Abstract

This paper presents a general overview on evolution of virus, malwares and defensive employed by advanced antivirus techniques. Computer viruses gradually improve codes to make them invisible. Antivirus technologies continually follow the tricks and technologies to overcome the virus. With the help of antivirus experts design and develop new methodologies to make them stronger. The purpose of this paper is to define the last malware and prevent the computer from malware, malicious and viruses.

Keywords: Computer Virus, Computer Anti-virus, programs, malware, malicious, viruses, Trojan, computer infection.

Introduction

The recent proliferation of malicious code that spreads with virus code exacerbates the problem [11]. Virus is main problem in the security because it can easily attach itself with the files and other programs. According to Fred Cohen, “A computer virus is a program that can infect other programs by modifying them to include a possibly evolved copy of itself "[8]. A virus copies itself into an infected executable without Permission or knowledge of a user [4].Given the widespread use of sharing in current computer systems, the threat of a virus carrying a Trojan house [5] is significant. Like Trojan horses [13], computer viruses are instances of *malicious logic* or *malicious programs*. Although a considerable amount work has been done in implementing policies to protect against the illicit dissemination of information [3]. And many system have been implemented to provide protection from to attack [1].little work has been done in the area of keeping information entering an area from causing damage[2].The antivirus expert usually follow the latest procedure used in malwares and attempt to overcome them and to solve these problems firstly know about the

previous methods. The antivirus techniques focus on detection of the static signatures of viruses. These procedures are valuable in their own they do not address the dynamic of a virus disease with in context of the fundamental system. The anti-virus specialists generally follow the new techniques used in advanced malwares and attempt to overcome them, however, all the new defense techniques are not sufficient and there is an extremely necessity for more researches.[7] A computer virus is an executable program. Depend on the nature of a nature of a virus, it may cause damage of hard disk contents, and/or interface normal operation of your computer. By definition, a virus program is able to replicate itself. This means that the virus multiplies on computer by making copies of it. This replication is intentional It is part of the virus program. Viruses and worms are self-replicating programs that sometimes have the goal of damaging their hosts and arranging for copies of themselves to propagate to new hosts [8]. In most cases, if a file that contains virus is executed or copied on to another computer, then that computer will also be "infected" by the same virus. A virus can introduced to a computer system along with any software program. For internet users, this threat can come from downloading files through FTP (file transfer protocol), or referencing email attachments. A computer virus is a malware that, when executed, tries to infect other executables and alter their default behavior [6].

A virus program gives the instructions when the computer is infected. Some examples are:

- Modification of data.
- Files overwritten or damaged.
- Hard drive should be removing.
- Decrease the memory or disk space.
- A frustrating message show on the computer screen.
- Generally a computer virus consists of three modules [5].

```
    def  virus() :

infect ()

     if trigger () is true then

          payload ()
```

Figure 1: Pseudo code of computer virus

Infect defines how a virus spreads. One common infection mechanism is to modify host to contain copy of virus code. Trigger is a test to decide to deliver the

payload or not. Payload defines damage done by the virus. Trigger and payload Trigger and payload are optional. Figure 1 shows pseudo code of a virus.

```
def infect() :
        repeat k times:
 target = select_target()
            if no target then
                return
  infect_code (target)
```

Figure 2: Pseudo code of infect module [6]

Infect module selects a target to infect. Generally k targets are selected on each run. *Select_target* defines criteria by which a target is selected. The same target should not be selected repeatedly otherwise infecting the same code repeatedly may reveal the presence of the virus. *Infect_code* performs actual infection by inserting virus's code into the target. The term virus refers to malicious software that requires help from computer users to spread to other computers. Email viruses, for instance require someone to read an email message or open an attached file in order to spread. We use the term worm for infection that spread without user intervention. Because they spread unaided, worms can often spread much faster than viruses. Computer infections such as viruses and worms spread over networks of contacts between computers, with different types of networks being exploited by different types of infections. Just as it does human diseases [6] and understanding this structure is thus a key element in the control of infection.

Malicious software

Malicious software (malware) is any software that gives partial to full control of your computer to do whatever the malware creator wants. Malware can be a virus, worm, Trojan, adware, spyware, root kit, etc. The damage done can vary from something slight as changing the author's name on a document to full control of your machine without your ability to easily find out. Most malware requires the user to initiate its operation. Some vectors of attack include attachments in e-mails, browsing a malicious website that installs software after the user clicks ok on a pop-up, and from vulnerabilities in the operating system or programs. *Malware is not limited to one operating system.*

Malware types can be categorized as follows

Viruses, worms, Trojans, and backdoors seek to infect and spread themselves to create more havoc. Adware and spyware seek to embed themselves to watch what the

user does and act upon that data. Root kits seek to give full access of your machine to the attacker to do what they want.

Virus: In computers, a virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette or CD. The immediate source of the e-mail note, downloaded file, or diskette you've received is usually unaware that it contains a virus. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are benign or playful in intent and effect ("Happy Birthday, Ludwig!") and some can be quite harmful, erasing data or causing your hard disk to require reformatting.

Trojan horse - A Trojan (or Trojan horse) is a malicious program disguised as a normal application. Like Trojan horses, computer viruses are instances of *malicious logic* or *malicious program* [9]. Trojan horse programs do not replicate themselves like a virus, but they can be propagated as attachments to a virus. Trojan horses cause damage or compromise the security of the computer. Trojan horses spread when people are lured into opening a program because they think it comes from a legitimate source. But while it runs, it could be allowing "back door" access to the computer by hackers or destroying files on the hard disk. Often an individual emails a Trojan horse-it does not email itself-and it may arrive in the form of a joke program or software of some sort. A recent Trojan horse came in the form of an e-mail that included attachments claiming to be Microsoft security updates, but turned out to be viruses that attempted to disable antivirus and firewall software.

Trojan horses can be included in software that you download for free. Never download software from a source that you don't trust. For protection against a Trojan horse, users must be suspicious of any unknown program and be sure it is safe before running it.

Worms: A worm is similar to a virus. A worm is designed copy itself to one computer to the other computer. In the other words Is a self-replicating computer program, similar to a computer virus but unlike a virus which attaches itself to, and becomes part of, another executable program, a worm is self-contained and does not need to be part of another program to propagate itself [9].Worms are effective at using e-mail system. Worms reside in memory and usually remain unnoticed until their effects become apparent, overwhelming. When new worms are unleashed, they spread very quickly, clogging networks and possibly making you wait twice as long to view Web pages on the Internet. This is called a Denial of Service Attack. The worm may do damage and compromise the security of the computer. Once a worm is in a computer system it can travel alone. Because worms don't need to travel via a "host" program or file, they can tunnel into the system and allow another person to take control of the computer remotely.

Backdoor: it is a secret point into a program that allows someone that is aware of the

backdoor to gain access without going through the usual security access procedures. Programmers have used backdoors legitimately for many years to debug and test program. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. However, attackers often use back doors that they detect or install themselves, as part of an exploit. In some cases, a worm is designed to take advantage of a back door created by an earlier attack.

Today's top Malwares

There are so many different types of viruses, which is the most widespread computer viruses today? It is a difficult to say because The most viruses have a defined and relatively short life cycle; they appear on the scene with a bang, doing considerable damage, but Then as defensive methods are working just as quickly disappear from the radar scope. From the Trends Micro smart protection network Report for Oct, 2011, analysis identified malware and other potentially unwanted programs including spyware and adware; since Oct, 2011. This reflects the rate at which Web sites are being compromised or created for the purpose of spreading malicious content. Often this number is higher when Web-based malware is in circulation for a longer period of time to widen its potential spread and increase its longevity.

BKDR_EXDEPH.A: This backdoor is related to the spammed message about the Gaddafi Death video. Upon execution, these backdoor drops open a .JPG file to trick users into thinking that the executed file is justifiable and to hide its execution in the background. It contains a picture of Gaddafi. This backdoor arrives as an attachment to email messages spammed by other malware/gray ware or malicious users. It adds registry entries to enable its automatic execution at every system startup. It opens a hidden Internet Explorer window. However, as of this writing, the said sites are inaccessible.

BKDR_IRCBOT.DAM: This malware arrives as a Gaddafi death video spam purporting to come from CNN. When executed, this backdoor sends specific information to the remote server. This backdoor downloads an updated copy of itself from a certain website. This backdoor executes then deletes itself afterward.

RTKT_DUQU.A: This malware is possibly connected with DUQU malware. This Trojan arrives as a dropped file of another malware. It also arrives with certain files. This Trojan is registered as a service that enables it to automatically execute during startup. This Trojan may be dropped by other malware. It arrives as a component bundled with malware/gray ware packages

TROJ_DUQU.DEC: This malware is possibly connected with DUQU malware, which shares code similarities in STUXNET malware. This Trojan is decrypted and loaded by RTKT_DUQU.SME from **TROJ_DUQU.ENC:** It finds processes related to antivirus programs running in memory. If no match is found, it creates a process of *lsass.exe* then patches it with the malware code. However, if any of the said processes

is found, it creates a new process of the reference file and patches malware code into it. It may also use processes to inject its code if the process name matches and if the malware is unable to determine the file path. It hooks APIs to load a component in memory, "sortxxx.nls". It connects to an IP address to contact its C&C server. It enables remote attackers to execute arbitrary commands in the affected system including downloading other malicious files. It also reads any certain files to get configuration settings.

TROJ_DUQU.ENC: This malware shares code similarities with the STUXNET malware. This is the Trend Micro detection for the encrypted .DLL files of TROJ_DUQU malware family. The malware RTKT_DUQU.SME is responsible in decrypting and loading TROJ_DUQU.ENC. The result of this routine is a .DLL file detected by Trend Micro as TROJ_DUQU.DEC. This Trojan may be dropped by other malware.

TROJ_SHADOW.AF: This malware is possibly connected with DUQU malware, which shares code similarities in STUXNET malware. This Trojan is executed using certain parameters. It finds certain processes, all of which are related to antivirus programs, running in memory to patch said processes with the malware code. If no match is found, it creates a process that it patches with the malware code. It hooks certain APIs to collect system information. This Trojan may be downloaded by other malware/gray ware/spyware from remote sites. It may be unknowingly downloaded by a user while visiting malicious websites.

BKDR_R2D2.A: This backdoor log keystrokes when using certain Internet Browsers. It is capable of listening to and recording conversations from certain applications. It also gathers certain information. It attempts to connect a remote IP address. It receives commands from a remote user and performs certain actions. This backdoor may be dropped by other malware.

J2ME_JIFAKE.AA: This Trojan may be downloaded using malicious QR codes. Once the malicious QR code is scanned, the user will be redirected to a URL where the malicious file can be downloaded. This Trojan disguises itself as *Jimm Application*, a mobile client for *ICQ*. This malware may send a pre-defined SMS message certain premium rate numbers.

ANDROIDOS_JIFAKE.E: This malware arrives as a Trojan zed application named Jimm Application (an instant messaging client for ICQ network). It sends SMS messages to premium-rate numbers thus the user is billed for these subscriptions. This Trojan may be downloaded using malicious QR codes. Once the malicious QR code is scanned, the user is redirected to a URL where the malicious file can be downloaded.

ANDROIDOS_FAKEBROWS.A: This malware uses social engineering methods to lure users into performing certain actions that may, directly or indirectly, cause malicious routines to be performed. Specifically, it disguises as a mobile web browser

Opera Mini. Once the user agreed with the services of the fake browser, it sends text messages to premium numbers. This Trojan may be unknowingly downloaded by a user while visiting malicious websites. It may be manually installed by a user. It bears the file icons of certain applications to avoid easy detection and consequent removal.

J2ME_FAKEBROWS.A: This malware uses social engineering methods to lure users into performing certain actions that may, directly or indirectly, cause malicious routines to be performed. Specifically, it disguises as a mobile web browser Opera Mini. Once the user agreed with the services of the fake browser, it sends SMS messages to premium numbers. This application disguises itself as the mobile web browser, *Opera Mini*. While running, it checks if the mobile phone uses any of the specific service centers .If it uses any of these, it proceeds to sending SMS to a number encoded in *data.res*. It sends the message *"424626 357 OX"* to specific premium numbers via SMS. This Trojan may be unknowingly downloaded by a user while visiting malicious websites. It may be manually installed by a user. It bears the file icons of certain applications to avoid easy detection and consequent removal.

ANDROIDOS_ANSERVER.A: This is the first known Android malware that reads blog posts and interprets these as commands. It can also download and install additional applications, therefore further compromising the affected device. This malware gathers specific information from the infected device. It connects to a malicious URL to send the gathered information and get an XML configuration file. This backdoor may be unknowingly downloaded by a user while visiting malicious websites. It may be manually installed by a user.

OSX_REVIR.A: This Mac malware disguises itself as a harmless document by dropping and executing a non-malicious .PDF file onto the affected system. This Trojan connects to a certain website to download and execute a malicious file detected by Trend Micro as OSX_IMULER.A. This Trojan may be unknowingly downloaded by a user while visiting malicious websites. It executes the downloaded files. As a result, malicious routines of the downloaded files are exhibited on the affected system.

Preventions

- Install a good firewall.
- Install an anti-virus program, even though it will only provide limited protection.
- Install anti-malware, or better yet install robust anti-Trojan software in addition. Ordinary anti-malware programs can be simply disabled by the Trojan.
- Be very careful with email, email attachments or files of any kind.
- Be very careful about strange or unexpected popup windows announcing that you need to download or install something.

Advanced antivirus techniques

In the antivirus techniques we highlight the two advanced antivirus techniques:

Digital immune system: it is a comprehensive approach technique which is developed by the IBM [KEPH97a, KEPH97b]. It is a sufficient technique to control the problem of the virus with the updating of the antivirus every month. The digital immune system is to remove the virus from the system as soon as it was introduced. It capture the virus when the virus comes into the system and adds detection and shield the virus and remove that and send the information to the antivirus so it cannot passes throughout the system.

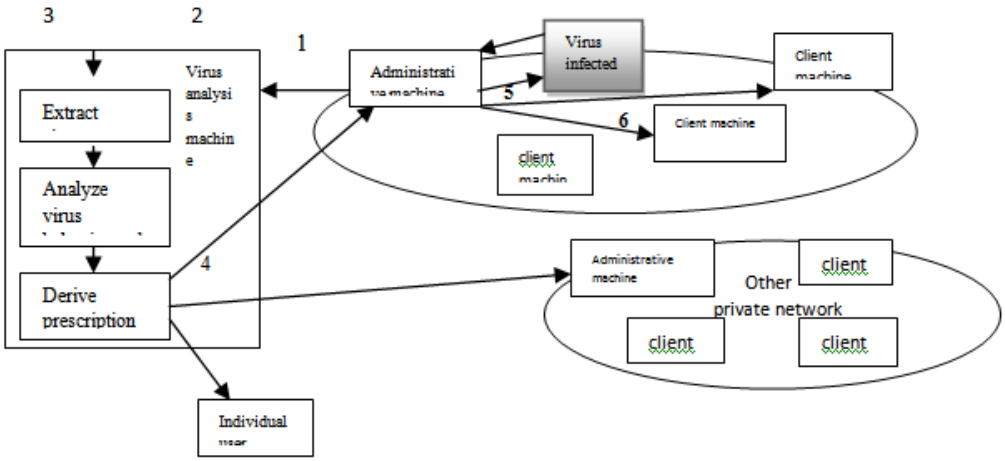

Figure: digital immune system

- In the first step the monitoring program forward the program to the administrative machine with an organization.
- The administrative machine encrypts the sample and sends it to central virus machine.
- This machine creates an environment for the infected programs can run for the analysis. This machine produces a prescription for identifying and removing the virus.
- The result prescription is sent back to the administrative machine.
- The administrative machine forwards the prescription to the virus infection.
- The prescription is send to the other clients in the organization.
- Subscribers in the whole world receive antivirus updates so that they protect their system from the new virus.

Behavior-blocking software: The behavior- blocking software integrates with operating of a host system. It monitors the program behavior in the real time for the malicious actions. In the monitored behaviors the following steps are added.

- Its attempts the open, view, delete, modify the files.

- It formats the disk drivers.
- It's also modifying the logic of the executable macros. provide the advantage hover such established antivirus detection technique as fingerprinting or heuristics

Reducing Chances of Infection in system

To make yourself less of a target for virus infection, take the following steps:

- **Restrict your file downloading to known or secure sources.** The surest way to catch a virus is to download an unknown file from an unknown site; try not to put yourself at risk like this unless you absolutely have to.
- **Don't open any e-mail attachments you weren't expecting.** The majority of viruses today arrive in your mailbox as attachments to e-mail messages; resist the temptation to open or view every file attachment you receive.
- **Up-to-date anti-virus program or service.** Antivirus programs work; they scan the files on your computer (as well as new files you download and e-mail messages you receive) and check for any previously identified viruses. They're a good first line of defense, as long as you keep the programs up-to-date with information about the very latest viruses and most antivirus programs make it easy to download updates.
- **Enable macro virus protection in all your applications.** Most current Microsoft applications include special features that keep the program from running unknown macros and thus prevent your system from being infected by macro viruses.
- **Create backup copies of all your important data.** If worse comes to worst and your entire system is infected, you may need to revert to non infected versions of your most critical files. You can't do this unless you plan ahead and back up your important data.
- **Exercise caution** when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site
- **Delete chain emails and junk email** Do not forward or reply to any to them. These types of email are considered spam - unsolicited, intrusive messages that clog up the inboxes and networks.
- **When in doubt, always err on the side of caution** and do not open, download, or execute any files or email attachments. Not executing is the more important of these caveats. Check with your product vendors for updates for your operating system, web browser, and email.

Conclusion and future recommendation

In this paper we discuss the categories of the computer virus and top ten latest viruses and the antivirus techniques to protect the system from the virus. Many systems have been implemented to provide protection from to attack by the viruses [10] little work

has been done in the area of keeping information entering an area from causing damage[12] We also discuss some steps to protect the system or reduce the chance of virus in the system. In the future we will make a program to remove the virus and protect the system from the virus. Although the antivirus software attempt to become updated and overcome the malware threats, however we have to accept that virus authors are one step more ahead, because they decide how to attack first and antivirus technologies have to only defense against their attack. Therefore computer needs more researches and investigation to guess or find the new upcoming threats.

References

[1] BD Gold, R.R Linde, R.J peeler, M Schaefer, J. F. Schied and P.D. Ward; A Security retrofit of VM/370 in National Computer Conference Pages 335-344 AIFIPS, 1979.
[2] D. E Denning: cryptography and data security Addison Wesley, 1982.
[3] D.E Bell and L J laPadula: Secure computer system mathematical foundation and model the MITRE Corporation, 1973 cited in many papers.
[4] E.Daoud and I. Jebril, "Computer Virus Strategies and Detection Methods," Int. J. Open Problems Compt. Math., Vol. 1, No. 2, September 2008.
[5] J.P Anderson; Computer Technology planning study technical Report ESD-TR-73-51, USAF Electric system Division, Oct, 1972, cited in denning.
[6] J. Aycock, "Computer Viruses and malware," Springer Science Business Media, 2006.
[7] Rad Babak, Bashari Maslin, Ibrahim Suhaimi "Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey", International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011.
[8] F. Cohen, "Computer viruses: theory and experiments, "Computer Security, 6(1):22-35, 1987.
[9] Fosnock Craig "Computer Worms: Past, Present, and Future," East Carolina University 2005.
[10] G J Popek, M Kampe, CS Kline, A Stoughton, M. urban, and E J Walton: UCLA Secure UNIX in National Computer Conference AIFIPS, 1979.
[11] Helen Martin, editor. The Virus Bulletin: Independent Anti-Virus Advice. World Wide Web.
[12] K.J Biba: Integrity considerations For Secure Computer System USAF Electronic System Division, 1977 Cited in Denning.
[13] P. Denning, "The Science of Computing: Computer Viruses," *American Scientist* **76**(3) (May 1988) pp. 236-238.