

Data security from malicious attack: Computer Virus

Narendra Kumar Tyagi(Asst.Professor)
DCE.Khentawas,Gurgaon
narendratyagi21@gmail.com

Abhilasha Vyas(Asst. Professor)
DCE.Khentawas,Gurgaon
abhimeenu2001@gmail.com

Abstract:

This paper is a hard work of theoretical and practical research work defending against computer virus and designing beneficial computer viruses for efficient processing specially in parallel processing. The damage, attack and detection had been the main research areas till now, but I am asserting my research scope to “limiting of transitivity, functionality, and sharing” is the only `perfect' defenses.

Key words: artificial life, transitivity, security measure, sharing, transitivity, Malware

Introduction:

The results of several experiments and continuous prolonged work established that viruses could spread, without any obstacle. The first computer virus called “Creeper”, came into existence in the early 1970s on the ARPAnet[1]. It spreads across the network and taunts its victims. The first malicious personal computer virus, which appeared in 1982, was called “Elk Cloner”. The virus can enter in the most `secure' computer systems and widespread and do unlimited damage without any effort on the part of the creator of virus. Many of the defenses that could be developed in a short order are not effective against a serious attacker. The best defenses are limited transitivity of information flow, limited functionality, and limited sharing. It is established that limited sharing, may cause the information flow in a system to form a partially ordered set of domains. It is proven that limiting of transitivity, functionality, and sharing are the only `perfect' defenses. A defense based upon complexity against viruses is possible.

The viruses could `evolve' into any result, thus creating a disastrous problem in detection and correction. Sloppy programming creates opportunities for viruses to spread, there is positive outcome with viruses is greater security measures and a good written application programming code. It may tighten the connection between computer viruses and artificial life. The viruses could be a very powerful tool in parallel computing.

What is a Malicious Attack?

The software programs which are particularly designed to spread from one computer system to another computer system by interfering with computer operations are the computer viruses. The virus can also spread through downloads from the internet they can be totally hidden in the software or other files or programs [2]. Computer viruses most easily spread by attachments of funny images, greeting cards, or audio and video files in e-mail messages or by instant messaging messages. So it is not advisable to open an e-mail attachment without knowing the sender or expectation of getting the e-mail attachment. New icons appear on the desktop which the user never desired. Some times the strange music /sound plays from the speakers autonomously which is uncontrolled. A program disappears from the computer even though you did not intentionally remove the program.

Symptoms of virus infected computers:

On suspicion a few indications may show that a computer is infected like –

- The system may lock anytime and will not respond. The system every time restarts after a crash.
- The system may not run in the usual pattern and restarts on its own.
- The user may be puzzled with a distorted menus and dialog boxes. The user may be surprised by getting unwanted error messages.
- Applications on the computer may not work as desired. The drives may not be accessible.
- Some times user is unable to print anything as desired.
- Double extension on an attachment of recently opened, such as a .jpg, .vbs, .gif, or .exe extension are usual.
- Most surprisingly the anti-virus program may not be restarted on being disabled without any reason. It may be the user fails to install / run an antivirus program. The infected file makes duplicate copies of itself. It may sometimes use up all the free space on the hard disk[3].
- Any copy of the infected file may be sent to all the addresses in an e-mail address list.
- Reformatting of the hard disk can be done by the computer virus and this may delete files and programs.
- The security of the system goes on high risk due to computer virus by enabling intruders to access the system or the network.

Different forms of electronic infections: The most common electronic infections are:

Viruses - A small piece of software that infects real programs fall in the category of viruses. A virus can attach itself to a program like a spreadsheet program. When the spreadsheet program runs, the virus runs too. It reproduce by attaching to other programs.

E-mail viruses – this type of virus goes on in the form of attachment to e-mail messages and replicates itself by mailing itself to many targets in the victim's e-mail address. Some e-mail viruses launch when the user view the infected messages in the preview pane of e-mail software.

Trojan horses – It is a computer program that claims to do one thing but instead doing so in real it damage when the user run it. It may erase the hard disk. Theses do not replicate automatically they do not reproduce by infecting other files nor self replicate like worms.

Worms - A small fragment of software which uses holds computer and uses network to replicate itself falls in this category. A duplicate copy of the worm search the security hole in the network to reach to another system very keenly and starts replicating from there. It has the ability to self-replicate, and can lead to negative effects on the user system. They are detected and eliminated by ant viruses softwares. Examples: Lovgate.F, Trile.C, PSWBugbear.B, Sobig.D, Mapson.

Resident Viruses - This virus dwells in the RAM memory and remain there permanently to overcome and interrupt all of the operations executed: corrupting files and programs which are opened, closed, copied, renamed or updated. Examples: CMJ, Randex, Meve, and MrKlunky.

Direct Action Viruses - They replicate and take action when executed on meeting a specific condition, the virus will infect files in the directory or folder or directories in the AUTOEXEC.BAT file PATH. The reason behind it is this batch file always located in the root directory of the hard disk and on booting the computer carries out certain operations.

Overwrite Viruses - They delete the information contained in the files that they infect, rendering the files useless. Examples: Trj.Reboot, Trivial.88.D, Way.

Boot Virus - These viruses affect the booting part of hard disk in which information is stored together with a program that makes it possible to boot the computer. Examples: Polyboot.B, AntiEXE.

Macro Virus - These infect the files which are created using certain applications or programs containing macros[4]. They automate the operations to perform as a single action; Thus save the user from carrying them out one by one. Examples: Bablas, Relax, Melissa.A, O97M/Y2K.

Directory Virus - They divert the root which indicates the location of a file by executing a program having extension .EXE or .COM infected by a virus. The user unknowingly runs the virus program, though the original file and program are already diverted by the virus.

Polymorphic Virus - They encode themselves in a many ways using different algorithms and encryption keys when ever they infect a system. Examples: Satan Bug, Elkern, Marburg, and Tuareg.

File Infectors - These viruses infect executable files with an .EXE or .COM extension. On running these programs, the virus is automatically creating the damage. Most of the viruses fall in this category and they infect most of the files they can be varied in types.

Companion Viruses - These viruses are like resident or direct action types. Once they get into the system they "accompany" the other files that already exist to carry out their infection routines. These viruses wait in memory until a program is run by making copies of them. Examples: Asimov.1539, Stator, Terrax.1069

FAT Virus - The part of a disk used to connect information and vital part of the normal functioning of the computer infected by the FAT virus. This virus attack is very dangerous because this prevent access to certain sections of the disk where important files may be stored. It may lead to information losses from files or directories.

Rootkit - A rootkit is a program designed to hide processes, files, or registry entries. In "modern" worms it's used to hide the worm from the computer user.

Logic Bombs - These are not viruses in a real sense as they do not replicate. They mask certain segments of other programs. They destroy data on meeting certain condition on the computer.

Status for Computer Virus as reported in 2008–

The number of virus detected (as counted cumulative found by a filer) was about 200,000 which decreased (3.3%) from 206,000 in April, 2008. The reported number of virus (counted as aggregated same type of viruses and variants coubnted on the same day as how many viruses are found by the same filer on the same day) was 1,737 in May, 2008 which increased from 1,703 in April, 2008. The worst detection number of virus was fallen on W32/Netsky with about 180T; W32/Mywife with about 0.6T and W32/Mytob with about 0.47T were ranked the second and the third, respectively.

Detection Number of Virus about 200T(206T) -3.3%

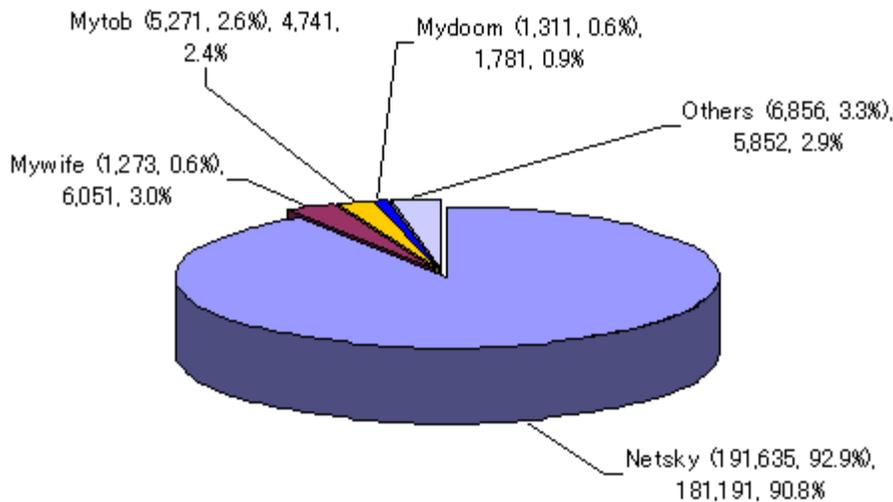


Fig: Detection of Virus about 200T (206T) Kaspersky Lab,2008

Reported # of Virus 1,737 (1,703) +2.0%

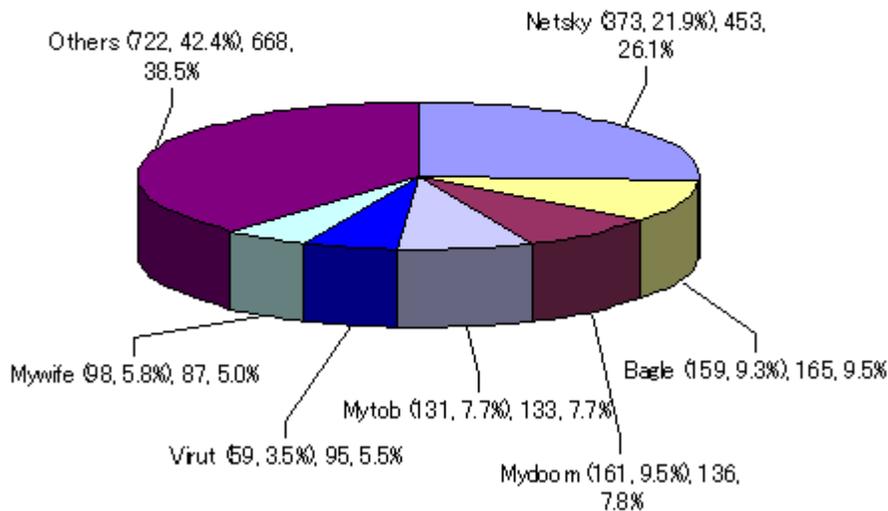


Fig: Report Kaspersky Lab,2008

The first half of 2008 confirmed the predictions about the evolution of malicious programs, namely:

- Continuing evolution of so-called Malware 2.0 technologies
- Evolution of Rootkits
- Return of file viruses
- Attacks on social networking sites
- Threats for mobile devices

The most notable malicious programs was the Storm worm (classified by Kaspersky Lab as Zhelatin) which remains in the vanguard of Malware 2.0. These developments lead to virus functions to a range of backdoors and worms, rather than the creation of new file viruses.

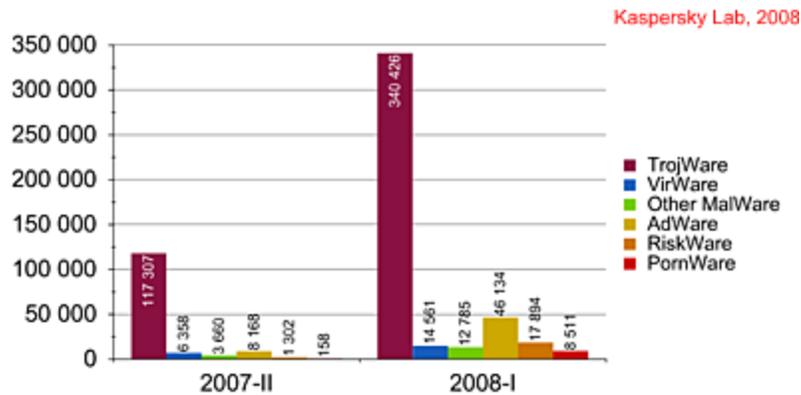


Fig: Report Kaspersky Lab, 2008

Nowadays viruses are not restricted to simple file infectors rather, they are powerful botnet components designed to steal user data. Examples are Alman, the Fujack, Allaple and Autorun worms. These programs caused infections around the world. It concludes that virus functionality will continue to backdoors and worms in future too. The Virus writers have shifted from searching for vulnerabilities in the social networking sites, simply learning to send messages from "friends" which contain a link to infected websites. MySpace and Orkut are the examples of such sites. The users in Russia are attacked by worms and Trojans which spread via Odnoklassniki.ru and V Kontakte a quite later period. Instead of attacking smartphones, the virus writers changed their working style and specialized in Trojan programs for J2ME (capable of running on almost any mobile phone). During the first six months of 2008, 440,311 programs were included to the antivirus database, against the 136,953 programs in the previous half year. Total number of new programs (1H 2007 and 2H 2008) detected

Programs detected	2H 2007	1H 2008	2H 2007%	1H 2008%	Change	Growth
TrojWare	117307	340426	85.65%	77.31%	8.34%	190.20%
AdWare	8168	46134	5.96%	10.48%	-4.51%	464.81%
RiskWare	1302	17894	0.95%	4.06%	-3.11%	1274.35%
VirWare	6358	14561	4.64%	3.31%	1.34%	129.02%
Other MalWare	3660	12785	2.67%	2.90%	-0.23%	249.32%
PornWare	158	8511	0.12%	1.93%	-1.82%	5286.71%
All programs detected	136953	440311	100.00%	100.00%		

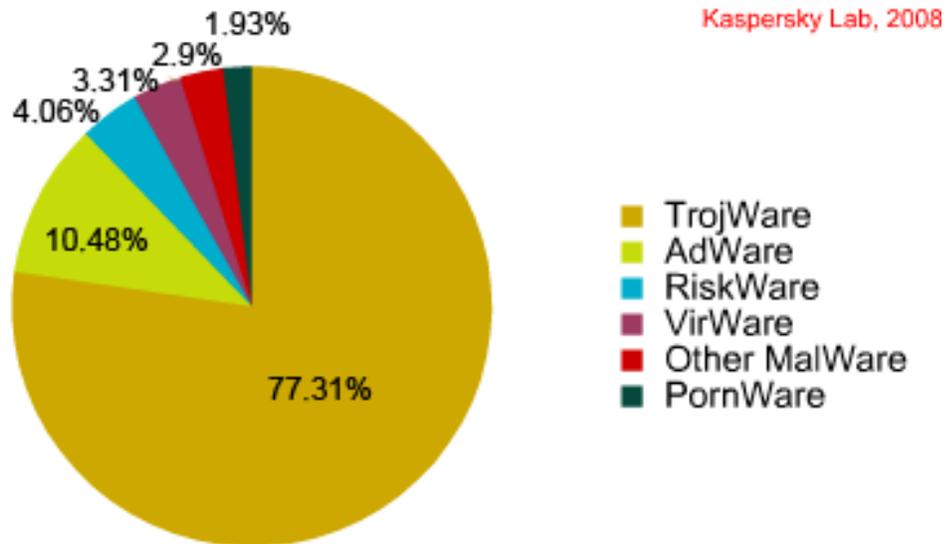


Fig: Distribution of programs detected by class

Data shows, the overall number of threats detected in the first half of 2008 tripled in comparison to the previous half year. The statistics used in this report were generated using the number of records added to the Kaspersky Lab antivirus databases in the first half of 2008. During the first half of 2008, Kaspersky Lab identified more than 5,000,000 unique files. The 440,000+ records which were added to the antivirus database detect all the threats present in these files.

Defense against viruses:

There is no defense better than a comprehensive security strategy that embraces user education, crisis-response teams, and technologically sound security measures including, but not limited to, those that relate specifically to the threats posed by viruses and worms. Protecting computers against viruses and spyware should be done before start using any program on it. The vital survey [5] [6] and the deep search suggests three modes to opt defense against the malicious viruses.

1. **Antivirus Software:** Anti-virus software is a necessity and most computers come with some form of anti-virus program already installed. It is necessary to set the automatic update feature of Antivirus, so as to add new coming virus definitions into Antivirus database. These require time to time new updates for not to let their protection lapse. Firewalls prevent uninvited visitors from the Internet from accessing user's computer. They also keep an eye on which programs on user's computer make Internet connections. Firewall attempts to probe the user computer. Windows XP has half a firewall built in but it monitors only incoming traffic and therefore is of no help in warning about programs on user computer that call up Internet sites without notifying. Firewall comes along with a variety of other programs. Example: "ZoneAlarm", etc. A firewall warns if something on system tries to call out and alert to many Trojans and Spyware. Example:

“AdAware” and “Spybot”. Proper defense of the user computer can be the appropriate configuration of the system and regular application of the security.

2. **Virus Removal:** Tools are designed, to remove the virus from the computer including spyware. Some viruses and spyware are designed to reinstall themselves when they are detected and removed. It is concluded that updating computer and using free, trial-period, or low-cost antivirus tools, permanently remove and prevent unwanted software.

Steps for the removal of viruses:

- a. Install the latest updates.
 - b. If using antivirus software; update software and then scan thoroughly the computer. If not having antivirus software, subscribe to a service and scan system.
 - c. Download, install, and run the Malicious Software Removal Tool. This tool does not prevent viruses from infecting your system; it helps to remove existing viruses.
3. **Virus Prevention:** It becomes very crucial to safe guard the system[7] from the malicious software programs, though sometimes it becomes overhead. The thorough study and survey paved the suggestion by the famous quote “Prevention is better than cure”. Limiting of transitivity hinders upto very high extent the malicious attack of the virus. The reason behind it is that while performing a transaction with so many messages, emails or file transactions, the maximum chance becomes to invite the unwanted attack from the virus. Functionality and sharing are the most important part in the series of prevention against virus. While sharing a file document to a malicious or maligned file or directory infected by a virus, chances are to get the similar infection of virus. Steps for virus prevention: Get good anti-virus software e.g. one of the below.
Recommended anti-virus software:
 - AVG - my most recommended Antiv Virus software.
 - Norton Anti-virus
 - McAfee Anti Virus
 - Sophos Anti Virus

Be sure to regularly update 'virus definitions' e.g. once per week. Install a standard quality Firewall. Some firewalls are good, some are bad. Reliable and standard quality firewall are the best selection. FREE “ZoneAlarm” is a good suggestion for the same. Install an anti-spyware application: It is very important to be aware from any spyware software problem that could attack the system very saliently. It is suggested to install a good antispysware. “Spybot” - Search & Destroy is available free. Email Attachments: Beware of attachments. Never open email attachments which are not expected. Viruses come with some very nasty messages to trick the user into opening the attachment e.g. *"Your email won the mega lottery, see attachment for details"*. The virus may come from

an email address the user recognizes e.g. from admin@userDomain.com (where 'user domain' is the domain name that the user use). When the user find a .zip attachment and open it – he must be sure that it doesn't contain a file with one of those extensions. Like .gif, .exe, etc.

Conclusion

The new threats are having a geometric progression, with threats having a reduced life span. It is concluded that proper defense of the user computer system involves the appropriate configuration of the system and regular application of the security & updating computer and using free, trial-period, or low-cost antivirus tools, permanently remove and prevent unwanted software. Only a few out of many new Trojans detected each day, continue to pose a threat to users after every week, month or year. The majority of antivirus companies will be capable of dealing with the issues. Good antivirus software coupled with central incident management in controlling the virus problem are very effective.

This Paper is focused on the causes of vital changes in virus prevalence. I found that antivirus softwares do not play major role in change because they chose the way in specific virus and class of viruses interact with computing environment. The spread of boot viruses is usual, which is the expected behavior of viruses in any population. Using 32-bit operating systems (like OS/2 and windows) cause a decrease in the prevalence of all DOS viruses because they viruses can be written for and spread by the operating systems. The decrease in DOS virus is due to the features that current DOS viruses use to spread changed in the current operating systems.

Infact efforts have to be directed in the direction of early detection of threats to solve problems. Till now it was possible to react to new threats in a couple of hours. The effort should be mounted on counting the window in seconds. So it is suggested that there is a need to identify new malicious code on the Internet – which means at any point around the globe. Now analyze it, release protection, and deliver it to the end user. Main assertion of the research scope is to “limiting of transitivity, functionality, and sharing” which is the only `perfect' defenses.

References:

- [1] White paper “The Evolution of Viruses“ (website MaximumPC.com.)
- [2] Charlie Kaufman, Radia Perlman, and Mike Speciner, "Network Security: Private Communication in a Public World," Prentice-Hall, 1995
- [3] James Riordan and Bruce Schneier, "Environmental Key Generation Towards Clueless Agents", in G. Vinga (Ed.), Mobile Agents and Security Springer-Verlag, Lecture Notes in Computer Science No.1419, 1998
- [4] Symantec's Macro Virus Protection, described on the Web at <http://www.symantec.com/education/var/modules/m5tab5i.html>

[5] J.O. Kephart and S.R. White, "How Prevalent Are Computer Viruses?," *Proceedings of the Fifth International Computer Virus and Security Conference*, March 12-13, 1992, New York, pp. 267-284.

[6] P.S. Tippet, "The Kinetics of Computer Virus Replication: A Theory and Preliminary Survey," *Safe Computing: Proceedings of the Fourth Annual Computer Virus and Security Conference*, New York, New York, March 14-15, 1991, pp. 66-87.

[7] IBM's Massively Distributed Systems home page on the World Wide Web,
<http://www.research.ibm.com/massdist>