Network Attacks: Comparative Analysis between worms and viruses.

Abstract:

Malicious programs are often mistaken for the common word of virus, whether it is a virus, a worm or even a Trojan. They all share some common characteristics that cause malicious activity resulting in disrupting or terminating a flow of processes in a computer or network system. This research essay will focus on a comparative analysis between viruses and worms to clarify how the two differ in characteristics and activities during their life cycle.

Keywords:

Viruses, worms, attacks, hacking, malicious programs.

Introduction:

In order to explain what viruses and worms are and how they work we will first look in to the history and evolution of these malicious programs. This will expose us to that they are actually different forms of malicious programs; probably an inspiration was conceived from viruses when worms were developed. There are however some characteristics that differ in both malicious programs, these will be critically evaluated. Recommendations about both types of malicious programs will also be made in the end.

Defined by Concise Dictionary of Computing, viruses and worms can be:

Viruses: “A small computer program that is capable of copying itself from one computer to another, thus emulating a biological virus that infects new hosts. Viruses are almost always written with malicious intent, and may inflict damage on the computer they infect” (1).

Worms: “A type of invasive computer program, similar to a virus but designed to infect networks rather than just individual computers” (1).

Factors promoting Malicious Programs:

There are three factors that promoted malicious programs since the 80s (2):

1. Rise in the number of personal computers. Computers were first only used by experts for scientific or business operation, however as PCs came along every small business and home was furnished with it, run by vulnerable users.

2. Computer ‘Bulletin Boards’. When games, programs, word processors and spread sheets gained popularity as downloads. There rose curiosity among users to download more and more from the internet. This gave rise to Trojans (programs that had an illicit function hidden under a normal or useful program).

3. Floppy disk boots. Early in the 80s operating systems booted from floppy drives as there were not many computers with hard disks. Floppies being very vulnerable of carrying viruses were highly exploited by malicious coders to attack personal

computers as users who had a disk infected could transfer the virus by using it on another computer.

History of Malicious Programs:

Programs with self replicating capabilities appeared theoretically as early as in the 40s, however the first program with malicious activities was ‘brain’ created by two brothers living in Lahore, Pakistan in 1986. This was the first virus that infected boot records of the floppy disk by occupying unused space (2). The table below shows the evolution of malicious programs classified as viruses and worms.

Year	Event
1949	Hungarian scientist John von Neumann – a Hungarian scientist devised the theory of self-replicating programs that provides the theoretical foundation for computers that hold information in their memory (3).
1979	At Xerox Palo Alto Research Center, engineers discover the computer "worm," a short program that searches a network for idle processors. It was designed to provide more efficient computer use; the worm is the ancestor of modern worms (3).
1983	The FBI busts a group of young hackers the "414s," who broke into several U.S. government networks, in some cases using only an Apple II+ computer and a modem (3).
1983	Fred Cohen of University of Southern California coins the term "computer virus" to describe a computer program that can "affect other computer programs by modifying them in such a way as to include a copy of itself." (3).
1986	"The Brain," is released by programmers in Pakistan known to be one of the first PC viruses ever created (3).
1987	“Christmas Tree Exec” worm had self replicating properties but was Trojan that infected the IBM network by sending Christmas cards (4).
1988	Robert Morris’s Internet worm invades ARPANET computers by disabling roughly 6,000 computers on the network and flooding their memory banks with copies of itself (3). It used TCP/IP protocols to generate a denial of service attack (4)
1988	The “Father Christmas” worm exploited the system administration flaws and utilized the DECnet protocols to allow outsiders to perform tasks on the system (4).
1994	Email system abused by the ‘Good Times’ mail that erases the recipients hard drive. This form of virus still exists in different forms (3).
1999	“Melissa” virus unleashed, that spreads through MS Outlook, infecting and distributing infected files (3).
2000	“I love you” virus, similar to Melissa sends login details of the infected

	computers to the author (3).
2001	"Anna Kournikova" virus, promising digital pictures of the young tennis star, and written using a software "toolkit" that allows even the most inexperienced programmer to create a computer virus. It mails itself to every person listed in the victim's Microsoft Outlook address book (3).
2001	“Code Red” worm infects thousands of systems running Microsoft Windows NT and Windows 2000 server software. Programmed to use the power of all infected machines against the White House Web site at a predetermined date (3).
2002	"Klez" worm -- a bug that sends copies of itself to all of the e-mail addresses in the victim's Microsoft Outlook directory. The worm also attempts to disable some common anti-virus products and has a payload that fills files with all zeroes (3).
2003	"Slammer" worm wreaks havoc on businesses worldwide, knocking cash machines offline and delaying airline flights. It holds the ranking as the fastest-spreading computer worm ever with a time of 3 hours (3).
2004	"MyDoom" worm uses "social engineering," or low-tech psychological tricks, to persuade people to open the e-mail attachment that contains the virus. It claims to be a notification that an e-mail message sent earlier has failed, and prompts the user to open the attachment to see what the message text originally said (3).

Analysing Worms and Viruses:

Worms and viruses may exploit the system to a same level achieving goals through different routes, however the main way a worm differs from a virus is that virus may be dormant on a system for a very long time until making itself known, where as a worm uses parts of the computer to stay active all the time without the user noticing it. It sits in the computer’s active memory and duplicates there until the computer’s basic functions are slowed down and the program is suspected due to performance factors (5).

Criteria for being a Virus or Worm:

A program that is called a virus falls to have features of executing itself with the capability of placing its own code in the execution path of another program. Along with this it should be able to replicate itself by replacing the existing computer files with the self infected copies of files using a host program to propagate it (6).

Sample pseudo code for a virus program (7):

```
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:}
```

A worm on the other hand is not typical in activity compared to a virus; it does require neither user nor host program intervention, like double clicking or sending outgoing emails. Worms release a document containing the ‘worm’ macro and sends copies to other computers through flaws in the computer network (6).

Worms being independent of interventions unlike Viruses:

Worms for example W32/Israz-A uses its own SMTP engine, creating copies of itself in the Windows temp folder by using filenames like Wizard.exe. The worm extract a freeware SMTP component for e.g. ossmtp.dll or vUser.exe in to the Windows system folder, collects email address from the Address Book and then sends itself as an email attachment (8).

Worms have functionalities of both Backdoors and Trojans, unlike viruses:

The variants of the worm Spybot have both the functionality of worms and backdoors. It spreads through a peer-to-peer file sharing network like that of Kaaza connecting to certain internet relay chat servers (IRC) being able to receive commands from remote users to process on compromised machines (8).

Variants of the worm like W32.HLW.Warpigs contain backdoor and Trojan functionality that attacks systems with weak administrator passwords. The Discworld.exe file performs its functionality of a backdoor Trojan by connecting to internet chat server, joining a specific channel to receive instructions through default ports 6666 and 6667 (8).

Viruses Vs Worms on Linux Systems:

Being considered a myth Linux were not considered to have been vulnerable to malicious programs. This is however not true, as long a program can be written and executed in any form, malicious programs can be created. Linux survived attacks by viruses as binary executable files or installation packages are rarely exchanged between users. Even if these files are exchanged through emails, Linux does not allow execution saving them from virus attacks (9).

However after the Admworm, Linux users are no longer safe. Network worms target mostly server machines exploiting vulnerabilities in programs that are found only from server systems such as ISC bind or Apache. Worms do not however need the root login in order to replicate, for example the Slapper worm will replicate even on a SSL-enabled Apache web server that is running under non-privileged account. All it requires is a write and execute access to the /tmp directory (9).

Viruses Vs Worms and Address Spaces:

Address space of the local network to which the infected host was connected was ignored by most worms and viruses that infected the system. Over the years worms have however gained the strength to scan not only the external addresses on the internet randomly selected, but also the internal address space. This ensures that if the local network is infected with one infection, multiple infections will be replicated (10).

Email Viruses and Worms:

The virus that shares most characteristics with a worm is the email virus. This is because it propagates itself from system to system over the internet. It is still classified as a virus as it requires a human to forward it. The way a worm works in conjunction to this is that it actively seeks out for more machines to infect and the infected acts as a launching pad for attacks on other machines using network connections (11).

Characteristic Phases both in Viruses and Worms (11):

- Dormant: the program is idle until activated.
- Propagation: the program places an identical copy of itself into other programs on the disk.
- Triggering Phase: the program activates to perform the intended functions.
- Execution: the intended function is performed.

Characteristics only found in Worms (11):

- Email Facility: a copy of itself is mailed to other systems.
- Remote execution: a copy of itself is executed on another system.
- Remote login: it has the capability of logging onto a remote system as a valid user resulting in user commands to be copied from one system to the other by establishing a connection with a remote system.
- Auto Searching: examines host tables or similar repositories of remote system addresses to search for other systems to infect.
- It may attempt to determine whether a system has previously been infected before copying itself to the system.

Conclusion:

With the growing trend of viruses and worms coming in the market to attack not only Windows systems but also Linux Systems, it is getting very hard to immune systems from attacks. The more secure a system is made, services are found by malicious coders to exploit the vulnerabilities in them. Malicious coding not being restricted by ethical boundaries posses to be a great threat with its history telling us that even though its replication may not be intended for illicit purposes, it is a skilled technology fallen in to wrong hands taking advantage of vulnerable users.

Recommendations:

Measures that can be taken to protect systems can be by reviewing government policies about cyber crime, Auditing files before being uploaded on the internet. The earlier may take time as different countries have different laws, making malicious coders get away. The Latter is suffering due to bandwidth sufferings. There still is not enough bandwidth supplied to each user that they can run tool kits that can audit files for malicious code. Abandoning or discouraging malicious coding practices in academia are not a good solution as a one should know how a system can be made vulnerable. The best solution and practice is to bring about user awareness about the ill effects of malicious programs on their system and how they can prevent it by being cautious while accessing file. Anti-virus scanners should be installed and regularly updated. In order to protect oneself a user has to be very cautious to the extent of suspecting every file accessed or imported on a network. While using either a peer to peer network or an internet relay chat server one should know what is on line to be compromised in exchange to what is being gained from them.

References:

1. Concise Dictionary of Computing. Penguin Publications
2. History of viruses: http://library.thinkquest.org/C0115901/history.htm
3. A Short History of Computer Viruses and Attacks: *Compiled by Brian Krebs.* Friday, February 14, 2003. http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26
4. History of worms: http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_2_1.html
5. Viruses and Worms. Learn the Difference Between a Virus and a Worm. Dated 21st April 2007. http://www.broadbandinfo.com/got-high-speed/security-and-patches/viruses-and-worms.html.
6. Worm or Virus...What's the Difference? By Sueann Allen. http://anti-virus-software-review.toptenreviews.com/viruses-and-worms.html.
7. Computer Viruses: theory and Experiments. http://vx.netlux.org/lib/afc01.html#p2.
8. Virus Alert: Worm Uses Own SMTP Engine to Spread. By eSecurityPlanet Staff. Dated July 10, 2003. http://www.internetnews.com/dev-news/article.php/2234041
9. Sound of Silence, by Sami Rautiainen. Senior Virus Researcher F-Secure Corporation. Information Security Technical Report. Vol. 9, No.2.
10. Worms and viruses: are we losing control? By Dr Eugene Schultz, Principal Computer Engineer, university of California-Berkeley Lab. Computers & Security (2004) 23, 179-180. Dated: 24th March 2004.
11. Cryptography and Network Security. Principals and Particles. By William Stallings. Third Edition. ISBN: 81-203-2385-8. Published by Prentice Hall.

Bibliography:

1. Comparison of Firewall, Intrusion Prevention and Antivirus Technologies. By Juan Pablo Pereira. Copyright 2006, Juniper Networks.

2. Analysis of Two recent worms. By Abiodun Akinrinola and Chris Imafidon, SCOT, University of East London. Dated: 20th August 2006. Published by Open Source Publications.

3. Defending Medical information systems against malicious software. By David E. Gobuty. Published by Elsevier. Available on www.ics-elseier.com

4. Hacking gains momentum, by Steven Hinde, Bupa, UK. Published by Computer Fraud and Security. Source: ScienceDirect.com

5. Observing Internet Worm and Virus Attacks with a small network telecope, available online at www.sciencedirect.com. Published March 2006.

6. Sober tops December virus charts. Available at science direct.com
7. The state of the hack by Pieter Claassen. Published by CounterSnipe Technologies. Dated: April 2004.
8. Network Security. December 2004 issue. ISSN 1353-4858. Available at sciencedirect.com.
9. Looking ahead- what could we do with formal modelling of events. By Peter Stephenson. Published by Computer Fraud and Security. Available at sciencedirect.com
10. Trends, codes and virus attacks – 2003 year in review, by Roger Lavenhagen, MD. Trend Micro UK. Available at sciencedirect.com
11. What is so bad about teaching virus writing? http://www.antivirus-china.org.cn/forum/zhjyzh_2003_virus/03-bingduzhizuo.doc.
12.