HALMSTAD UNIVERSITY

Network Design and Computer Management

Course Title:

Network Security

Project Title:

WORMS

Project members:

- **Tchape Philippe 841122-T099**
- **Jose Enrique Charpentier 830112-9154**

Lecturer: **Kristina Kunert**

May 2008

Table of Contents

1. **Introduction**

The purpose of our project is to get in touch with the principal terms, characteristics and topics related to worms. During the following pages we will explain a little about history, types of worms, how worms affect computers in a network and finally how to protect against worms.

According to the definition in Wikipedia, a **computer worm** is a self-replicating computer program. It uses a network to send copies of itself to other computers on the network and it may do so without any user intervention. Worms are very different from viruses. Unlike a virus, it does not need to attach itself to an existing program. It is always important to protect a network from worms because they almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. Also, worms are not only developed to serve a bad purpose; there are worms with good intent.

As we said one characteristic of a worm is that it actively seeks out more machines to infect and those machines serves as a way to attack other hosts, this is why a worm is different form a virus because it does not need human intervention to move on. In order for a worm to replicate uses some sort of network vehicles such as electronic mail facilities, remote execution capability and remote login capability

2. History

The first implementation of worms was by John F Shock and Jon A Hupp, researchers of Xerox PARC in 1978. The purpose of creating worm was to improve the performance of the network by finding idle processors on the network and assign them tasks, sharing the processing load and so improving the use of the processor across an entire network.

Shoch and Hupp originally designed the worm to find idle processors on the network and assign them tasks, sharing the processing load, and so improving the 'CPU cycle use efficiency' across an entire network. They were self-limited so that they would spread no farther than intended.

3. Types of worms

There is a wide range of worms varying from their infection technique, propagation method and their effects on the infected computer (terminal). Dangerous worms can use even more than one method. We can cite 5 main types worms, namely:

- Email worms
- Instant Messaging worms
- Internet worms
- IRC worms
- File Sharing network worms

4. How worms infect a computer

The Morris worm released in 1998 is a good example to explain how worms affect systems, this worm propagates with different techniques, after execution it discover different host known by this host checking tables and lists that were stated trusted by the host. Basically I could penetrate tables and gain access to the remote accounts. After penetration it executes a program.

It is important to differentiate worms from virus. Unlike viruses, worms do not need a host program to propagate.

Worms can propagate and attack different platforms including Unix and windows. They penetrate systems in different ways trough E-mail, web servers, browsers and file sharing. Another technique to spread is to accumulate internet addresses of host that could be vulnerable, they could adopt the polymorphic technique of viruses, they are metamorphic so can change the appearance. Finally Zero Days exploit is a characteristic of worms, mostly when they are introduce and spread the hole network community will be affected since is a new treat.

a. Email Worms

And email worm can spread worldwide in just minutes. The infection method is through infected email. It is generally in form of attachment or a link to an infected website. Usually this is done when the user opens the infected attachment or when he clicks on the link to the infected website. Nowadays, a computer can be infected by simply opening an infected email (one most not necessarily open an attachment or click on a link, but gets infected by simply opening the mail for reading). They are sent to all email addresses found on infected users' machines.

Known methods to spread are:
- MS Outlook services (or other mail client services like Eudora, Pegasus,)
- Direct connection to SMTP servers using their own SMTP API
- Windows MAPI functions

This type of worms is known to harvest an infected computer for email addresses from different sources.
- Windows Address Book database [WAB]
- MS Outlook address book
- Files with appropriate extensions will be scanned for email like strings

Be aware that during spreading some worms construct new sender addresses based on possible names combined with common domain names. So, the sender address in the email doesn't need to be the originator of the email.

b. Instant Messaging Worms

The spreading used is via instant messaging applications by sending links to infected websites to everyone on the local contact list. While sent to the contact list, the links might contain very attractive messages like "*Ben Laden has been arrested Click the following link to read more*". The only difference between these and email worms is the way chosen to send the links. Sometimes it can even place a link to an infected website on the user profile.

c. Internet Worms

These ones will scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. Attempt will be made to connect to these machines and gain full access to them. Internet worms can also scan the Internet for machines still open for exploitation. Data packets or requests will be sent which install the worm or a worm downloader. If succeeded the worm will execute and there it goes again!

d. IRC (Internet Relay Chat Client) Worms

Chat channels are the main target and the same infection/spreading method is used as above - sending infected files or links to infected websites. Infected file sending is less effective as the recipient needs to confirm receipt, save the file and open it before infection will take place. It also acts like internet worms.

e. File-sharing Networks Worms

Copies itself into a shared folder, most likely located on the local machine. The worm will place a copy of itself in a shared folder under a harmless name. Now the worm is ready for download via the P2P network and spreading of the infected file will continue.

5. Some examples of worms

Here are some few examples of worms classified as good or bad worms according to the effect they have on the network.

a. Good worms (improve the quality of the network)

- **Nachi worm**, tried to download and install patches from Microsoft's website to fix vulnerabilities in the host systems

b. Bad/dangerous worms (depreciate the performance of the network

- **Morris worm** (internet worm) was one of the first computer worms distributed on the internet. The worm was written to gauge the size of the internet. But its capacity to replicate itself has caused a lot of damage on the internet

- **Sasser worm,** The worm scans different ranges of IP addresses and connects to victims' computers primarily through TCP port 445. Sasser worm has caused the new agency Agence France-Presse having its satellite communication blocked for hours; the U.S. flight company Delta Air Lines having to cancel several trans-atlantic flights; The Nordic insurance company *If* and their Finnish owners *Sampo Bank* came to a complete halt and had to close their 130 offices in Finland; The British Coastguard had its electronic mapping service disabled for a few hours; Goldman Sachs, Deutsche Post, and the European Commission also all had issues with the worm. The X-ray department at Lund University Hospital had all their four layer X-ray machines disabled for several hours and had to redirect emergency X-ray patients to a nearby hospital.

- **Blaster worm** (also known as Lovsan or Lovesan) was a computer worm that spread on computers running the Microsoft operating systems, Windows XP and Windows 2000, during August 2003.

- **I love you worm,** is the famous VBS/Loveletter or know as well as Love bug worm this worm came in 2000 by e-mail it massively spread out to the internet because it used mailing lists and took targets so when the people read their emails it source look kind safe. This worm spread out in just one day infecting 10 percent of all computers connected to the internet. It is believe that it was written by Chris Moon

6. Protection against worms

Today network protection is consider a primary need in computer systems there is not a specific tool that will assure us 100 percent that our system will be free of malicious software, there will always be a path for these programs to spread, new viruses, worms, spyware comes to the network and cause huge damages in our system.

Even our antivirus detects the problem is too late the worm is in our computer and could move on. The best solution against this problem is prevention. We cannot allow a malicious code to enter our system.

Knowing that prevention is not enough because even with systems up to date and scan for those infected e-mails it helps to reduce the successful attacks. Removing a malicious code without cleaning up or re-installation of our system could be a really difficult task even for someone with enough knowledge in computers.

When a system has been infected the detection is the next step, after detection identify the specific worm, and remove it. If either detection or identification is not possible we need to start thinking to use our back up files, restore our system to a previous state and do a clean backup version.

This chapter focuses not on system recovery but on prevention. There are different techniques we can use to have our computers updated. It is important to have a good back up system in case of infection. Mostly all antivirus have protection against worms as antivirus and generally all kind of

treats, the important point here is to do frequent updates to have our antivirus up to date. For those that uses windows, having windows update service is a good tool for prevention. Enable automatic updates is recommended.

Other kind of protection is firewalls, routers provide firewall protection but it requires technical hands, in the other hand for personal computers there are good choices with low prices to get firewalls for personal use. In case of windows they provide now a build-in firewall for their customers that I recommend to use even for those that has previously configure a firewall in a router.

One important point is to keep away from those emails we don't know the sender and not even try to download or open any attachment with those files or open web pages that involves those emails. One way of spreading is trough chat services without concern our friend could be sending us an attach file or link that is actually a malicious code, so it is important to identify and be aware of that.

It is not enough consideration having just an antivirus protection, is highly recommended to have a fully updated system. If we are an administrator is really important to keep our host with software firewalls and keep our traffic well scanned with a firewall regarding our topology.

One last point regarding prevention is updating our software regularly mostly the office packets and other applications. Is a good practice as well to check the different online resources and web sites that help us to protect against worms and all malicious code.

7. Conclusion

Worms are programs that replicate themselves and do it over the network they can activate and replicate systems in different ways.

Even there are worms with good intent such as the first ones they really harm our systems. Today it is really important to have updated systems against malicious code.

The best tool against worms is prevention because after they penetrate our system we must detect and identify them in order to eliminate them. We have mentioned some techniques that can help us in order to prevent our system form malicious software some of them are antivirus, keep our systems up to date, good firewall protection, be aware of those links, false e-mails, and attached files that may come infected.

As future network technicians it is necessary to have a deep understanding of how important is the security of our network, not only against worms but all types of malicious software, it is our responsibility to secure our company network or just our personal computer.

8. References

- Wikipedia (en.wikipedia.org)
- http://www.virusall.com/worms.shtml
- http://www.viruslist.com/en/virusesdescribed?chapter=152540408
- http://antivirus.about.com/od/securitytips/a/emailsafety.htm
- Network security essentials William Stallings. P 341 - 344