Högskolan i Halmstad
School of information Science, Computer and Electrical Engeineering (IDE)
Network security spring 2008
2008-05-13

Malicious programs

Emil Mattsson, 870410-4655
Alexander Turkalj, 800625-4612
Henrik Karlsson, 840825-4814

Contents

1.1 Preface

We chose this subject because it was the most appealing in the list when we first saw it. Dealing with network security to us is being very aware of the dangers of viruses and such malicious programs. When we began writing this we had no idea of where to start, not a clue.

1.2 Introduction

This paper is about viruses and malicious programs. They infect your system and take over, wanting to do many bad things. Some of them want to use your cpu-cycles others want your rams, they control your computer and take it from you. It is not your computer anymore when it has been infected. This is a big issue now that we are seeing more viruses that even steal your bank account and take your money from you.

1.2.1 What are malicious programs?

So we have begun talk about malicious software but what is it really? Well it is easy just to think about viruses and Trojan horses, but there are many more types of attacks that define new names of what these viruses do. It is important to remember that viruses alone is the only form of malicious programs, the programs them selfes might be the virus.
As an overview we take a look at what they can be on wikipedia; “Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software” http://en.wikipedia.org/wiki/Malware

1.2.2 Can you trust any developers?

Yes, you do have to be able to trust your program developers. Who to buy from? If you cannot trust that the program you are using is in fact what it says it is. Take as an example a windows application that is a wordprocessor like the one that exists in the officepackage, what if it is that but really in the background there is a builtin function to record your keystrokes as a scheme to collect this data and later send it to Microsoft. Well yes, who knows right?

2 Malicious Programs

2.1 Types of malicious software

2.1.1 Virus

First of all, what is a Virus? Just the word Virus tells us that it is some kind of infection. And just as a regular virus that is found in the human world it spreads from host to host and can create a nasty disease that can be hard to cure. But usually we have some kind of antibiotics.

It's just the same in the digital world, a virus infects and contaminates the hosts that it is spread to, mostly they seem quite harmless, and doesn't really do any damage.

Other times they can destroy valuable data, or even hardware, depending on how the virus is written and what it is made to do.

Some people say that the only true computer virus is the ones that can only be spread by the help of the human hand. Nowadays, that isn't really what it's about, it's more of "How-many-ways-can-we-spread-this-so-that-we-can-take-over-the-world?" viruses, seeing as people uses different bugs/backdoors in operative systems to gain access. Most viruses is targeting the windows platform, due to the easy-to-use system there is usually something that can activate/change stuff depending on what it is told, this however isn't the same on UNIX/Linux, since they usually require someone to actually type in commands to become the super user.

One of the first known Viruses was actually a very harmless one, it didn't do anything nor did it destroy anything, the virus was called ©Brain, and was more of an advertisement then it was a virus. It was a stealth virus that hid in the boot sector, and originated from Pakistan.

The creators of this has been rumoured to be two brothers who ran a shop where they sold software, and they did this to try and stop the software piracy, the virus however, quickly spread from Pakistan to other countries quite fast.

2.1.2 Trojan horses

A Trojan horse, with the name taken from the old Greek history about how the soldiers invaded Troy using a huge wooden horse where they hid soldiers inside to get through the walls and destroy it from the inside, it describes how these programs work.

It's a program hidden inside another program with the purpose to destroy data, gather information from the user, (keyloggers are one type of Trojan horses) or remotely control another persons computer.

A few years back, a friend of mine showed me a program he had made, a file was sent to another friends computer, and after that he took over his mouse, keyboard and so on, it wasn't very advanced but it still showed how easy it is to actually remote someone else computer with just some small programs.

That which he showed me, is basically a ripoff of one of the most famous Trojan Horses, namely the NetBus Trojan, created by a Swedish person named Cal-Fredrik Neikter and it was released in 1998, the program was installed in a few different ways, one of them was when someone sent a game called Whackamole.

The Program consisted of two parts, a client-program, to run the show, and a server-program which was the actual backdoor, commonly named patch.exe, SysEdit.exe or explore.exe.

Everyone who had the client-program could access any infected system and make it do their bidding.

Some of the functions that this program carried was to: Open CD-ROM, Control Mouse, Mouse position, Play Sounds, Exit Windows, Send text and the possibility to take a screendump of whatever the user was doing at the time it was done.

I've been looking for information about a rumour I heard about this program, which is that it was first created to be able to remotely help people with computers, similar to the windows remote help function, but I have not found anything that strengthens this, nor anything that denies it.

2.1.3 Rootkits

The name rootkits comes from a group of commands in UNIX like the passwd, ps and the netstat commands, but the malware uses these commands to disguise it self from the user and the antispyware/antivirus programs. One of the things the program does is open a SSH connection to the intruders computer and give it full access with root/administrator rights.

2.1.3.1 Types

There are about 5 different types or levels of rootkits and they are:

Firmware:	This type of rootkits is imbedding them self in hardware firmware because the are not checked.
Virtualized:	It changes the boot sequence to make the computer load a different OS and then load the users OS as a virtual machine. Therefore it will have full access to the hardware and see all the communication between the OS and the hardware.
Kernel level:	This is one of the hardest to find and it is considered to be a more dangerous rootkit. This type disguises it self in drivers and the kernel by replace one part with them self and this can cause big stability problems since the new code isn't as good written as the original.
Library level:	Changes system calls with their own to hide information so they stay undetected.
Application level:	Disguises it self as ordinary applications with a imbedded Trojan.

2.1.3.2 Prevention, detection and removal

There are not many good detection tools since the rootkits hides them self with in the system or even above it so the best way to stop it is before it has gain access to your computer and this can be done with a good firewall to control the communication to and from your computer. A complement to the firewall is good antimalware software that is updated and of course activated, and to keep your software safe keep an eye out for updates from the developer.
If you do get a rootkit inside your computer, there are a couple of ways to notice it.
If your computer is much slower or work much more, this can be a warning of rootkits or other malware. The antivirus program can detect some of the most common rootkits by searching all the files and compare with known signatures. Other ways is to compare test results of file and memory test from a time were you are sure no rootkit was in your system.
To remove a rootkit is some of a challenge some thinks it is almost impossible and the only way is to save your most important files and format your hard drive completely and reinstall everything but this is most for those that have much sensitive data and not for the common user. For them it should be enough to run different sorts of malware detection and removal softwares to remove the most of them.

2.1.4 Backdoors

These are programs that open a door to the intruder which can use this at any time they wants. The intruders may stay in the system even if the system administrator notice it and resetting all the passwords, fill security holes.
One sort of backdoor is that the program creates a user account with administrative privileges but this is easy for the system administrators to find and stop. The most common way for the intruder to hide their presence is to create a service in windows. These programs is devided into two parts, the first is a server that is installed on the victims computer and the client that is the intruders side (Often a GUI to make it easy to search for servers).
If you have a backdoor server on your computer a intruder can easily connect and use your computer or just screw with you, and open/close the CD-ROM tray or if you got a webcam and a microphone they can see and listen to what you are doing but this is only the most advanced backdoors, the simple ones can run, upload and download files.
The server program can easily be included in worms or similar to reach many computers and control them

2.1.4.1 Removal

The removal of the most backdoor program is pretty easy since the are considered to like viruses so most of the antivirus software removes them and even some of the more advanced spyware removers have the ability to detect and remove them.
For the more advanced backdoors the antivirus programs can fail to remove them but then there are some good resources on the internet to help that is specialized in those kind of threats.

2.2 Malware profits

So i have you heard about program stealing your money? Well this is a question we asked ourselves unknowing that there actually exist such that can do this. we completely astonished by the fact that this takes place in the magnitude stated in report we just read. as stated in a report published by Financial Insights 400 million dollars where stolen in 2004. (SophosSecurityReport_2005.pdf)
Email attachments designed to lure users into accepting them is a big issue. An example of this is the 2006 Sober-N worm that was pretending to be actual tickets to the 2006 World Cup in Germany. Many believed this and nothing happened, but little did they know that what they had accepted would turn out to be not a hoax but a worm. This particular one later upgraded itself and used the infected zombie computers to spread propaganda. What's important to see here is that it could have been created to steal information about bank accounts and such that later could be used in financial gain. It was a faker and a big one. (Sophos page 5)
In the previous example the email spreading this worm was flooded in large scale. Looking back at it it is easy to see that this could have been detected, given the mass spam of it. The next year a different setup appeared which then seemed more profitable, at least for the cybercrimials. Concentrating on a small group of companies the criminal cyber gangs focused their efforts into focused nuke attacks, contrary to the mass chaos of before. (Sophos)
The bottom line is they will take your money. This is done in a number of ways, examples are; allowing others access, downloading webcode, stealing information, keylogging, turning off anti-virus and exploiting known vulnerabilities. Once they are in your system any number of ways previously stated and their combinations are possible. (sophos page 6)

Another area emerging is the use of online networks of computers that are leased to do the users bidding. This qoute from Global Security Threats and Trends report says a lot: "Botnets can be easily rented for denial-of-service attacks, spam distribution, and pay-for-click scams. Without protective measures, your systems could become part of an active botnet, or your company could be the target of a DoS attack launched from a botnet. " (Global Security Threats and Trends 2006)

3. Summary

This subject hasn't really taught us that much new, mainly given some information about rootkits, which we didn't know to much about. The viruses and the Trojan horses didn't really stand for a lot of challenge since it's so normal and basic when you move in the world of computers.

Well, this subject was after all still quite interesting, but still, it's a lot of things that you usually already know since it contains the basic parts of the daily basis of protection, in short, with a good Anti-virus program, you can stay up and running for a long long time, but if you go without it, just as in the real world, you just might catch an infection, and that wont be pretty.

If you don't know exactly what you're downloading, or what your friends (or so-called friends) send to you, then you'd better have something to stay safe, no one knows just what is being sent, if you don't trust it, don't accept it, unless you might want to get some weird programs that starts fucking about your computer.

4. References

http://www.dalepreston.com/Blog/2005/04/rootkits-and-hooks.html
http://www.pandasecurity.com/homeusers/security-info/types-malware/rootkit/
http://www.rootkitonline.com/types-of-rootkits.html
http://www.5starsupport.com/tutorial/rootkits.htm
http://www.windowsecurity.com/articles/Hidden_Backdoors_Trojan_Horses_and_Rootkit_Tools_in_a_Windows_Environment.html
http://www.f-secure.com/v-descs/backdoor.shtml
http://www.2-spyware.com/backdoors-removal
http://www.g4tv.com/techtvvault/features/30494/The_Five_Most_Famous_Computer_Viruses_pg2.html Info about the top 5 known viruses
http://www.windowsecurity.com/articles/The_Netbus_trojan.html information about one of the most known Trojan horses.

http://www.sophos.com/sophos/docs/eng/marketing_material/SophosSecurityReport_2005.pdf - "sophos security threat management report 2005"

http://mcafee.imiinc.com/nai7588/aug06/article3.jsp -

Global Security Threats and Trends 2006

http://en.wikipedia.org/wiki/Malware