Malware in Windows environment
(What it is and how to prevent it)

Aleš Zavec, Sašo Tomažič
Faculty of Electrical Engineering, University of Ljubljana, Slovenia
ales.zavec@.fe.uni-lj.si, saso.tomazic@fe.uni-lj.si

Abstract - *This paper first focuses on the most popular variants of malware circulating today and finally provides some guidance and concrete countermeasures that you can implement to prevent, detect, remove or respond to malware attacks. Many of malware programs will reinstall themselves even after you think you have removed them, or hide themselves deep within Windows, making them very difficult to clean. This paper details the different varieties of malware along with basic preventive measures. We examine the removal process and review a set of spyware removers and some other very useful tools.*

1. INTRODUCTION

Malware is short for malicious software. It is any program or file that is harmful to a computer user (or computer?). It can cause damage to a single computer, a server or a computer network. We can divide malware into several - categories:

- **Cookies** - Cookie is a text file on computer which contains information that identifies users to a particular website.
- **Spyware** - Spyware is any program that aids in gathering information from infected system without the user's knowledge.
- **Viruses** - This is the most known malware category. In this category we have programs that can reproduce themselves. Viruses need user interaction to propagate.
- **Worms** - This type of programs can self-propagate via a network and Internet.
- **Trojan horses** - This is software that does something other than its apparent functionality.
- **Rootkits and back doors** - Programs designed to infiltrate a system, hide their own presence and provide administrative and monitoring control to attacker.
- **Bots and zombies** - These programs are very similar to rootkits. They are focused on usurping the victim systems resources to perform a specific task (DoS attack, spam attack).

Malware is perhaps the biggest IT security threat facing your systems today. But how do you know if your systems are properly protected or if they are full of gaping holes making them vulnerable to a malware attack?

In addition to threatening the security and privacy of your business and personal data, malware affects your PCs speed and drains network bandwidth. This ultimately results in lost productivity and more calls to your helpdesk. But sometimes you don't even know malware is infecting your systems. It can remain hidden on your PCs for months and perpetually wreaking havoc on your machines over and over again.

However, there are many solutions and procedures on the market. As an average user, how can you know when, and where to begin to protect your systems from this growing threat?

First important thing is to learn how you can get infected. Malware often comes bundled with freeware or shareware programs. These malware programs usually pop-up ads, sending revenue from the ads to the program's authors. Others are installed from websites, pretending to be software needed to view the website. Still others, most notably some of the CoolWebSearch variants, install themselves through holes in Internet Explorer like a virus would, requiring you to do nothing but visit the wrong web page to get infected. The vast majority, however, must be installed by the user. Unfortunately, getting infected with malware is usually much easier than getting rid of it, and once you get malware on your computer it tends to multiply.

Most dangerous malware programs features:

- Capturing keystrokes
- Stealing passwords
- Stealing data and information (search and copy files)
- Remotely restarting operating systems
- Gaining the list of running processes and applications
- Starting and stopping running processes and applications
- Perform any administrative functions with administrative privileges

The final result if any of these events happens could be computers taken offline, stolen confidential data and information or even deleted data.

2. TYPES OF MALWARE

Majority of most notable attacks with malware aren't the ones to worry about. You should worry about unknown or special hackers malware attacks.

2.1. Cookies

Cookies are a legitimate tools used by many websites to track visitor information. Unfortunately, they can be used to track web surfing habits across many different websites without informing tracked users. Acquired data is used to customize the advertisements on websites or other commercials. Cookies are the lowest form of malware and are typically considered as an invasion of privacy.

2.2. Spyware

Spyware is any software which employs a user's Internet connection without user's knowledge or his explicit permission. This type of software is used for spying, capturing information or even for transmitting confidential information. Spyware programs are installed as cookies, entries in windows registry and as executable files on infected computer. Such programs could be very dangerous, because they are capable of capturing screen shots, turn on the local microphone, track user's web browsing habits, search hard drives and report back what programs are installed on infected computer. They also can forward copies of sent and received electronic mails to unknown address. Other malicious acts include stealing e-mail client's address book (could be used for spamming), login names, passwords, credit card numbers, etc. Spyware often works in conjunction with toolbars. For collecting data it may use a program that is always running in the background or it may be integrated into Internet Explorer. Integration allows spyware to run undetected whenever Internet Explorer is started.

Adware is mildest form of spyware. Main Adware function is to track user's habits and then based on the collected information pulls the adequate ads to the specific users.

One of the oldest and best known examples of malware is from the company Claria, which changed its name from Gator in 2003. Unlike most malware creators, Claria is a legitimate corporation with several big name advertisers and offices in both the United States and Europe. Claria is the maker of Gator Advertising and Information Network Publishing (or just GAIN), which actually consists of two programs that run in the background and work together. One program pops up ads while the other collects personal information. GAIN is typically bundled with other programs, including several published by Claria.

2.3. Viruses and Worms

Viruses and Worms are still the most known/popular forms of malware today. Viruses are often self-replicating programs able to attach themselves to executable files, delete data from hard drives and crash the infected computer whenever virus program is started. On the other hand Worms are programs that use security holes and computer networks for self-propagation. Worm scans the computer network for another computer with specific security hole. After that, it copies itself to that computer by exploiting specific security hole and then starts to propagate from there.

The most important qualities for this type of malware are:

- Propagation mechanism
- Payload
- Insertion points
- Detection avoidance

For the past several years, the most dominant Virus/Worm propagation mechanisms probably are e-mail attachments and software vulnerabilities. Payloads and post-infection activities have focused primarily on self-propagation and remote control of the infected computers with additional use of trojan horses, back doors, rootkits, bots and zombies. Insertion points refer to the locations where the files and data in the payload that actually execute the Virus or Worm functionality are installed or hidden. There is wide diversity of different possibilities used by Virus or Worm authors to do their bidding, but almost all of them attempt to write values to the ″Run″ keys in the Windows Registry in order to ensure the code will restart at the next logon. The ″Run″ keys in the Windows Registry are at:

- *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run* and
- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*.

You should regularly check these locations and in case that you see something suspicious, your system may be infected.

Today's Viruses and Worms tend to avoide detection by monitoring for key components of popular antivirus and personal firewall programs. Main goal is to avoide common detection tools by deleting registry entries related to starting such programs at logon or by terminating processes of common detection tools.

Some of the popular viruses and worms are: **ILOVEYOU** viruses, **Code Red** worms - replicated itself over 250,000 times in approximately nine hours on July 19, 2001, **Slammer** worm - exploited a hole in Microsoft's SQL server, **Mydoom** - mass-mailing worm and **Sasser** worm - and it variants.

2.4. Trojan horses

Trojan horse is a malicious program that is disguised as legitimate software. Trojan horses or Remote Administration Trojans (RATs) are a class of backdoors that are used to enable remote control over the compromised machine. They provide apparently useful functions to the user, and at the same time, open a network port on a victim computer. Then, once started, some trojans behave as executable files, interact with certain keys of the registers responsible for starting processes and sometimes create their own system services.

Contrary to common backdoors, Trojan horses hook themselves into the victim operating system and always come packaged with two files – the client file and the server file. The server, as its name implies, is installed in the infected machine while the client is used by the intruder to control the compromised system. Some well known trojan functions include: managing files on the victim computer, managing processes, remote activation of commands, intercepting keystrokes, watching screen images and also restarting and closing down infected hosts. Some are even able to connect themselves to their originator. Of course, these possibilities vary among individual Trojan horses.

In most cases, Trojan horses propagate via email. They are usually found within attachments, because their authors exploit vulnerabilities of the email client. Another technique relies on the fact that they bound into other programs. There are many programs in the Web that malts files to create a single executable file.

Some well known Trojan horses are **NetBus**, **SubSeven** and **Back Orifice**.

2.5. Rootkits and back doors

A backdoor is a program or a set of related programs that a hacker installs on the victim computer to allow access to the system at a later time. A backdoor's goal is to remove the evidence of initial entry from the systems log. But a backdoor will allow a hacker to retain access to a machine it has penetrated even if the intrusion factor has in the meantime been detected by the system administrator. Resetting passwords, changing disk access permissions or fixing original security holes in the hope of remedying the problem may not help. A trivial example of a backdoor is default BIOS, router or switch passwords set either by careless manufacturers or security administrators.

Adding a new service is the most common technique to disguise backdoors in the Windows operating system. This requires involving tools such as Srvany.exe and Srvinstw.exe that comes with the Resource Kit utility and also with Netcat.exe. The principle of this operation is that the srvany.exe tool is installed as a service and then permits netcat.exe to run as a service. The latter, in turn, listens on an appropriate port for any connection.

Rootkit is a collection of tools used by an intruder to hide his presence in an attacked system. It is usually used by attacker (hacker) to conceal his presence on a compromised system. After successful Rootkit placing, attacker has a possibility to return undetected at some time later.

Rootkits are composed of two basic parts: a dropper and a payload. The dropper is anything that can get the target system to execute the proper code. This can be done by tricking a user into opening an electronic mail attachment or be it security vulnerability. The payload is typically a kernel-hooking routine or kernel-mode device driver that performs one or more of the following techniques to hide its presence and performs its malicious activities:

- Kernel modification
- Service hiding
- Process hiding
- Port hiding
- File or directory hiding
- Registry key or value hiding
- User or group hiding
- Keystroke loggers

Some rootkits use multiple techniques to provide redundant reinfection vectors if one or more are discovered. More detail information on rootkits can be found on the next site: http://www.rootkit.com. The most common rootkits found on compromised system are: **Hacker Defender**, **FU Rootkit**, **Vanquish** and **AFX**.

2.6. Bots and zombies

It is very easy to hide things from average users with rootkits. If your computer becomes infected with one of the common mechanisms from previous chapter (electronic mail attachment, a software vulnerability, etc.), your system may wind up hosting a bot. Bot term is derived from ″robot″ and has referred to a program that performs predefined actions in an automated fashion on unmonitored IRC (Internet Relay Chat) channels. IRC connection is very important, because it is primary mechanism for controlling majority bots today. Bot will turn your computer into a zombie in a larger army of mindless computers under the control of an attacker.

With an army of zombies hooked up to the Internet, abuse falls into the following categories:

- Spam
- Distributed denial of service (DDoS) attacks
- Harvest valuable information
- Secondary infection
- Laundered connections and hosting

Today, these (large) bot networks have achieved economic value and are now bought and sold by the CPU cycle to anyone willing to pay for their use in spamming, DDoS and other similar attacks.

Some of the most popular bots in use today are**: Agobot**, **AttackBot**, **SubSeven**, etc.

3. PROPAGATION, DETECTION AND CLEANING MALWARE

Old fashioned malware programs spread very slowly by today's standards. It could take months or even years for a few thousand systems to be infected. Today, the Internet allows malware to propagate around the world very quickly. How quickly can malware infect large numbers of systems we all can saw with the Code Red, Nimda Worms (critical situation within a few weeks) and with even faster Slammer/Sapphire Worm (critical situation within a few minutes). Because of increasing numbers of online computer systems, users and a greater number of applications that can be affected, more and more automated malware attacks will appear. The most common malware attack/propagation is through electronic mail or system vulnerability.

If you think your system has been infected with malware, one of the first things to do is unplug the network cable (from all supposedly affected computer systems). This prevents further communication with outside entities that may react to attempts to investigate or clean the infected system. It also prevents spreading the infection to other systems on the computer network (assuming it hasn't already) or performing other malicious tasks such as DDoS attacks. With the network cable unplugged, you now have time to investigate and identify possible presence of malware. If you need some help from resources on the Internet, use good judgment about when to reconnect or try to use alternative/clean computer system for assistance.

How to find out, that you are infected? Next situations should raise the suspicion that your system may be infected with malware:

- Unexplained change of default home page in Web browser.
- Increased opening of new windows (pop-up ads) in Web browser.
- Appearance of new toolbars in Web browser.
- Change of safety settings in browser.
- Change of default side for search or mysterious search results.
- Unexpected slow downs or sluggish computer performance.
- Increased network traffic.

If you confirm a malware infection on your system, then you have two choices:

1. Assume that the malware you found was the only malware installed on your system and it was cleaned with the appropriate tools and/or techniques.
2. Assume that the malware you found was only one of potentially many infections on your system. Back up your critical data, erase the system, and rebuild from trusted sources.

For malware removal you have two possibilities, manual removal or turning to appropriate tools. For 99 percent of the infections you are likely to encounter, antivirus and antispyware software is sufficient to detect and clean malware on your system. If you have it installed on your system before you get infected, chances are that the malware was detected and blocked before it even had a chance to infect you. With antivirus and antispyware software you can successfully detect and clean first five mentioned categories in first chapter (Cookies, Spyware, Viruses, Worms and Trojan horses). When it comes to rootkits, back doors and bots, the situation becomes more complex. Most antivirus and antispyware software (both types are complimentary today) will detect the default installations of such tools, but with only minimal customizations, they become undetectable. Although antivirus software also use heuristics to identify polymorphic or metamorphic malware, we've yet to see the big antivirus vendors start looking for techniques such at kernel hooking and modification. Many antivirus programs use the very same hooking techniques to identify malware but if the rootkit gets there first, the antivirus software will not see it.

For antivirus software you can use one from the next site: http://anti-virus-software-review.toptenreviews.com/?ttreng=1&ttrkey=antivirus+software
For antispyware software you can use one or more from site: http://anti-spyware-review.toptenreviews.com/. Our recommendation is the use of:

- Webroot SpySweeper [5]
- Spybot [6]
- Microsoft Windows Antispyware [7]

Beside Microsoft tools (Task manager, msconfig, etc.) there are some other very handy tools (freeware and shareware) useful for fighting malware. Very useful tool for tuning your computer is The Ultimate Troubleshooter (http://www.answersthatwork.com). It displays detailed information on every Task, Service, and Windows Startup that is running on your computer and enables you to configure your computer. The Ultimate Troubleshooter also detects spyware, adware and many viruses. Another nice tool for seeing active processes is Process Explorer (http://www.sysinternals.com/Utilities/ProcessExplorer.html). It shows information about which handles and DLLs processes have been opened or loaded. Port Explorer (http://www.diamondcs.com.au/portexplorer) is the premier port-to-process mapper, allowing you to see all the open ports on your system and what programs own them. Along with this ability it also has many tools including the packet sniffer, bandwidth throttling and country detection to name just a few. Port Explorer is a powerful network monitoring utility and has an intuitive GUI that allows you to quickly see all the network activity your computer is involved in. For monitoring TCP/UDP connections you can use TCPView (http://www.sysinternals.com/Utilities/TcpView.html) is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. There are numerous free tools and published techniques that tend to keep pace the ever evolving landscape of stealth software techniques. Some tools for detecting rootkits:

- RootkitRevealer [8]
- BlackLight [9]
- IceSword [10]
- RKDetect [11]
- VICE, Patchfinder and Klister [12]

The last tool is ProcessGuard (http://www.diamondcs.com.au/processguard). This is a powerful new cutting edge program that greatly increases the security of your computer by preventing processes from being able to attack each other. It is considered by experts to be a must-have program for all users of Windows, and is the only program available that can prevent the infection of all known rootkit trojans.

We also suggest paying closer attention to the registry keys that are responsible for starting programs on the system startup, these registry elements usually contain some indication of how the intruder gained access. These keys are:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs
HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\KnownDLLs
HKEY_LOCAL_MACHINE\System\ControlSet\Services
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\WinLogon
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows (run)
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnceEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows (run)
HKEY_CLASSES_ROOT\exefile\shell\open\command

One technique shared across all rootkit detection tools is the concept of comparing disparate sources of information about the same system to identify inconsistencies, this concept is sometimes referred to as “diff-ing” two information sources. Rootkit detection tools are still in early stage of development. Soon after F-Secure released his first version of rootkit detector BlackLight (beta version), we could saw very powerful demonstration by the author of the most famous rootkit (Hacker defender) today, which shows how Hacker defender bypasses several rootkit detectors. You can see bypassing RootkitRevealer, BlackLight, IceSword and some other rootkit detectors, movie demonstration is available at [13].
The concept of rootkits itself illustrates the folly of trying to rescue a Windows system that has been compromised at so fundamental level. If you find yourself in this kind of situation, probably the best advice would be to backup all good data and then flatten and rebuild your system.

Luckily, the rootkit technology is not a big problem at the moment. The number of affected systems is a small fraction compared to the number of virus infections. But it is better to be prepared to handle outbreaks that install rootkit technology in a large number of systems, when it happens.

4. MALWARE COUNTERMEASURES

There is no general and efficient protection, which would be protecting us from all malware. Our first goal is to not get it in the first place. For malware prevention we should take next steps:

- Keep up to date on all relevant software security patches. (Use of Windows Automatic Updates is recommended.)
- Use of anti-virus protection software (with daily updates).
- Use of anti-spyware protection software (with daily updates).
- Use of software firewalls.
- Use of suitable settings in web browsers.
- Change Windows default configuration.
- Obligatorily testing on malware presents for all from Internet acquired programs, before their use in standalone systems or in network environment.
- Regular make of safety copies for critical systems.
- Use of policy which prevents opening of unsolicited electronic mails and mail attachments from unknown users.
- Filtering of electronic mail with certain mail attachments (.exe, .vbs, .pif, .com, .scr)
- For daily use, it isn't recommended using of administrative privileges. Never use account with administrative privileges on system that you will use to browse the Internet or read electronic mail.
- Education and increasing awareness of user's.
- Disable unneeded build-in programming interfaces (ActiveX controls, VBScripts, JavaScripts programs, etc.)

Even if you are careful, you can pick up all forms of malware through normal Internet activities!

5. CONCLUSION

We represent short overview of malware and its impact on computer systems and networks. Our dependence on interconnected computing systems is rapidly increasing, and even short-term disruptions from malware can have major consequences. Identifying, removing malware and the basics of prevention is a complicated topic on its own. If you will follow all procedures and techniques, you should stay safe from malcious software.

6. REFERENCES

[1] Ed Tittel, PC Magazine Fighting Spyware, Viruses, and Malware, Wiley Publishing, Inc., 2005

[2] Kevin Beaver, Hacking for Dummies, Wiley Publishing, Inc., 2004

[3] Ed Skoudis, Lenny Zeltser, Malware: Fighting Malicious Code, Prentice Hall PTR, 2003

[4] http://www.microsoft.com/security/default.mspx

[5] http://www.webroot.com

[6] http://www.safer-networking.org/en/download

[7] http://www.microsoft.com/athome/security/spyware/software/default.mspx

[8] http://www.sysinternals.com/Utilities/RootkitRevealer.html

[9] http://www.f-secure.com/blacklight

[10] http://xfocus.net/tools/200505/1032.html

[11] http://www.security.nnov.ru/soft

[12] http://www.rootkit.com

[13] http://www.hxdef.org/download/brilliant.php