Malware – What It Is and How to Avoid It.

Daniel G. James

East Carolina University

DTEC 6865

Dr. Phil Lunsford

November 19, 2007

Abstract

The Internet is a popular place in this day and age. Almost everyone young and old uses it in some form or another. Although there are many benefits to connecting your personal or business computer to the Internet there are also many threats to your data that come along with that decision. Many people are unaware of these threats and how they can adversely affect your data and ultimately your life. These threats include viruses, spyware, adware, key loggers, botnets, remote administration tools (RATs), and the list goes on. All of these threats fall under the umbrella known as malware. Malware is basically a software program that contains malicious code and is sent or released into the public with the intent to do harm. The damage can come in many forms such as destruction of data and/or theft of data. Many people use computers on a daily basis that are infected with some type of malware, yet they have no idea. How could this be possible? Simple, they have not been educated enough in this area to know the symptoms of infection. Perhaps many believe they are protected against all malware because they have an antivirus program running and keep its virus signature database up to date, but they are wrong. There are some attackers who are able to circumvent the antivirus scanning software by “packing” and “repacking” the malicious code. Each threat has a different goal as does each attacker that is using these threats against someone. The attacker may simply be curious, a graduate student having fun, or they could be a identity thief looking for their next victim. The best approach to this problem is to be knowledgeable of the potential threats and the defenses you can use against each one. In most cases a layered defense approach will be the best way to go.

What is Malware?

Malware is short for malicious software. Malware is software designed specifically to disrupt a computer system. A Trojan horse, worm or a virus could be classified as Malware. Some advertising software can be malicious in that it can try to re-install itself after you remove it. Malware can be dangerous to your data and you personally if your identity is stolen. If your identity is stolen just once it can take years to recover from the damage to your credit and takes a lot of time to sort out the mess left behind. Some folks are infected with Malware and do not even know it! This is especially dangerous because if you don't know you are infected then you will not seek treatment and the problem could continue for an extended period of time. During this time, a criminal could be collecting your personal data and tracking your every move on the Internet.

The first step toward containing the spread of malware is to understand the various technologies and techniques that malware authors can use to attack your computer. Malware threats directly target both users and computers, but the majority of threats target the user rather than the computer. If user with administrator-level user rights can be tricked into opening the door to a malware attack, the malicious code has more power to perform its tasks. Such an attack can frequently cause more damage than malware that relies on breaching a vulnerability in an application or the operating system. Some malware requires the installation of a particular application on the target computer before it can work. A huge number of Internet scams and phishing attacks have made the computer user a target to install such applications. It is often easier to trick a user into

running a piece of malware than it is to develop an automatic mechanism. For this reason it is important to train staff and managers to recognize likely

Internet scams and phishing attempts. Once inside the firewall, malware often targets a computer's operating system. The Windows operating system has been a significant target for a number of years due to its popularity. However, malware that specifically targets other operating systems has been on the rise, in addition to malware that targets applications and even antivirus software. For these reasons, it is important to keep both the operating system and the applications that you use up to date. (Simorjay)

Your computer should already have real-time antivirus and antispyware programs running on it to alert you if they detect an infection. However, even in the absence of an alert, if you notice unusual behavior or your system slows down, it is time to run a full system scan.

Performance issues that could indicate that your computer might be infected include:

- Your computer runs more slowly than normal or stops responding to program or system commands.
- Your computer fails and requires you to restart it frequently, or restarts on its own and then fails to run normally.
- Applications do not run correctly.
- You cannot access disks or disk drives on your computer.
- You cannot print correctly.
- You receive unusual error messages or pop-up windows.
- You see distorted menus and dialog boxes.
- Your browser's home page unexpectedly changes.

- You cannot access administrator shares on the computer.
- You notice an unexplained loss of disk space.

Although this list is not complete, it describes the types of unusual behavior that might suggest a problem. If you encounter any of these issues, run a full scan to better determine if you have a malware problem. Note: Not every computer that experiences these issues has a malware problem. Misconfigured applications or software bugs can also cause such issues. To avoid false indications of malware, ensure that your operating system and applications have the latest security updates and service packs, and that the computer has adequate RAM to run your applications. (Simorjay)

Since we have defined malware and some symptoms of infection let’s talk about some specific types of malware and how to combat each one.

Spyware, AKA Adware

Despite its name, the term "spyware" doesn't refer to something used by undercover operatives, but rather by the advertising industry. In fact, spyware is also known as "adware." It refers to a category of software that, when installed on your computer, may send you pop-up ads, redirect your browser to certain web sites, or monitor the web sites that you visit. Some extreme, invasive versions of spyware may track exactly what keys you type. Attackers may also use spyware for malicious purposes. Because of the extra processing, spyware may cause your computer to become slow or sluggish. (McDowell, Lytle)

There are also privacy implications:

- What information is being gathered?

- Who is receiving it?
- How is it being used?

The next important question is “how do you know if spyware is on your computer?” The following symptoms *may* indicate that spyware is installed on your computer:

- You are subjected to endless pop-up windows
- You are redirected to web sites other than the one you typed into your browser
- New, unexpected toolbars appear in your web browser
- New, unexpected icons appear in the task tray at the bottom of your screen
- Your browser's home page suddenly changed
- The search engine your browser opens when you click "search" has been changed
- Certain keys fail to work in your browser (e.g., the tab key doesn't work when you are moving to the next field within a form)
- Random Windows error messages begin to appear
- Your computer suddenly seems very slow when opening programs or processing tasks (saving files, etc.)

To avoid unintentionally installing it yourself, follow these good security practices:

- Don't click on links within pop-up windows - Because pop-up windows are often a product of spyware, clicking on the window may install spyware software on your computer. To close the pop-up window, click on the "X" icon in the titlebar instead of a "close" link within the window.

- Choose "no" when asked unexpected questions - Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. Always select "no" or "cancel," or close the dialog box by clicking the "X" icon in the title bar.
- Be wary of free downloadable software - There are many sites that offer customized toolbars or other features that appeal to users. Don't download programs from sites you don't trust, and realize that you may be exposing your computer to spyware by downloading some of these programs.
- Don't follow email links claiming to offer anti-spyware software - Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating. (McDowell, Lytle)

As an additional good security practice, especially if you are concerned that you might have spyware on your machine and want to minimize the impact, consider taking the following action:

- Adjust your browser preferences to limit pop-up windows and cookies - Pop-up windows are often generated by some kind of scripting or active content. Adjusting the settings within your browser to reduce or prevent scripting or active content may reduce the number of pop-up windows that appear. Some browsers offer a specific option to block or limit pop-up windows. Certain types of cookies are sometimes considered spyware because they reveal what web pages you have visited. You can adjust your privacy settings to only allow cookies for the web site you are visiting. (McDowell, Lytle)

Rootkits

The term “rootkit” describes any software that hides the presence of either processes or data. The term was first used by hackers who got “root” access to a UNIX system. According to a study by security vendor McAfee, virtually all of the rootkits that are currently in use target some version of the Windows operating system, where the privileged role goes by the name “administrator” instead of “root”. But the term “rootkit” is still used to describe such programs and the technology that they use. After gaining root access to a system, a hacker often uses a rootkit to conceal the fact that the system has been compromised, often installing hidden backdoors that can be used later to gain access or to selectively disable audit logging while the hacker is logged in to a compromised computer. More recently, hackers have been installing software that turns compromised computers into members of a “botnet,” a group of computers under the control of the hacker and used for implementing things like spam, phishing attacks, or distributed denial-of-service attacks. Rootkit technology provides hackers an easy way to implement such attacks undetected by the owners of the compromised computers, and the use of rootkit technology is now currently used in viruses, Trojan horses, spyware and adware. Even commercial software vendors have started to use rootkit technology to conceal information from users, possibly providing an opportunity for hackers to conceal their exploits. (Martin) (Honan)

The best defense against rootkits is to make your systems difficult to compromise. They suggest that the following five precautions will reduce the chances that an attacker will be able to install a rootkit on one of your computers:

- Use and maintain antivirus software to protect your computers

- Use a firewall to protect your network from some malicious traffic
- Use good passwords that are difficult for attackers to guess
- Keep software up to date by keeping current with patches
- Follow good security practices, especially when using applications that are particularly vulnerable, such as email and Web browsers (McDowell)

In addition to general good security practices, utilities that detect modifications to files are useful for detecting rootkits. File integrity checking tools like Tripwire create cryptographic checksums for the files on a system, and can identify any differences between the correct checksums and the current checksums. Any difference indicates that a file was tampered with in some way. Because they try to conceal their presence, rootkits are inherently difficult to detect, but it may be possible to infer that one is present by the behavior of a computer. If a computer has been compromised and had a rootkit installed on it, it will often be used for illicit purposes and may be possible to identify such compromised computers by the unusual behavior that they exhibit. Decreased performance or increased network traffic that cannot otherwise be accounted for may be indicators that a computer has a rootkit installed, concealing the presence of some sort of malicious program that is causing the unusual behavior. Rootkits need to be running to conceal their presence, so one technique that may aid in the detection of rootkits is to boot a computer that is suspected of being compromised from an unmodified version of the operating system, like one from a CD-ROM. Booting off of a clean source denies the rootkit the chance to start running. Many rootkits may then be detected by using antivirus software. After finding that a rootkit has been installed on one of your systems, the next step is usually to remove the rootkit. This can be tricky. Kernel-level rootkits make

modifications to the operating system, and their removal may disable vital parts of the operating system if the removal of the rootkit is not done carefully. It is often possible for a skilled system administrator to remove a rootkit without crippling the operating system, but it is usually faster and thus less expensive, to simply reinstall a clean version of the operating system from a backup image of the compromised computer. If there is a chance that the information on the compromised machine will be needed to help investigate the compromise, be sure to make a backup copy of the compromised machine before reinstalling the operating system. After reinstalling to remove a rootkit, remember to check for other malicious applications that may still be present – it is likely that the rootkit was concealing the presence of this additional application, and this application will also need to be removed. (Martin) (Honan)

Viruses and Worms

A Trojan is a program that appears to be legitimate, but in fact does something malicious. Quite often, that something malicious involves gaining remote access to a user's system. Unlike viruses, a Trojan does not replicate (i.e. infect other files), nor does it make copies of itself as worms do. There are several different types of Trojans. Some of these include: remote access Trojans (RATs), backdoor Trojans (backdoors), IRC Trojans (IRCbots), and keylogging Trojans. Many Trojan encompass multiple types. For example, a Trojan may install both a keylogger and a backdoor. IRC Trojans are often combined with backdoors and RATs to create collections of infected computers known as botnets.

It can happen to anyone. Considering the vast number of viruses and Trojan horses traversing the Internet at any given moment, it's amazing it doesn't happen to *everyone*. Hindsight may dictate that you could have done a better job of protecting yourself, but that does little to help you out of your current predicament. Once you know that your machine is infected with a Trojan Horse or virus, what can you do? If you know what specific malicious program has infected your computer, you can visit one of several anti-virus web sites and download a removal tool. Chances are, however, that you will not be able to identify the specific program. (Durkota) Unfortunately your other choices are limited, but the following steps may help save your computer and your files:

1. Call IT support.

If you have an IT support department at your disposal, notify them immediately and follow their instructions.

2. Disconnect your computer from the Internet.

Depending on what type of Trojan horse or virus you have, intruders may have access to your personal information and may even be using your computer to attack other computers. You can stop this activity by turning off your Internet connection. The best way to accomplish this is to physically disconnect your cable or phone line, but you can also simply "disable" your network connection.

3. Back up your important files.

At this point it is a good idea to take the time to back up your files. If possible, compile all of your photos, documents, Internet favorites, etc., and burn them onto a CD or save

them to some other external storage device. It is vital to note that these files cannot be trusted since they are still potentially infected.

4. Install an anti-virus program and scan your machine.

Since your computer is infected with an unknown malicious program, it is safest to install an anti-virus program from an uncontaminated source such as a CD-ROM. You will have to visit your local computer or electronics store to a purchase the software. There are many to choose from, but all of them should provide the tools you need. After you install the software, complete a scan of your machine. The initial scan will hopefully identify the malicious program(s). Ideally, the anti-virus program will even offer to remove the malicious files from your computer; follow the advice or instructions you are given. If the anti-virus software successfully locates and removes the malicious files, be sure to follow the precautionary steps in Step 7 to prevent another infection. In the unfortunate event that the anti-virus software cannot locate or remove the malicious program, you will have to follow the next steps.

5. Reinstall your operating system.

If the previous step failed to clean your computer, the only available option is to reinstall the operating system. Although this corrective action will also result in the loss of all your programs and files, it is the only way to ensure your computer is free from backdoors and intruder modifications. Before conducting the reinstall, make a note of all your programs and settings so that you can return your computer to its original condition.

It is vital that you also reinstall your anti-virus software and apply any patches that may be available.

6. Restore your files.

If you made a back up CD in Step 3, you can now restore your files. Before placing the files back in directories on your computer, you should scan them with your anti-virus software to ensure they are not infected.

7. Protect your computer.

To prevent future infections, you should take the following precautions:

- Do not open unsolicited attachments in email messages.
- Do not follow unsolicited links.
- Maintain updated anti-virus software.
- Use an Internet firewall.
- Keep your system patched. . (Durkota)

Botnets

A "botnet" is a collection of computers that have been infected with remote-control software. An IRC "bot" is the software that gets installed by a virus, which in turn connects to an IRC (Internet Relay Chat) server — the control plane for sending commands to the bots. A typical botnet scenario involves thousands of compromised Windows machines and a single "attack" command issued by the owner of the botnet, resulting in once innocent computers executing an attack on an unsuspecting Web site.

This article will explore common methods of infection and the capabilities the bots have, for the sake of better understanding these perils. When an unpatched Windows computer connects to the Internet, survival is an unlikely prospect. Within minutes, the computer can become infected with a trojan or virus that installs an IRC bot. The bot will immediately "phone home" by connecting to an IRC server then stand by, awaiting commands. SANS has cited 24 minutes as the average amount of time a freshly installed Windows XP computer can last on the internet before infection. If you're running a fresh install of MS-SQL server, the time is considerably shorter. Some have cited sub-minute survival times for new, unpatched SQL servers. (Schluting)

Botnets have various capabilities, including denial of service attacks, spam relays, theft of personal information, and they even start web servers on infected computers to aid in phishing attacks. These are all illegal activities, and definitely not something you want coming from your computer. There's nothing worse than receiving e-mail from a different company's security officer with evidence you've been attacking them or sending spam. Reading the source code for one specific IRC bot leads to much enlightenment, and fright. The repertoire of tasks a bot can carry out on its owner's behalf is truly astounding. Here's a brief list of a few of the more interesting things bots can do:

- Run their own IRC server, becoming a master for other bots to connect to
- Capture or "harvest": CD Keys from the Windows registry, AOL traffic including passwords, and the entire Windows registry itself
- Start flooding a specific IP or network using TCP, UDP, or ICMP
- Add/delete Windows services from the registry
- Test the Internet connection speed of the infected computer

- Start the following services: http proxy, TCP port redirector, and various socks proxies
- Scan and infect other computers on the local network
- Send spam
- Download and execute a file from a given FTP site (Schluting)

And if that wasn't horrific enough for you, consider the following: most of the IRC bots also have modular capabilities. So if someone programs a new module to extend the bots' capabilities, the owner of the botnet simply runs a single command to install and use the new module on every bot. The capabilities listed above were taken from the agobot source code, but other popular ones probably have similar, if not better, functionality. (Schluting)

So, you may be asking what can I do to prevent this from happening to me? IRC bots are normally installed via known vulnerabilities, so preventing your computer from being taken over should be as easy as keeping up to date on Windows Updates and virus definitions. Windows file sharing (ports 135-139 and 445) and MS-SQL (1433, 1434) should never be allowed in from the Internet. In a case where a new computer is being installed, it is common for an infection to take place before Windows update has a chance to complete. Installing in a secure area with the appropriate ports blocked should allow for a safe installation and update, assuming no internal computers are infected and trying to fan out. Network Address Translation (NAT) is the obvious solution for this, but doesn't always work in enterprise environments doing unattended installations of Windows. (Schluting) (Russinovich)

Tracking IRC bots has become quite a hobby for some people. From a network perspective, most anomalous traffic these days is turning out to be IRC bot related. IRC bots will respond to an "infect" command, and start scanning the local network and infecting others. This type of activity (scanning) normally raises a few eyebrows on carefully managed networks. Intrusion detection systems, like snort, also have signatures for some of the more common IRC bots. For example, if the string "Exploiting IP" is seen in an IRC message, chances are very high that this is an IRC bot reporting home. They don't attempt to conceal what they are doing most of the time, as can be seen by running ngrep "#exploit" on a network monitoring host (#exploit is the IRC channel name). Even though you will be able to see the IRC traffic once you have identified which host is possibly infected, detecting infected computers on your network is not always a simple task. Snort does a fair job, if you've updated the signatures to tell it what to look for.

Owners of a botnet are always looking to expand operations. They are in a constant struggle to own more and more slave computers. The more high quality the botnet, the more revered the owner will be. Corporate and educational owned computers are prime targets, since they are normally well connected in terms of Internet bandwidth. The sad part is, in general, infecting corporate and educational networks is just as easy as infecting residential computers. Sdbot, rxbot, and agobot are a few of the most common bots at the moment. It doesn't really matter which bot is running on a computer, since they all provide complete control to the new owner of the compromised computer, resulting in a very bad day for the original owner. (Schluting) (Russinovich)

Antivirus software, along with the new Malicious Software Removal Tool from Microsoft, are both able to detect existing bots. Some bots have been known to propagate via e-mail as well, making the infection a bit harder to block. Aside from user education, the best method to prevent previously unseen infections from taking over a computer is to simply block the above mentioned ports. New Windows vulnerabilities may exist in the future, but for the time being, you should be relatively safe. (Schluting) (Russinovich)

Conclusion

Hackers and spammers may be using your computer right now. They invade secretly and hide software to get access to the information on your computer, including your email program. Once on your computer, they can spy on your Internet surfing, steal your personal information, and use your computer to send spam — potentially offensive or illegal — to other computers without your knowledge. Computers that are taken over this way often become part of a robot network, known as a "botnet" for short. A botnet, also known as a "zombie army," usually is made up of tens or hundreds of thousands of home computers sending emails by the millions. Computer security experts estimate that most spam is sent by home computers that are controlled remotely, and that millions of these home computers are part of botnets. (Onguard)

Spammers can install hidden software on your computer in several ways. First, they scan the Internet to find computers that are unprotected, and then install software through those "open doors." Spammers may send you an email with attachments, links or images which, if you click on or open them, install hidden software. Sometimes just visiting a website or downloading files may cause a "drive-by download," which installs

malicious software that could turn your computer into a “bot.” The consequences can be more than just annoying: your Internet Service Provider (ISP) may shut down your account. It can be difficult to tell if a spammer has installed hidden software on your computer, but there are some warning signs. You may receive emails accusing you of sending spam; you may find email messages in your “outbox” that you didn’t send; or your computer suddenly may operate more slowly or sluggishly. (Onguard)

Botnets are not inevitable. You can help reduce the chances of becoming part of a bot — including limiting access into your computer. Leaving your Internet connection on and unprotected is just like leaving your front door wide open. The FTC encourages you to secure your computer by:

- Using anti-virus and anti-spyware software and keeping it up to date. You can download this software from ISPs or software companies or buy it in retail stores. Look for anti-virus and anti-spyware software that removes or quarantines viruses and that updates automatically on a daily basis.
- Setting your operating system software to download and install security patches automatically. Operating system companies issue security patches for flaws that they find in their systems.
- Being cautious about opening any attachments or downloading files from emails you receive. Don’t open an email attachment — even if it looks like it’s from a friend or coworker — unless you are expecting it or know what it contains. If you send an email with an attached file, include a text message explaining what it is.

- Using a firewall to protect your computer from hacking attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A firewall is different from anti-virus protection: while anti-virus software scans incoming communications and files for troublesome viruses, a properly-configured firewall helps make you invisible on the Internet and blocks all incoming communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection because the connection is always open. Most common operating system software (including Windows XP and Vista) comes with a built-in firewall, but you may have to enable it.
- Disconnecting from the Internet when you're away from your computer. While anti-virus and anti-spyware software, along with a firewall, are critical protections when you're connected to the Web, they're not foolproof. Hackers just can't get into your computer when it's disconnected from the Internet.
- Downloading free software only from sites you know and trust. It can be appealing to download free software like games, file-sharing programs, customized toolbars, and the like. But remember that many free software applications contain other software, including spyware.
- Checking your "sent items" file or "outgoing" mailbox for messages you did not intend to send. If you do find unknown messages in your out box, it's a sign that your computer may be infected with spyware, and may be part of a botnet. This isn't foolproof: many spammers have learned to hide their unauthorized access.
- Taking action immediately if your computer is infected. If your computer has been hacked or infected by a virus, disconnect from the Internet right away. Then scan

your entire computer with fully updated anti-virus and anti-spyware software. Report unauthorized accesses to your ISP and to the FBI at www.ic3.gov. If you suspect that any of your passwords have been compromised, call that company immediately to change your password. (Onguard)

Works Cited

Durkota, M. (2004, January). US-CERT. *Recovering from a Trojan Horse or Virus* Retrieved September 5, 2007, from the World Wide Web: http://www.us-cert.gov

Hackworth, A. Ianelli, N. (2005, December). US-CERT. *Botnets as a Vehicle for Online Crime* Retrieved September 5, 2007 from the World Wide Web: http://www.us-cert.gov

*Honan, B. (2007, May). ISSA Journal. *Malware: Containment and eradication.* Retrieved September 5, 2007 from the World Wide Web: http://www.issa.org/Members/Journal.html

Lytle, M. McDowell, M. (2007, August) US-CERT. *Recognizing and Avoiding Spyware* Retrieved September 5, 2007 from the World Wide Web: http://www.us-cert.gov

*Martin, L. (2007, January). ISSA Journal. *Regarding Rootkits: An Overview.* Retrieved September 5, 2007 from the World Wide Web: http://www.issa.org/Members/Journal.html

McDowell, M. (2006, January). US-CERT. *Understanding Hidden Threats: Rootkits and Botnets Retrieved* September 5, 2007 from the World Wide Web: http://www.us-cert.gov

OnGuard Online. (2007, June). OnGuard. *Botnets and Hacker and Spam (Oh, My!)* Retrieved September 5, 2007 from the World Wide Web: http://www.onguardonline.gov

Russinovich, M. (2007, July). Microsoft. *Advanced Malware Cleaning.* Retrieved September 5, 2007 from the World Wide Web:

http://www.microsoft.com/emea/spotlight/Mark_Russinovich_Advanced_Malware_Cleaning.aspx

Schluting, C. (2005, May). Enterprise Networking Planet. *Botnets: Who Really "0wns" Your Computers?* Retrieved September 5, 2007 from the World Wide Web: http://www.enterprisenetworkingplanet.com

*Simorjay, F. (2007, September). ISSA Journal. *Removing Malware* Retrieved September 5, 2007 from the World Wide Web: http://www.issa.org/Members/Journal.html