

Virus and Spyware Policy

Definitions

Virus

In computer security technology, a **virus** is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of the virus into a program is termed *infection*, and the infected file (or executable code that is not part of a file) is called a *host*. Viruses are one of the several types of malware or malicious software. In common parlance, the term *virus* is often extended to refer to computer worms and other sorts of malware. This can confuse computer users, since viruses in the narrow sense of the word are less common than they used to be, compared to other forms of malware such as worms. This confusion can have serious consequences, because it may lead to a focus on preventing one genre of malware over another, potentially leaving computers vulnerable to future damage. However, a basic rule is that computer viruses cannot directly damage hardware, but only software.

While viruses can be intentionally destructive (for example, by destroying data), many other viruses are fairly benign or merely annoying. Some viruses have a delayed payload, which is sometimes called a *bomb*. For example, a virus might display a message on a specific day or wait until it has infected a certain number of hosts. A *time bomb* occurs during a particular date or time, and a *logic bomb* occurs when the user of a computer takes an action that triggers the bomb. However, the predominant negative effect of viruses is their uncontrolled self-reproduction, which wastes or overwhelms computer resources.

Computer Worm

A **computer worm** is a self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers.

In addition to replication, a worm may be designed to do any number of things, such as delete files on a host system or send documents via email. More recent worms may be multi-headed and carry other executables as a payload. However, even in the absence of such a payload, a worm can wreak havoc just with the network traffic generated by its reproduction. Mydoom, for example, caused a noticeable worldwide Internet slowdown at the peak of its spread.

A common payload is for a worm to install a backdoor in the infected computer, as was done by Sobig and Mydoom. These zombie computers are used by spam senders for sending junk email or to cloak their website's address. Spammers are thought to pay for the creation of such worms, and worm writers have been caught selling lists of IP addresses of infected machines. Others try to blackmail companies with threatened DoS attacks. The backdoors can also be exploited by other worms, such as Doomjuice, which spreads using the backdoor opened by Mydoom.

Spyware

Spyware is a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, however, spyware is designed to exploit infected computers for commercial gain. Typical tactics furthering this goal include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card numbers); monitoring of Web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites.

As of 2005, spyware has often been described as the #1 security threat for computers running the Microsoft Windows operating systems. Some malware on the Linux and Mac OS X platforms has behavior similar to Windows spyware, but to date has not become anywhere near as widespread.

Malware

Malware (a portmanteau of "MALicious softWARE") is a type of software designed to take over and/ or damage a computer user's operating system, without his or her knowledge or approval. Once installed, it is often very difficult to remove, and depending on the severity of the program installed, its handiwork can range in degree from the slightly annoying (such as unwanted pop up ad while a user is performing regular computing tasks on or offline), to irreparable damage requiring the reformatting of one's hard drive, since much of malware is poorly written. Examples of malware include viruses and trojan horses.

Reference: <http://en.wikipedia.org/wiki>

Known downloaded software programs that contain spyware/malware

(This list is not intended to be complete. These are some of the best known programs.)

Gator/Gain, Web Shots, Weatherbug, TimeSync, Kazaa

Common Threats

1. Hijacking your home web page; modifying system so it is very difficult to reverse it back to normal.
2. Changing your dial-up connection to a server in South Africa, so next time you dial-up to your Internet Provider it costs you \$3-5 per minute.
3. Generating a multitude of pop-up screens; an attempt to close them redirects your browser to unwanted websites (sometimes of the offensive nature);
4. Turning your PC into a “zombie machine”, waiting for a command to come from its “master” anywhere in the world; it could be turned into a source of spam, scan and/or just for grabs for any malicious activity the “master” chooses.
5. Installing a keystroke logger – a small program that captures every keystroke and sends a captured data to a remote server. It looks specifically for passwords, account names and numbers, etc.
6. Installing “backdoors”, through which multitude of spyware and worms can be easily installed. The sheer number of those installed programs might cripple the performance even of a powerful PC. If installed on multiple PC’s, excessive network traffic generated by those worms can bring the network down.
7. Certain activities of “zombie” PC’s can be qualified as illegal (movie sharing, attacks, spamming), and hold an unsuspecting PC user and organization liable for that activity.

Town Procedures

1. Do not download any software from the Internet. Consult with Information Systems regarding any software that is required for your position.
2. Do not download any music.
3. Do not turn off or remove Anti-virus software for any reason.
4. Do not open any email that seems suspicious. Delete the email.
5. Do not acknowledge any online prompts, like ones suggesting to “improve performance”, “remove spyware”, “make this your home page”; 99% of those applets have malicious content.
6. For the reason above, do not click on any pop-up windows in your Internet browser.
7. If you suspect that you have a virus or spyware problem, contact Information Systems immediately. The best method to contact Information Systems is through the Work Order System at <http://www.townofmanchester.org/infosys/mainmenu.cfm>

Virus Protection

1. The Town currently uses Computer Associates E-Trust.
2. Every Town computer (Windows and Novell) and server must have it installed.
3. Signature Updates are done automatically. The first reference is the Virus server which is a redistribution server. The second reference is the FTP site: ftpav.ca.com. Updates should be scheduled for every 4 hours.
4. E-Trust should be set to monitor incoming and outgoing files at all times.
5. E-mail protection is achieved via complex antispam and antivirus solution based on Spamassassin, Amavisd-new and F-prot antivirus mail server. F-prot is checking for and downloading new signatures every 4 hours.
6. For diagnosing and troubleshooting of a suspicious activity, the network monitoring and diagnostic tools are used, such as:
 - a. SolarWinds Engineer Edition
 - b. WhatsUpGold
 - c. Snort
 - d. Sniffer Investigator
7. Other tools available for virus scanning are:
 - a. Stinger
 - b. BitDefender
 - c. F-Secure
 - d. Symantec Virus Removal Tools

Spyware Protection

1. The Town does not have any automated Spyware protection.
2. Prevention is accomplished through user education.
3. Several programs are used to remove spyware:
 - a. AdAware
 - b. Spybot
 - c. HijackThis
4. The Police Department is using a corporate version of Webroot. This software runs in the background on the PC and continuously scans the computer.