



## **Do-It-Yourself Computer Surveillance Overview of Technology and Methods**

### **How could someone monitor another person's computer?**

#### **Remote Control Software**

- Designed as a legitimate tool to remotely access your computer from another location
- Can be configured to covertly monitor someone else using a computer

Example: RealVNC

#### **Web Monitoring Applications**

- Marketed as tools for parents and employers to monitor and control internet use by kids and employees
- Can be configured to operate covertly without any noticeable indications that the software is running
- Records keystrokes, emails, instant messages, chat sessions, web sites visited, screen shots, webcam images, and more
- Collected information can be automatically forwarded to a website on the internet or an email address
- Commercial antivirus/antispyware applications often do not detect these applications because they are considered to be legitimate software packages
- Some offer methods to con an unsuspecting person into installing the software on their computer, such as a customizable email attachment that silently installs the software when opened.

Examples: Spector Pro, WebWatcher, Guardian Software

#### **Hardware KeyLoggers**

- Hardware devices installed between the keyboard and computer or inside a computer to covertly record all keystrokes on the computer.
- Impossible to detect with anti-virus/anti-spyware software
- Keystrokes are recorded to memory inside the device itself for later retrieval

Examples: Keelog, KeyCarbon

#### **Web-Based Applications**

- Increasingly many people are using online web-based applications for everything from email to word processing to home banking
- These applications can be accessed from anywhere on the internet
- All you need is a password, which can be guessed, stolen with a keystroke logger, or reset using the site's automated password reset system
- Most of these systems keep a history of activity - emails sent, chat sessions, previous versions of documents, etc.

Examples: Google Mail, Yahoo Mail and Messenger, Facebook, MySpace, Google Docs

#### **Email Redirection**

- Many email systems allow a user to send a carbon copy of all email messages they received to another email address. Some also allow you to include messages you send as well.
- Legitimate uses include convenience of consolidating multiple emails addresses to one and message archiving for regulatory compliance



## **How could someone install surveillance software on someone else's computer?**

### **Physical access to a computer**

- No password or easy to guess password – many people use very simple passwords or no password at all to protect their computer, making it easy for someone to access their computer and install surveillance software.
- There are a variety of tools freely available on the internet that can retrieve or reset passwords on Windows computers if someone has physical access to the machine.

### **Email attachment**

- It's very easy to forge an email message to make it look like it came from someone other than the real sender.
- Consider this: A "friend" sends you an email with an attachment purporting to be a holiday greeting. When you open it, you see a funny animation involving Santa and his reindeer. What you don't see is the rootkit software that quickly installed in the background and promptly buried itself deep in the operating system.

### **Bundled software**

- Spyware is often bundled with or made to look like software that is fun or useful in some way, like a free game or productivity application. Once you install the software, the spyware component will remain even if you uninstall the original software.

### **Exploit a flaw in the operating system, web browser, or other application**

- Software vulnerabilities (i.e. bugs) are regularly discovered in operating systems, web browsers, and other applications. These are often exploited by attackers to gain access to a target computer
- A scary example of this was the infamous JPEG vulnerability 5 years ago that affected many applications and operating systems that all used a common, flawed piece of software. In theory this vulnerability would allow an attacker to gain complete control of a computer just by getting someone to open a graphics file on a website or in an email. Software updates were quickly developed to fix this problem, but there are likely many computers still out there that have not been updated.
- There are a "kits" available on the internet to allow people with moderate experience in computer programming to quickly develop a program that takes advantage of a vulnerability to gain unauthorized access to a computer

### **USB Hard Drive**

- By default Windows will automatically run software on a CDROM or USB hard drive that is inserted into the computer if the device is configured for autorun.
- If someone gives you CDROM or USB drive as a way of transferring large electronic files to you, beware that you could be getting more than you bargain for.

## **How can I protect my computer from spyware?**

- Use good passwords for your computer and any websites that contain private information
- Change your password regularly – at least every 90 days
- Install and regularly update commercial anti-virus and anti-malware software
- Use Microsoft Update or another update service to install the latest security updates for your computer on a regular basis. Service companies like TCW Computer Systems offer managed services to monitor your computers and ensure that the latest updates are applied to all computers on your network



- Disable the autorun feature in Windows. Instructions on how to do this can be found here: <http://www.us-cert.gov/cas/techalerts/TA09-020A.html>, but depending on your experience level you may wish to enlist some help with making the required registry change.
- Do not download and install free software from the internet – only install software from trusted commercial suppliers
- Do not use peer to peer file sharing services like BitTorrent, LimeWire, or eMule, as they are particularly susceptible to vulnerabilities and the content available on these systems is not reviewed by any third party
- Consult a professional computer services company to review the security of your network to ensure that you have appropriate access controls and intrusion prevention systems in place

### **How can I tell if my computer has been infected?**

#### **Scan your computer regularly with anti-virus/anti-malware software**

- Many common types of spyware can be detected by using commercial anti-virus and anti-malware software. Scan your computer with at least two different software packages, as some are better at detecting certain spyware than others. Malwarebytes' AntiMalware is a software package that I would currently recommend for spyware removal, and there is a feature-limited free version available.

#### **Enlist the services of a professional to:**

- Review the list of processes running on the system and look for any non-standard or suspicious applications
- Use a tool like HiJackThis to find all applications that are configured to start up automatically, web browser plugins, Windows Explorer plugins, etc.
- Perform an "offline" anti-virus/anti-malware by connecting the computer's hard drive to another computer or by booting from a CDROM disk – this is necessary to defeat stealth techniques used by certain types of spyware.

If your computer has already been compromised, it can be VERY difficult, even for a professional, to detect the stealthiest types of spyware. Certain hard-to-detect spyware applications, called rootkits, actually modify the operating system in order to hide themselves from any software-based detection method (like antivirus software, task list, etc). Performing an offline scan of a computer hard drive is an effective way of finding known rootkits, but the only way to be certain that an infection has been removed is to backup your data, securely erase the hard drive, and re-install Windows and applications from scratch.

#### **Feel free to send me follow-up questions:**

Delmar Zimmerman  
TCW Computer Systems, Inc.  
717-653-2700  
[dzimmerman@tcwcomputers.com](mailto:dzimmerman@tcwcomputers.com)  
[www.tcwcomputers.com](http://www.tcwcomputers.com)