Protecting your Computer
Against Malware and Malsubjects

By
Felix Uribe

felix@uribe100.com

NOTE:
This document assumes some knowledge of the Internet and network communication devices and programs.

Based on Verizon's 2012 Data Breach Investigation Report[1], "incidents involving hacking and malware were both up considerably last year, with hacking linked to almost all compromised records." 98% of these breaches stemmed from **malsubjects**[2] whose motives included financial or personal gains, protests, and fun among others. The report identified that 81% of these breaches came as a result of hacking and 69% due to malware.

Broadband communication, or high speed dedicated connections to the Internet, allows the computer to be "always" connected to the Internet, which significantly increases the risk of a breach or an attack. Fortunately, if your computer is properly equipped with the installation of some of the basic types of security software programs: firewall, anti-virus, anti-spyware, encryption, and intrusion detection system, the likelihood of a breach or an attack can significantly be reduced. They create a line of defense that makes it harder for malsubjects to compromise your computer.

Personal Firewalls:

A personal software firewall[3] blocks an intruder and stops programs installed on your computer from transmitting unauthorized information to an external system. Firewalls also filter out unauthorized or potentially dangerous types of data from the Internet before they reach your computer.

Malsubjects are constantly scanning the Internet for vulnerable computers. With the advent of broadband connections [always connected], they can access and scan systems faster and easier, making it more likely that your system will get hit with one of those scans. Firewalls block these attempts and provide you with the ability to log and review who and when an intruder attempted to gain access to your system. Today, malsubjects use automated tools that constantly search or "probe" computers connected to the Internet in order to identify vulnerable systems.

---

[1] A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service.

[2] Malsubject: **Mal**icious **Subject** (plural: malsubjects) is a term coined by computer security analyst Felix Uribe (http://www.uribe100.com) to identify an unauthorized individual or subject whose activities are intended to break into an information system with malicious intents to compromise the information's confidentiality, integrity, or availability of organizations and individuals. Malsubjects include hackers, cyber-thieves, phishers, spammers, hacktivist, and nation states among others.

[3] Software-based firewalls are computer programs (software) as opposed to hardware-based firewalls, which are dedicated devices.

Anti-Virus Software

Viruses are the number one threat for computer users connected to the Internet. Within the past several years, these threats have spread at an alarming rate due to the heavy use of the Internet and e-mail services. The loss of millions of dollars suffered by private companies and government agencies caused by virus infections, such as the "I love you" and "Melissa" viruses or some other form of the same virus showing up somewhere in the world continues to make headlines.

Fortunately, anti-virus software is equipped with features that not only check your files in your system or when downloading them from the internet, but also check your in-coming and out-going e-mail attachments for viruses and other malicious programs. Anti-virus software is constantly updated to protect against newly discovered threats.

In addition to anti-virus programs, the following two good security practices can prevent your computer from getting infected: 1) delete unopened e-mail messages with attachments if received from an unknown source, and 2) do not open any e-mail if you do not recognize the sender or the message seems suspicious.

Anti-Spyware Software

Spyware are programs installed in your computer by software manufacturers, market research companies, and malsubjects to transmit private information from your computer to another computer without your permission. They are typically hidden components of freeware or shareware programs installed on the user computer usually without the users' knowledge or consent.

Spyware programs are mostly used to gather information (username, passwords, and other personal information) and the user's surfing habits, and then send the information back to the home site. Some spyware are also famous for causing sluggish computer performance and system instability. They are to blame for most of the infamous "pop-up" ads and unsolicited e-mails or spam. In addition, some sophisticated spyware can 'hijack"or take control of your Internet connection. Programs, such as Napster, Kazaa, and other peer-to-peer (P2P) services, brought spyware programs to the masses.

Encryption Software

Encryption software allows a computer user to change the information on any file (pictures, music, documents, etc.) and make it unreadable to anyone, but the person holding a special "key" that is able to transform the unreadable file back to a readable format. When files are encrypted only the person with the key can actually read them.

We have to admit, there are many types of information that we do not want others to see (personal documents, financial, business, etc). Once the information has been encrypted,

it can be stored on insecure media or transmitted through an insecure network (like the Internet), and still remain secret. Then the information can be decrypted into its original form. For example, if your computer is lost, stolen or accessed by someone, if important files are encrypted, you can be sure that no one can read them as long as you hold the key.

Intrusion Detection Systems (IDS)

Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems[4]. An IDS on you computer will allow you to monitor, alert, and document any attacks in the event of any unauthorized intrusion by malsubjects.

There are two basic types of IDS on the market today, host-based IDS and network-based IDS. Host-based IDS monitors individual computers or hosts. Network-based IDS monitor the entire network by analyzing the flow of the network traffic and the content of individual packets for any malicious traffic.

General Safety Precautions

As computer users, we are also responsible for developing good computer use practices and exercising good common sense to detect, prevent and mitigate the risks associated with malware and malsubjects. Two of the best advice that one can take to avoid these threats are:

- Do not open an email from unknown individuals or organizations containing links to a website on the Internet or a file attachment. Delete them immediately. If you know the person or organization and you are not expecting the message or doubt of its contents, check the accuracy of the message by contacting the person or organization that sent it, it is better to be safe than sorry.

- Keep your computer software up to date with all patches and updates for its operating system and other programs residing on the computer.

For many years, I have been able to keep my computer safe and protected with the help of these or comparable security software programs. They provide you with layers of protection at different levels and complexity. You too can prevent many of these breaches and attacks by simply installing such programs on your computer or home network.

For additional information on malsubjects and software to combat malware, visit www.uribe100.com.

[4] National Institute of Standards and Technology (NIST) Special Publication 31 “Intrusion Detection Systems”, November 2001.