# Defending Against Malware and Trojan Horse Threats

Malware – software written to infect private computers and commit crimes such as fraud and identity theft—has become big business in the cyber underworld. As a result, if you use a computer for web surfing, shopping, banking, email, instant messaging, and gaming without proper protection, you are putting yourself at high risk of being victimized.

By exploiting vulnerabilities in operating systems and browsers, malware can sneak malicious Trojan horse programs onto unsecured PCs. Unsuspecting and unprotected users can also download Trojans, thinking they are legitimate game, music player, movie, and greeting card files. Trojans can also lurk in files shared between friends, family, and coworkers using peer-to-peer file sharing networks.

Trojans have traditionally hidden in worms and viruses spread by email, but they're increasingly showing up in instant messages and on PDAs and cell phones. Organized crime rings have devised insidious new ways of delivering Trojans, and consumers must stay informed of the latest tricks. Protection against these multi-faceted attacks requires integrated anti-virus, firewall, and anti-spyware technologies. Below are the top 10 things you need to know to protect yourself against malware and Trojan attacks.

## What Do Trojans Do?

Trojans corrupt important files and place adware, spyware, keyloggers, and screen scrapers that can steal personal information and your online experience. They can also redirect you to fake phishing web sites—even when you type valid web addresses (URLs) into your browser.

Trojan programs are most dangerous because they can create a back door into your computer that gives malicious hackers direct access to your system. Once installed, Trojans can hijack your PC and upload usernames, passwords, credit card numbers, social security numbers, and bank account numbers to specified computers for as long as they remain undetected.

Hackers use chat rooms and peer-to-peer file sharing networks to target and hijack unsecured PCs. Once the Trojan opens a back door, the computer joins hordes of other "zombie" computers that the hacker can control remotely. The hacker can launch Denial of Service (DoS) attacks, generate ad traffic, send out infected software to other vulnerable computers, and pump out spam.

Cyber gangs even rent networks of these zombie computers (a.k.a. *bots*) by the hour to other criminals for extortion and fraud. Users are rarely aware that their machines have been hijacked, since usually the only indicator is slightly slower performance.

A new trend in malware is to extort money. This *ransomware* is a Trojan that encrypts a PC's files or threatens to delete them one by one unless the victim pays up. After the person pays using a money transfer service, the extortionist sends them a special disarming code or decryption application. Hackers also use Trojans to exploit weaknesses in legitimate banking, online bill pay, and e-commerce sites.

## How Does My PC Get a Trojan?

Today, Trojans can be spread by *browser drive-bys*, where the program is downloaded in the background when you simply surf to a rigged web site. Shell code runs a Trojan that downloads additional payload code over HTTP—various forms of bots, spyware, back doors, and other Trojan programs. Hackers then send phishing emails to lure users to web sites, where unsuspecting victims are tricked into revealing personal information. Hackers can also exploit security weaknesses on sites, and then piggyback their Trojans onto legitimate software to be downloaded by trusting consumers.

## Top 10 Ways to Defend Against Malware and Trojans

Although hackers never stop developing new tricks to commit fraud and steal identities, consumers can take proactive steps to safeguard their systems. All it takes is a combination of robust security software and a commitment to following basic safety rules.

1. **Protect your computer with strong security software** and make sure to keep it up to date. McAfee® SecuritySuite provides trusted PC protection from Trojans, hackers, spyware, and more. Its integrated anti-virus, anti-spyware, firewall, anti-spam, and anti-phishing work together to combat today's advanced multi-faceted attacks. It scans disks, email attachments, files downloaded from the web, and documents generated by word processing and spreadsheet programs.

2. **Use a security-conscious Internet service provider (ISP**) that implements strong anti-spam and anti-phishing procedures.

3. **Enable automatic Windows® updates** or download Microsoft® updates regularly to keep your operating system patched against known vulnerabilities. Install patches from other software manufacturers as soon as they are distributed. A fully patched computer behind a firewall is the best defense against Trojan and spyware installation.

4. **Use extreme caution when opening attachments**. Configure your anti-virus software to automatically scan all email and instant message attachments. Make sure your email program doesn't automatically open attachments or automatically render graphics, and ensure that the preview pane is turned off. This will prevent macros from executing. Refer to your program's safety options or preferences menu for instructions. Never open unsolicited business emails, or attachments that you're not expecting—even from people you know.

5. **Be careful when engaging in peer-to-peer (P2P) file-sharing**. Trojans sit within file sharing programs waiting to be downloaded. Use the same precautions when downloading shared files that you do for email and IM. Avoid downloading files with the extensions *.exe*, *.scr*, *.lnk*, *.bat*, *.vbs*, *.dll*, *.bin*, and *.cmd*. Anti-virus software and a good firewall will protect your system from malicious files.

6. **Download the latest version of your browser** to ensure that it is also fully updated and utilizes the latest technologies to identify and filter out phishing sites that can install Trojans.

7. **Use security precautions for your PDA, cell phone, and Wi-Fi devices**. Trojans arrive as an email/IM attachment, are downloaded from the Internet, or are uploaded along with other data from a desktop. Cell phone viruses are in their infancy, but will become more common as more people buy phones with advanced features. Anti-virus software is available for PDAs and cell phones.

8. **Configure your instant messaging application correctly**. Make sure it does not open automatically when you fire up your computer. Turn off your computer and disconnect the DSL or modem line when you're not using it. Beware of spam-based phishing schemes—don't click links in emails or IM.

9. **Be certain a web site is legitimate before you go there**. Use software that automatically checks this, such as AccountGuard from eBay and ScamBlocker from Earthlink. You can also check the validity of individual web addresses (URLs) with a WHOIS search such as http://www.DNSstuff.com.

10. **Back up your files regularly** and store the backups somewhere besides your PC. If you fall victim to a Trojan attack, you can recover your photos, music, movies, and personal information like tax returns and bank statements.

McAfee
227 Bath Road
Slough, SL1 5PP
United Kingdom
+44.1753.217.500
www.mcafee.com