

# ZOMBIES, TROJAN HORSES AND YOU



BY PAM GREENBERG

**C**reeper first appeared in 1971. It came with this message, “I’m the creeper, catch me if you can!”

Creeper, the first computer virus, ushered in an era of malicious software or “malware.” These pests include viruses as well worms, Trojan horses, spyware, scareware, ransomware, phishing and more, all colorfully named but seriously dangerous. Attacks have changed from mere pranks to costly criminal acts.

One way to avoid malware is to give up e-mail, stop searching the Web, sign off all social networks and give up your new great mobile devices. But if you’d rather stay connected, it’s important to understand who these high-tech enemies are.

## THE HACKER’S TOOLBOX

Hackers break into government and other computer systems to change existing settings,

*Pam Greenberg tracks technology issues for NCSL. Members of the National Association of Legislative Information Technology contributed to this article.*

and when done maliciously, they can disrupt or even destroy computer systems or networks. The hacker’s toolbox consists of viruses, worms, zombies and botnets, which are combined with other tactics to go viral.

Here’s how these tools work.

**Viruses.** Remember the Michelangelo virus? It appeared in 1992 and threatened to erase computer hard disks each year on the artist’s birthday, March 6. Although Michelangelo the artist was a lot more successful than his namesake, the virus was the precursor of a large but unknown number of viruses that have cost millions in damages and lost productivity. Viruses—so-called because they “infect” a computer and spread to others without the knowledge of the computer user—are sent through a network or the Internet by an infected file or link, or are installed through infected disks or other devices.

**Worms.** Worms are viruses that create copies of themselves across the Internet. Unlike a virus, they do not need to attach to an existing program or file. They wiggle themselves into operating systems and use communication between computers to spread. They can be destroyed by

downloading updates and patches provided by vendors.

Insure.com in 2010 identified the 12 costliest computer viruses and worms, ranging from \$10 million in damages caused by the Morris virus, the first widespread worm on the Internet, to \$38.5 billion caused by MyDoom—the costliest malware so far.

**Bots, Botnets and Zombies.** Viruses and worms implant software robots, or “bots,” into a computer. They can be controlled remotely to perform tasks without the knowledge of computer owners.

Bots allow hackers into a computer’s “back door” to seize control, and then turn into “zombies” that send out spam or search for other vulnerable networks. Armies of these zombies are known as botnets, which are used for sending huge amounts of spam and malware. The Kneber botnet was orchestrated by an Eastern European criminal gang and compromised about 2,500 commercial and government computer systems worldwide in 2010, gaining access to e-mail, banking sites, and social networking sites.

## THE ACCOMPLICES

Hackers and online criminals have exploited the most intractable security problem: human nature. They persuade computer users to bypass security measures and tools through clever manipulation and deception, with Trojan horses, spyware, spoofing and phishing. Security features must be incorporated into computer systems that do not rely on the judgment of computer users to be effective.

**Trojan Horses.** Trojan horses, unlike viruses and worms, are not self-replicating and don't reproduce by infecting other files, although some can carry a worm or virus. Instead, they are a piece of programming code disguised as another program or file. Users spread Trojans by running or installing an attractive program, like pretty screen savers, fun games or other programs they think are legitimate. Along with these programs, the Trojan installs another that causes problems. Some are minor irritants, such as popup windows or changes to a user's home page. Others do more damage, such as deleting files, stealing information by installing a keystroke logger or opening a back door for unauthorized purposes. Many Trojans are invited into computers when a user clicks a bad link in spam e-mail.

**Spyware, Scareware and Ransomware.** Spyware is software that surreptitiously monitors and tracks a user's computer activity for hackers to sell to advertisers or steal identities through usernames, passwords, credit card numbers and other personal information. Spyware, like Trojan horses, is often unknowingly installed by users who think they are getting a different program, or are downloaded along with legitimate software.

Other variations of spyware include scareware and ransomware, which usually appear in the form of fake anti-virus or anti-spyware advertisements. Alarming popup messages falsely claim to have found computer viruses and offer to scan and remove them for a price. Scareware links also appear in e-mail and Internet searches about viruses and malware.

Ransomware spreads through worms or Trojans and denies users access to their own files until a ransom is paid.

**Spoofing and Phishing.** These are like the eerie Grady twins in "The Shining" who say "come and play with us forever and ever." Spoofers create e-mails or websites that are not what they appear to be. An e-mail spoofer makes the e-mail look authentic and appear to be from a trusted company or friend, but instead

it contains a malicious link. Some spoofed e-mails contain malware that collects the e-mail addresses in the recipient's contacts, and then resends the e-mail to all the user's contacts. Some spoofing is even more malicious. In December, a spoofed e-mail Christmas card that appeared to be from the White House was sent to government staff members in other countries. The e-mail card contained a malicious link to a virus and was "phishing" for passwords and online banking information.

Phishing schemes trick recipients into sharing sensitive information. An e-mail may contain a link that appears to connect to a legitimate website, but actually links to a spoofed version of the website where hackers collect account numbers and passwords.



## RISKY NEIGHBORHOODS, OPEN DOORS

Popular advances in technology offer new opportunities to hackers.

**Social media.** These sites are especially vulnerable to hackers. Facebook's popularity, combined with its information sharing and social features, make it especially attractive to malware creators. Some of the ads, surveys, games and apps that appear to be created for social media sites actually spread malware when downloaded.

Hackers have successfully targeted several high-profile individuals on Facebook. A British politician's Facebook account was hacked in 2009; messages sent to his Facebook friends directed them to a malicious web page. Hackers also have been able to make changes to the Facebook pages of French president Nicolas Sarkozy and even Facebook co-founder and CEO Mark Zuckerberg.

Other social media sites also are attractive to online criminals. Sites such as Twitter that have shortened web addresses can be easily disguised

and connected to malicious websites. Twitter users in 2009 received phishing messages from their online followers encouraging them to visit a website that attempted to steal their username and password.

**Wi-Fi hotspots.** Free Wi-Fi hotspots at coffee houses, airports and Internet cafes are open networks and do not have the security features typically present on a private wireless government or corporate network. Hackers can use "sniffer" software programs at hotspots to capture user IDs and passwords sent across the Wi-Fi network.

Recently, another malicious software program called Firesheep has spread like wildfire. The software is free, easy to install and use, and reportedly has pulled the wool over the eyes of more than 3 million users. Firesheep allows hackers to see and use the usernames and passwords of nearby Wi-Fi users. Banking sites and most e-commerce sites are encrypted to protect the user during his or her time on the site, but many websites, including some social media sites and webmail programs, do not use end-to-end encryption and are vulnerable to Firesheep.

**Mobile devices.** The features that make today's mobile devices so popular—Internet and wireless connectivity, text and multimedia messaging, and easy storage of information—also make them more vulnerable to malware. An increasing number of smart phone users also are checking bank balances and paying bills through their phone.

Bluetooth wireless devices that allow cell phone users to speak hands-free can allow other unauthorized devices to connect and intercept communications. Malware can be passed to or from devices when they are synced to a network, and unvetted apps for mobile devices also can carry malware.

USB or flash drives also are vulnerable to malware. They can carry worms that execute automatically as soon as the device is plugged into a computer.

It appears these high-tech pests are here to stay. Fortunately, if you work in a state legislature, your IT professionals fight them for you. But knowing what they are, and the harm they can do, can help you protect yourself and your information. 

## SL ONLINE

Read an interview with Jerry Gamblin, a security specialist with the Missouri House of Representatives at [www.ncsl.org/magazine](http://www.ncsl.org/magazine).

## 9 WAYS TO STAY SAFE ONLINE



### #1

Install and update anti-virus/anti-malware, anti-spam and web security software.

Install operating system updates when prompted. For Windows, go to Microsoft Windows Update to check for updates. For Apple computers, click on the Apple logo, then Software Updates. Install updates for software you use, especially if they indicate they provide security fixes.

### #2

Don't open file attachments or click on links in e-mails from people you don't know or who you did not expect to hear from. If the link may be legitimate, type—don't cut and paste—it into the web address field or use a bookmark you've set up previously.

### #3

Don't click anywhere on pop-up messages or messages warning that your computer is infected. Instead, turn off the computer and, after turning it back on, run your antivirus or antispyware software. Be cautious about clicking on links with shortened web addresses posted by Twitter.

### #4

Use strong passwords longer than 14 characters with a combination of numbers, symbols, and upper and lower case, or better yet create passphrases that are easy for you to remember but difficult for others to guess. Don't use a public computer when visiting a site that requires your password, and change your passwords regularly.

### #5

Protect smart phones, laptops and other mobile devices by setting up passwords, installing updates and anti-malware software. Do not reply to texts from senders you do not recognize or install programs or apps on your smart phone without checking them out first.

### #6

Use encrypted USB/flash drives when storing sensitive information. If you use a Bluetooth headset, be sure to change the default password and turn it off when not in use.

### #7

Use caution at Wi-Fi hotspots. Avoid visiting websites that require your passwords, and

change security settings in Facebook—under Account Security in Account Settings—and other social media and web e-mail accounts to enable https secure browsing when possible, which will block programs like Firesheep. Disable your wireless adapter and Wi-Fi mode on smart phones when working offline.

### #8

Be sure your computer is protected by a firewall. A firewall blocks worms and other unauthorized programs and prevents Trojans from making contact with hackers. Computers with later versions of Windows or Apple operating systems come with a firewall built in and turned on by default.

Similarly, newer wireless routers that connect computers, laptops, printers, iPods or other mobile devices come with password-protected firewall protection.

### #9

Back-up your data regularly. Internet service providers and security software vendors may offer backup storage, or, for sensitive information, use CDs or encrypted USB/flash drives to store files.