Published on *InfoWorld* (http://www.infoworld.com)

# Your quick guide to malware types

By Roger A. Grimes
Created *2012-10-23 03:00AM*

When it comes to security, people tend to play fast and loose with the terminology. But it's important to get your malware classifications straight because knowing how various types of malware spread is vital to containing and removing it.

Here's a quick malware bestiary. If nothing else, you'll have your malware terms right when you hang out with geeks.

**[ Prove your security smarts in InfoWorld's malware IQ test, part 1 [1] and part 2 [2]. | Find out how to block the viruses, worms, and other malware that threaten your business, with hands-on advice from expert contributors in InfoWorld's "Malware Deep Dive [3]" PDF guide. | Keep up with key security issues with InfoWorld's Security Central newsletter [4]. ]**

**Viruses**
A computer virus is what most of the media and regular end-users call every malware program reported in the news. Fortunately, most malware programs aren't viruses. A computer virus modifies other legitimate host files (or pointers to them) in such a way that when a victim's file is executed, the virus is also executed.

Pure computer viruses are fairly uncommon today, compromising less than 10 percent of all malware. That's a good thing: Viruses are the only type of malware that "infects" other files. That makes them particularly hard to clean up because the malware must be infected from the legitimate program. This has always been nontrivial in the best of times, and today it's almost impossible. The best antivirus programs struggle with doing it correctly and in many (if not most) cases will simply quarantine or delete the infected file instead.

**Worms**
Worms have been around even longer than computer viruses, all the way back to mainframe days. Email brought them into fashion in the late 1990s, and for nearly a decade, computer security pros were besieged by malicious worms that arrived as message attachments. One person would open a wormed email and the entire company would be infected in short order.

The distinctive trait of the worm is that it's self-replicating. Take the notorious Iloveyou worm [5]: When it went off, it hit nearly every email user in the world, overloaded phone systems (with fraudulently sent texts), brought down television networks, and even delayed my daily afternoon paper for half a day. Several other worms, including SQL Slammer [6] and MS Blaster [7], ensured the worm's place in computer security history.

What makes an effective worm so devastating is its ability to spread without end-user action. Viruses, by contrast, require that an end-user at least kick it off, before it can try to infect other innocent files and users. Worms exploit other files and programs to do the dirty work. For example, the SQL Slammer worm used a (patched) vulnerability in Microsoft SQL to incur buffer overflows on nearly every unpatched SQL server connected to the Internet in about 10 minutes, a speed record that still stands today.

**Trojans**

Computer worms have been replaced by Trojan horse malware programs as the weapon of choice for hackers. Trojans masquerade as legitimate programs, but they contain malicious instructions. They've been around forever, even longer than computer viruses, but have taken hold of current computers more than any other type of malware.

A Trojan must be executed by its victim in order to do its work. Trojans usually arrive via email or are pushed on users when they visit infected websites. The most popular Trojan type is the fake antivirus program, which pops up and claims you're infected, then instructs you to run a program to clean your PC. Users swallow the bait and the Trojan takes root.

Trojans are hard to defend against for two reasons: They're easy to write (cyber criminals routinely produce and hawk Trojan-building kits [8]) and spread by tricking end-users -- which a patch, firewall, and other traditional defense cannot stop. Malware writers pump out Trojans by the millions each month. Antimalware vendors try their best to fight Trojans, but there are too many signatures to keep up with.

**Hybrids and exotic forms**

Today, most malware is a combination of traditional malicious programs, often including parts of Trojans and worms and occasionally a virus. Usually the malware program will appear to the end-user as a Trojan, but once executed, it attacks other victims over the network like a worm.

Many of today's malware programs are considered rootkits or stealth programs. Essentially, malware programs attempt to modify the underlying operating system to take ultimate control and hide from antimalware programs. To get rid of these types of programs, you must remove the controlling component from memory, beginning with the antimalware scan.

Bots are essentially Trojan/worm combinations that attempt to make individual exploited clients a part of a larger malicious network. Botmasters have one or more "command and control" servers that bot clients check into to receive their updated instructions. Botnets range in size from a few thousand compromised computers to huge networks with hundreds of thousands of systems under the control of a single botnet master. These botnets are often rented out to other criminals who then use them for their own nefarious purposes.

**Spyware and adware**

If you're lucky, the only malware program you've come in contact with is adware, which attempts to expose the compromised end-user to unwanted, potentially malicious advertising. A common adware program may redirect a user's browser searches to look-alike Web pages that contain other product promotions.

Another category of malware is spyware, which is most often used by people who want to check on the computer activities of loved ones. Of course, in targeted attacks, criminals can use spyware to log the keystrokes of victims and gain access to passwords or intellectual property.

Adware and spyware programs are usually the easiest to remove, often because they aren't nearly as nefarious in their intentions. Find the malicious executable, and prevent it from being executed -- you're done.

**Fighting the menace**

Today, many malware programs start out as a Trojan or worm, but then dial home to a botnet and let human attackers into the victim's computer and network. Many advanced persistent threat attacks [9] start out this way: They use Trojans to gain the initial foothold into hundreds or thousands of companies, while the human attacks lurk, in search of interesting intellectual property. The vast majority of malware exists to steal money -- directly out of a bank account or indirectly by stealing passwords or identities.

If you're lucky, you can find malicious executables using a program like Microsoft's Autoruns [10] or Silent Runners [11]. If the malware program is stealthy, you'll have to remove the hiding component from memory first (if possible), then work on extricating the rest of the program. Often I'll boot into Safe Mode or through another method, remove the suspected stealth component (sometimes by just renaming it), and run a good antivirus scanner a few times to clean up the remainders after the stealth part is removed.

Unfortunately, finding and removing individual malware program components can be a fool's errand. It's easy to get it wrong and miss a component. Plus, you don't know whether the malware program has modified the system in such a way that it will be impossible to make it completely trustworthy again.

Unless you're well trained in malware removal and forensics, back up the data (if needed), format the drive, and reinstall the programs and data when you find malware on a computer. Patch it well and make sure end-users know what they did wrong. That way, you get a trustworthy computer platform and move ahead in the fight without any lingering risks or questions.

*This story, "Your quick guide to malware types [12]," was originally published at InfoWorld.com [13]. Keep up on the latest developments in network security [14] and read more of Roger Grimes' Security Adviser blog [15] at InfoWorld.com. For the latest business technology news, follow InfoWorld.com on Twitter [16].*

- Security
- Anti-spyware
- Anti-virus
- Malware
- Security

---

**Source URL (retrieved on *2012-10-23 11:38AM*):**
http://www.infoworld.com/d/security/your-quick-guide-malware-types-205450

**Links:**
[1] http://www.infoworld.com/d/security/are-you-cyber-sleuth-test-your-malware-iq-187066?source=fssr
[2] http://www.infoworld.com/d/security/malware-iq-test-round-2-198237?source=fssr
[3] http://www.infoworld.com/d/security/download-infoworlds-malware-deep-dive-report-186438?source=ifwelg_fssr
[4] http://www.infoworld.com/newsletters/subscribe?showlist=infoworld_sec_rpt&amp;source=ifwelg_fssr
[5] http://en.wikipedia.org/wiki/ILOVEYOU
[6] http://www.infoworld.com/t/malware/exorcizing-the-ghost-slammer-492
[7] http://en.wikipedia.org/wiki/Blaster_(computer_worm)
[8] http://www.infoworld.com/d/security/malware-and-hackers-increasingly-targeting-macs-780
[9] http://www.infoworld.com/d/security/5-signs-youve-been-hit-advanced-persistent-threat-204941
[10] http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx
[11] http://www.silentrunners.org/
[12] http://www.infoworld.com/d/security/your-quick-guide-malware-types-205450?source=footer
[13] http://www.infoworld.com/?source=footer
[14] http://www.infoworld.com/d/security?source=footer
[15] http://www.infoworld.com/blogs/roger-a.-grimes?source=footer
[16] http://twitter.com/infoworld