



FACT SHEET

U.S. Army Cyber Command and Second Army
The Nation's Army in Cyberspace
www.arcyber.army.mil

THE FACTS: MALWARE AND BOTNETS

What are computer viruses?

Viruses are harmful computer programs that can be transmitted in a number of ways and differ in many ways, but are all designed to spread themselves from one computer to another through the Internet. Most commonly, they are designed to give the criminals access to the infected computers.

What are "spyware" and "adware"?

The terms "spyware" and "adware" apply to several different technologies. The two important things to know about them is that:

- They can download themselves onto your computer without your permission (typically when you visit an unsafe website or open an unsafe attachment)
- They can make your computer do things you don't want it to do. This might be as simple as opening an advertisement you didn't want to see, or as devastating as tracking your online movements, stealing your passwords and compromising your accounts.

What is a "botnet"?

Botnets are networks of computers infected by malware (computer viruses, key loggers and other malicious software) and controlled remotely by criminals, usually for financial gain or to launch attacks on websites or networks.

If your computer is infected with botnet malware, it communicates and receives instructions about what it's supposed to do from "command and control" computers located anywhere around the globe.

Many botnets are designed to harvest data such as passwords, Social Security numbers, credit card numbers, addresses, telephone numbers and other personal information. The data is then used for identity theft, credit card fraud, spamming, website attacks and malware distribution.

What can I do to protect myself?

- Keep a clean machine: Having the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats.
- When in doubt, throw it out: Links in email, tweets, posts and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete it or mark it as junk email.
- Protect all devices that connect to the Internet: Along with computers, smartphones, gaming systems and other web-enabled devices need protection from viruses and malware.
- Plug and scan: "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

SOURCE: National Cyber Security Alliance Cyber Threat Resources booklet, November 2012