Learn About Malware Menaces (Viruses, Spyware, Botnets & More)

Stephanie Obodda - 2022-10-31 - Comments (0) - Antivirus and Malware

Malware ("malicious software") -- spyware, bogus anti-virus apps, rogueware, viruses, scareware, trojan horses, worms, etc.-- is lurking everywhere. Hackers and their botnets are constantly rattling virtual doors looking for easy prey. If you become infected, all sorts of unpleasant things can happen to make your life miserable, including a hacker taking control of your computer as well as your identity.

What Can You Do?

First, "Know Thy Enemy"

- ***Botnet:*** A network of compromised computers, each acting as a robot (or bot) under the control of a remote user. Often used to send out spam and phishing emails. More background in Botnet 101: Don't Get Own3d!
- ***Spyware:*** An annoying, intrusive, and sometimes offensive program that allows some to covertly gather your information through your Internet connection, often for advertising purposes. Read more in the SANS' documents Advances in Spyware (SANS document) and Top 15 Malicious Spyware Actions.
- ***Virus:*** A program that can copy itself, attach itself to other programs or files, and perform unwanted and unauthorized tasks. May not be easily detected and can be widely spread through the sharing of files, memory devices or email.
- ***Worm:*** A computer program that can run independently, cloning itself onto other computers connected to a network. Known to consume computer resources destructively.

Second, Protect Yourself

- Keep your computer's OS and software current. Configure your computer to update its operating system automatically. Accept application updates when offered.
- Protect your computer with an approved anti-malware app. Brown provides comprehensive anti-malware protection, free of charge.
- Look out for bogus antivirus software, which could clandestinely disable any real product, redirect computing resources to it, put your data and privacy at risk, and be nearly impossible to remove.
- Install software, such as Ad-Aware or Spybot Search & Destroy or Malwarebytes, that detect and remove threats. The IT Service Center is only suggesting the use of this

software and is only meant to be run on personal, non-Brown devices.

Third, How to Recover from a Compromise

- Disinfect your computer following the suggestions in the article Clean an Infected Computer.
- If you have problems or are uncomfortable with the process, contact the IT Service Center for assistance.

Fourth, Keep an Eye Out for Threats

- Read the IT Alerts
- Learn how to spot a phish
- Other sources for alerts: Symantec "Threat Explorer" List, US-CERT Alerts and SANS Internet Storm Center