STOP | THINK | CONNECT™

# Botnet Fact Sheet

## What are botnets?

Botnets are generally networks of computers infected by malware (computer virus, key loggers and other malicious software) and controlled remotely by cybercriminals, usually for financial gain or to launch attacks on website or networks. Botnets may infect and use laptops, desktops, servers, routers, smartphones, or any other network equipment to conduct malicious activity.

All computers connected to the Internet are susceptible to malware infections. The malware employed by botnets can be surreptitiously installed on your computer. If you open an email attachment or visit a website that is distributing malware, your computer may become infected and be turned into a "bot" (short for "robot"). If your computer becomes part of a botnet, it may wait for instructions from the "command and control" (also sometimes known as "C2" or "C&C") computers or perform automated tasks, such as keystroke monitoring, without your knowledge. Cybercriminals like botnets because botnets give the criminal control of thousands of computers at once, and they help to hide the cybercriminal's identity.

How your computer acts when infected is dependent on what the cybercriminals are trying to accomplish. 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 nefarious purposes, such as identity theft, credit card fraud, spamming, and malware distribution. Bots can also be used to launch attacks on websites and networks, which as are sometimes referred to as Distributed Denial of Service Attacks or DDoS.

## How do you know if your computer is part of a botnet?

Botnets can be difficult to detect. In the past, sluggish performance and annoying advertisements were signs your computer was infected. These days, there may be no outward signs you have malware. Criminals try to hide their malware in an effort to infect as many computers as possible.

Internet service providers are beginning to take a proactive approach by issuing notices to customers when botnet traffic has been detected from their devices. You may have to opt in for the service. If you receive such a notice, confirm the legitimacy of the notice, then use the tools offered or take the steps indicated to check your device(s) and eliminate the malware. For more information, contact your Internet Service Provider.

## Are botnets illegal?

The installation of malware on the victim's computer, without the victim's consent, to build the botnet is illegal and the activity the botnet conducts may be illegal.

## How can you prevent botnets?

While 100 percent prevention is not possible, there are a few things you can do to dramatically reduce your computer's risk of infection, starting with these tips from STOP. THINK. CONNECT., the national cybersecurity education and awareness campaign:

### Keep a Clean Machine

- **Keep software current:** Having the latest operating system, software, anti-virus protection, web browsers and apps are the best defenses against viruses, malware, and other online threats.
- **Enable automatic updates:** Most security software will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- **Protect all Internet-connected devices:** Remember smartphones, tablets, gaming systems and other devices can be infected with viruses and malware, too. Protect them like you would your computer, including updating apps and operating systems.
- **Plug & scan:** USB sticks, thumb drives, CDs, DVDs and other external media can be infected by viruses and malware. Use your security software to scan them.

### Connect With Care

- **When in doubt, throw it out:** Delete any online communications (i.e., texts, emails, social media posts) that look suspicious, even if you think you know the source.
- **Get savvy about Wi-Fi hotspots:** When using a public or unsecured wireless connection, avoid using sites and apps that require personal information like log-ins.
- **Be cautious about "scareware:"**Cybercriminals have used fear to compromise your computer and to steal your personal information, which may include credit card information and banking login credentials. If you get security notices saying you are infected and need to purchase software, these could very well be attempts to compromise your device.

## If You Think You're Infected

If you are notified, become aware, or suspect your computer has become a bot, take immediate steps to remove malware. You can find a list of free botnet detection and remediation resources at www.stopthinkconnect.org/keepacleanmachine.

Learn about industry efforts to fight botnets at www.industrybotnetgroup.org.

NATIONAL CYBERSECURITY ALLIANCE

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY