Cybersecurity

Attacks, Threats, and Vulnerabilities

1.2.6 Bots and Botnets

What are bots and botnets and how can students defend themselves against them?

Overview

Given a scenario, the student will analyze potential indicators to determine the type of attack.

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 1.2

- Given a scenario, analyze potential indicators to determine the type of attack.
    - Command and control
    - Bots

Bots and Botnets

Botnets are a network of remotely controlled computers or "bots." A ***bot*** is a host that has become infected. Cybercriminals who control these botnets are referred to as botmasters. The botnet of computers work together to follow the directions of the botmaster. One common way to control botnets is through what's called ***command and control***. The bots will contact the botmaster who will then give them commands on what to do next. They can tell the bots to perform an action, do nothing and contact back at a certain time, or just communicate back so they know how powerful the botnet is.

A botnet's power is measured by how many bots operate as part of the network. The more bots that are connected the bigger the botnet, and thus, the bigger the potential impact. Botnets are used to create disruption online. Botmasters command the botnet to overload a website to the point where it is nonoperational (a distributed denial of service or DDoS) or to send out thousands of emails per second to spread spam messages.

Botnets can often be leased or sold on the black market. Botmasters can rent out the use of the botnet for a specified amount of time or purpose (two days or two million messages). When an attacker is trying to spread his message, or malware, to the widest audience possible, botnets are often used.

Botnets are usually not designed to compromise a single computer. They are designed to infect millions of devices. Botnets are often deployed through a trojan horse virus or some other malware. More complex botnets can even self-propagate by finding and infecting other devices automatically (such as the Conficker worm). Botnets take time to grow in size. Many bots will sit idle and wait for the botmaster's directions ("spam these people", "go to this website") via a command and control (C&C) channel. Early botnets relied on a single C&C server – either a single website or Internet Relay Chat (IRC) channel. As security researchers discovered which servers the bots

Teacher Notes:

were listening to, the C&C server could be taken offline, rending the botnet useless. New botnets communicate via distributed channels in a peer-to-peer manner to minimize the risk of the C&C being taken offline.

Defense

Prevention is the key when it comes to botnets. Stay up to date with security patches and updates for the operating system, applications, and anti-virus software. Avoid email attachments from suspicious or unknown sources. Scan downloads before executing files. Make use of firewalls to deny access from the host to the botmaster. Documented botnet vulnerabilities often provide the IP address and/or domain names of command and control servers that should be blocked.