Availability: Attacks, DDoS, and Bots

Created in partnership with Mandy Galante

TOPIC: FOUNDATIONAL PRINCIPLES OF CYBERSECURITY

GRADES: 6-8

LESSON DURATION: N/A

Introduction:

- This lesson is designed to get students thinking about foundational concepts of cybersecurity. It could be done by any teacher with a basic knowledge of technology but would best be utilized in a tech course.

Learning Outcomes:

- Students will describe basic attacks on availability and verbalize ways to prevent being a victim.

Materials:

- Video from Symantec about bots
- Video from Symantec about DOS
- Presentation of Cybersecurity principles

Activities:

1. The teacher should introduce the topic of the day: attack on availability, one of the foundational principles of cybersecurity.
2. The teacher may choose to use this presentation to review the basic foundational principles of cyber before beginning the discussion.
3. Explain that today the discussion with revolve around two different types of cyber attacks that involved availability: bots and DDoS. Both issues involve one's own computer being used against oneself or being used for malicious intent without one's knowledge.
4. Ask students to define bots and DDoS attacks. Give them time to research, if needed. Make sure all students understand before proceeding.
5. Begin the discussion with bots. What are bots? Why can bots be dangerous? What are some warning signs that your computer may be attacking as a bot? *A bot is a software application that runs automated simple and structured tasks on the Internet. Bots can perform much faster than a human. Bots can be used in both a positive and negative fashion. We will discuss bad bots. When your computer is infected, the malware is often a Backdoor program installed onto your PC. This malware gets into your computer by finding flaws or "holes" in the software/ operating system on your computer. They can be prevented by updating operating systems and*

software to close loopholes and dangers within the code. Malware infections can also occur through the use of free malware or adware from downloads.

6. Once a Backdoor program is installed, it is used to communicate back to the "Command & Control server (aka Botmaster) " of the malware. Your PC becomes a "bot" or "zombie", following program code from the Botmaster to send out spam or steal information or be part of a DDoS attack. A "Botnet" is a LOT of bots controlled by the C2. This Symantec video is a bit old but gives an accurate and entertaining explanation of Bots.
7. DDoS (Distributed Denial of Service) is an attack done by multiple users in which the goal is to take down a server by flooding it with traffic; therefore making it unavailable to users. The Botmaster sends the command to the Bot PCs and they all send requests to the victim server, so many that it can't answer them all and sometimes it even makes the server crash or shut down. Your computer could be used in a DDoS attack and you may never know it! This Symantec video is a bit old but gives an accurate and entertaining explanation of DDoS attacks. To bring this to life for students: have them complete this simple activity.
   A. Have each student in the room take a scrap piece of paper and make it into a ball. Choose a target in the room-a stuffed animal or an easy landmark. Tell the students that when you call their name-and only when you call their name, they should throw their paper ball at the target.

   B. Proceed to call a few students names-one at a time.

   C. Now have students make 3 paper balls each. On your command, everyone in the room should throw all of their balls at the target.

   D. After they have thrown them, explain that this is similar to a DDoS attack on a server. One request is easy to handle...however too many requests at once is overwhelming and mass chaos on the server.
8. But there ARE some good bots. These are automated software programs that run on the internet to run tasks that are simple and repetitive and can operate faster than a human. Some examples of good bots are chat-bots that are used to answer simple questions from users. (weather, sports scores, sales questions, FAQs).