LESSON NOTES

CYBERSECURITY

Domain 2.0 - General Security Concepts

2.4.3 - Trojans, Backdoors, and RATs

Lesson Overview:

Students will:

- Analyze potential indicators to determine the type of attack.

Guiding Question: What are trojans, backdoors, and RATs and how can students defend themselves against these attacks?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

2.4 - Given a scenario, analyze indicators of malicious activity

- Malware attacks
  - Trojan

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).

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Trojans, Backdoors, and RATs

In cybersecurity, a ***trojan*** is software that is downloaded and installed on a computer that may seem harmless but is malicious. The term "Trojan Horse" is a reference to a story from Greek mythology. There was a battle between the Greeks and the city of Troy. The Greeks had the Trojans surrounded but could not break through the city's walled defenses. The Greeks built a large, wooden horse and presented it as a "gift" to the Trojans before leaving. The people of Troy then pulled the horse statue into the city and celebrated their victory. At night, Greek soldiers who were hiding inside the horse emerged and opened the city's gates to let in their fellow Greek soldiers to take over the city. Usually, a computer trojan is hidden in an attachment to an innocent-looking email or a free download. When the victim downloads the program or clicks on the email attachment, the malware that was hidden inside is unleashed on the victim's computer. Unlike a computer virus, a trojan is neither able to self-replicate nor can it propagate without user assistance. Social engineering tactics are often used to trick users into downloading malicious applications.

A ***backdoor*** is a means to access a system or data that bypasses the system's customary security controls. When someone "leaves a backdoor open," this is a way to avoid the normal login process. Similarly, a burglar may be able to enter through an open backdoor even if the normal means of entry, the front door, remains closed and locked. Backdoors are often installed through malware. Some software contains accidental backdoors. Sometimes programmers create backdoors for maintenance during development and forget to close them prior to releasing the final code. In other cases, backdoors are deliberately left open by malicious software to allow intruders in.

Remote Access Trojans (RAT) are a specific type of trojan horse that includes a backdoor allowing for administrative or remote control of the infected host. A RAT allows hackers to connect via remote software. Once a RAT is installed, a hacker can remotely examine local files, log keystrokes, find passwords, take screenshots, or use the connection to download additional types of malware. There are other common types of trojan horses, including the Downloader trojan, the Distributed Denial of Service (DDoS) trojan, and the SMS trojan. The Downloader trojan is a type of trojan that targets a computer that is already infected by downloading and installing a new version of pre-existing malware. The DDoS trojan, as its name states, performs a DDoS attack attempting to take down a network by flooding it with traffic that comes from the victims infected computers. The SMS trojan infects mobile devices and can send or intercept messages.

Defense

To protect against trojan horses, do not download or run unknown or untrusted software. Verify the signatures and hashes of all new software before installing it. Ensure that all anti-virus and security software is up to date. Back up all important files and folders on a regular basis so that they can be recovered if a Trojan horse attack occurs. Lastly, be careful with email attachments, even from recognized senders. It is possible that a Trojan horse has infected the computer of a friend or family member and is using it to spread malware.