Module 11 Assignment

Nathan Cosendine

The seven steps of the cyber kill chain are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives.

Step 1 is Reconnaissance; during reconnaissance a bad actor will identify a target and find out their weaknesses. Attackers might also try and gather information through physical means such as talking to employees or looking in the business's trash for unshredded documents.

Step 2 is Weaponization; in this step the attacker creates or obtains malware, ransom ware, a virus, etc that they plan to use for the attack.

Step 3 is the Delivery phase, during this step an attacker will try and get the attack vector onto the system that they are trying to infiltrate. This can be in the form of phishing emails or by giving the target an infected USB drive. This stage can also more affective when combined with social engineering.

Step 4 is Exploitation, in this step the attacker executes the code that they had planted in step 3.

Step 5 is Installation, where the attack vector is actually installed onto the targeted device. With the attack vector installed, the attacker will have free access to the infected system.

Step 6 is Command & Control, during this step the attacker assumes control of the targeted device and established more entry points for the future.

Step 7 is Actions on Objectives and is the final step. This is the step where the attacker carries out their mission. The mission will vary from hacker to hacker but they could be financial gain, political and military motivations, or destruction of important data.

A real world example of a root kit attack might look like this.

During Reconnaissance, the bad actor identifies a bank as its target and gathers information on its online security system and also obtains a few of the employees email addresses. During the Weaponization phase, the bad actor creates remote access malware that they plan to use for the attack. During Delivery, the hacker infiltrates the banks systems by having a bank worker open an infected email and embedding the malware into the machine. During Exploitation, the attacker will now execute the malware. During Installation, the malware is then installed onto the bank's system. During Command & Control, the hacker remotely takes control over the bank's system and creates more access points for the future. During Actions on Objectives, the attacker will steal the banks' customer's important information and sell it for a profit.

To make the cyber kill chain model more comprehensive, a step could be added called Evasion. In this step an attacker would work to get around security measures to make sure that their presence is undetected while they carry out their attack. Often times an attacker will want to remain undetected for as long as possible so they can move around the system easier and without interference.

References

Spitzner, Lance. “Lance Spitzner.” *Cyber Security Training, Degrees & Resources*, 31 Mar. 2019, https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain/.

“What Is the Cyber Kill Chain? Introduction Guide: Crowdstrike.” *Crowdstrike.com*, 14 Oct. 2022, https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/.