Austin Cupp

CS 462

10/31/2022

The Lockheed Martin Corporation used inspiration from a military model to form the cyber kill chain, which was originally established to identify, prepare to attack, engage, and destroy the target network or system, and gain information. Since the cyber kill chains' formation, it has evolved to better anticipate and be able to recognize insider threats, social engineering, advanced forms of ransomware and innovative attacks. In the kill chain, there are several core stages that take place. They range from reconnaissance, which is the first stage in a malware attack, to lateral movement, where they move laterally throughout the network to get access to more data, and to data exfiltration which is getting the data out. All the common attack vectors, whether they are phishing or brute force or the latest strain of malware, trigger activity on the cyber kill chain. A step that could make the cyber kill chain even more comprehensive would be to add a step that involves Privilege Escalation Attacks. This step would be important because it can help attackers gain more privileges on a system to get access to more data and permissions. For a privilege escalation attack, they need to escalate their privileges often to an admin. What do privilege escalation attacks even do? Privilege escalation attacks exploit weaknesses and security vulnerabilities in the systems with the endgame goal of elevating access to a network, applications, and mission-critical systems. There are 2 main types of privilege escalation attacks, them being a vertical attack and a horizontal attack. A vertical attack is when an attacker can gain access to an account with the intent to perform actions as that user, while a horizontal attack gains access to account with limited permissions, which requires an escalation of privileges, such as an escalation to the administrator role, in order to perform the desired actions. What is a privilege escalation attack? Privilege escalation is an attack vector that a lot of businesses face due to the loss of focus on various

permission levels due to having to focus on other sectors. As a result, security controls end up not being sufficient enough to prevent a privilege escalation. When do these attacks occur? Privilege escalation attacks occur when the cyber attacker is able to gain access to an employee's account within an organization, then is able to bypass the proper authorization channel, and finally is able to successfully grant themselves access to data they are not authorized to have. Process injections, Android Metasploit's, and Linux password user enumeration are examples of a privilege escalation attack. This step would add more comprehension to the cyber kill chain because an important aspect of a successful cyber attack is being able to gain necessary control of the system or network in order to gain the target data and information. If a cyber attacker is able to gain administrator privileges and act as the authorized individual, it makes the rest of the kill chain almost easier to complete, due to being able to gain the necessary data and complete the remaining tasks on the chain.

Sources:

Allen, J. (2022, October 24). *Privilege escalation attacks: Everything you need to know*. PurpleSec. Retrieved November 1, 2022, from https://purplesec.us/privilege-escalation-attacks/

Myers, L. and Korolov, M. (2022, April 14). *What is the cyber kill chain? A model for tracing cyberattacks.* CSO Online. Retrieved November 1, 2022, from https://www.csoonline.com/article/2134037/what-is-the-cyber-kill-chain-a-model-for-tracing-cyberattacks.html