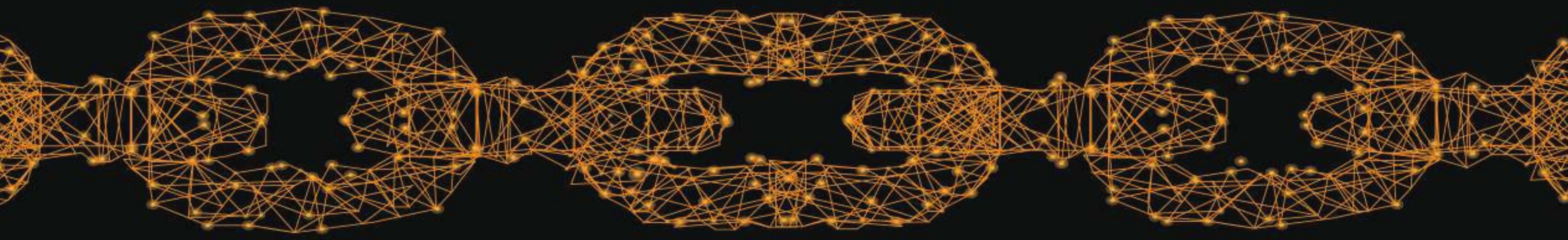
Lodestone

Mastering the Cyber Kill Chain

Step Four: Exploitation



STEP FOUR: EXPLOITATION

Knock, knock, open up the door – it's real! While DMX is unlikely to be the threat actor, exploits certainly can give it to you, and with potentially devastating effects to your business. Once malicious tools have been surreptitiously placed within the boundaries of a target environment, cyberattacks are primed and ready to strike at the first command or trigger.

Exploitation is the fourth step in Lockheed Martin's Cyber Kill Chain®, a framework that outlines the common steps attackers take during a security event or incident. In the earliest steps, Reconnaissance and Weaponization, information about a potential victim or group of victims is collected and used to develop tools that can exploit weaknesses in their environments. Delivery is then used to place these tools at or near the target in preparation to launch a cyberattack.

For cyberattacks from the meticulously planned to spur-of-the-moment attempts, this is where abstract theory is translated into direct action. Malicious code is triggered, malware attempts to run, and the threat actors' plans for the cyberattack are put to the test. Successful execution rewards them with the compromise of the targeted account, system, or other section of the network; however, even failed execution attempts can have adverse effects and damage an environment.

EXPLOIT MARKS THE SPOT

Threat actors must exploit a vulnerability to gain unauthorized access to an environment, whether it be software, hardware, or even human. These may include known flaws that can be used against unpatched systems, or zero-day exploits that have never before been seen. Once placed, malware can be activated remotely or set off by pre-determined factors, such as time of day. However, attackers may not have sufficient access to the environment at that point in time to do so. Here, too, employees serve as a critical line of defense – it only takes a single individual lacking the appropriate security awareness training to be tricked into executing a malicious file by a threat actor posing as a legitimate party.

This monthly series, Mastering the Kill Chain, follows the impact of each step in the Cyber Kill Chain® on three fictional businesses: The Second Breakfast, a small, local brunch restaurant; Fhloston Paradise, a moderately-sized operation that manages spa retreats for celebrities; and Cash Williams, a retail giant that uses a complex infrastructure to sell outdoor goods online and across numerous locations across the country.

The first of these hypothetical businesses, The Second Breakfast, has a small attack surface but limited funds to dedicate to security. As a result, an opportunistic attacker performing reconnaissance identified an unpatched system facing the public Internet and weaponized this vulnerability by downloading malware for a botnet, delivering it onto the system using a known exploit for the outdated version of the exposed system.

Despite the measures it takes to protect the confidentiality of its high-profile clients, Fhloston Paradise is also now in the danger zone of exploitation. After using reconnaissance to identify a “Contact Us” page with a form that included a scripting error, the attacker weaponized the vulnerability with a custom script that delivered a ransomware package into the environment.

Finally, Cash Williams is in a precarious position. Attackers easily collected a wealth of information about the company and its organization during the reconnaissance phase thanks to the company’s recent boom in success and subsequent media coverage. The threat actor has prepared weaponized malware and tricked an unwitting employee into delivering it into the network by posing as a member of the remote Information Technology (IT) team.

SERVING SECOND BREAKFAST

Small companies like The Second Breakfast are often mistakenly lured into a false sense of security by the belief that they have little value to attackers. The truth, however, is that they are still prime targets, especially for novice hackers or as part of a larger-scale attack. By using a known flaw in an outdated, unpatched, and external-facing systems, a threat actor can hijack the resources of several small companies for use in a botnet to perform denial of service attacks, mine virtual currency, or perform other malicious activities using their combined computing power.

In the Exploitation step, the malware that has been placed on The Second Breakfast’s outward-facing systems must be activated to allow the attacker to gain control of them. However, because the systems face the public Internet, the attacker can communicate with relative ease and without much risk of detection. By configuring the malware to await instructions from an attacker command-and-control (C2) server and activate itself when prompted, the attacker can simply send that instruction to cause the malware to install itself and go to work.

POUNCING ON FHLOSTON PARADISE

Businesses with particularly sensitive, protected information like Fhloston Paradise may be careful with storage and passwords, but attackers are creative – it only takes one gap in the armor to potentially slip through. Data such as Personally Protected Information (PII), credit card information, or Health Insurance Portability and Accountability Act (HIPAA) information is valuable, and the loss of or unauthorized access to such data can spell disaster for a company, from lawsuits to the loss of important certifications.

Ransomware has become popularized with well-known threat actor groups such as REvil for the bargaining chip it provides to threat actors to make monetary demands of victims. The ransomware version lurking in Fhloston Paradise's environment will, when run, exfiltrate as much data as possible to an attacker-controlled server before attempting to delete backups and shadow copies and encrypt all data and systems. Even if the ransomware is unable to spread to the entire company, locking down critical portions of the network such as file shares could be enough to cripple operations.

COMPROMISING CASH WILLIAMS

Security awareness is crucial for companies of all sizes, but especially for large companies like Cash Williams, where hundreds of employees are spread out across the country. Even with a strong security setup that includes monitoring and automatic responses, attackers can deceive personnel into thinking they are members of the IT team or new employees. From there, they may be able to convince legitimate employees to unknowingly download and deploy malware.

Once the attacker has played off the goodwill and inexperience of a member of Cash Williams' staff to install malware, convincing them to double-click the file and run it sets the stage for their next step. They may use cover stories such as being a member of IT that needs to walk through installation for a new, required piece of software on employee workstations. From there, with little to no technical work, they can activate the malware that will allow them to fully exploit the system or environment at large. Even if the first attempt isn't successful, Cash Williams' size provides a wealth of employees to target; the attackers need only one susceptible individual to gain a foothold.

EXPECTING (AND EXPELLING) EXPLOITATION

Exploitation represents the phase in the Cyber Kill Chain® in which a cyberattack is truly put to the test. Even if the malware or malicious files do not perform as expected, however, they may still cause massive outages, data loss, or corruption. The key to defending against the Exploitation step is a combination of traditional, resilience-based hardening measures and a strong awareness of a company's environment and its most critical resources. As Paul Brunney, a Senior Consultant in Lodestone's Forensic Investigations group advises, "Know your threats. What would [an attacker] be trying to do, and what do I have to worry about from where I'm at?"

Prior to joining Lodestone, Brunney operated as a cyber warfare expert with the National Security Agency (NSA). As a post-breach case lead that runs investigations into cyberattacks including business email compromises (BECs), ransomware, and more, he has seen exploits from weak configurations to threat actors physically entering a company's building to directly install malware. In addition, the cyberattack landscape is always changing, with new techniques coming to the forefront. "Phishing has gotten super sophisticated – it's not always just malicious links," he said.

Brunney recommends that companies implement thorough training, hardening, and monitoring to help stop exploits, including:

- Security awareness training.
- Logging and endpoint process auditing.
- Regular backups and segregated networks.
- Secure coding training, including OWASP.

In the examples described above, endpoint monitoring and response could have helped The Second Breakfast and Fhloston Paradise detect and isolate malware the moment it began running within their environments. Meanwhile, Cash Williams could have combatted more sophisticated forms of social engineering by implementing and regularly testing employees and implementing protocols for IT personnel, for example, to confirm their identities when requesting access to a workstation.

Brunney recommends a combination of protection and resiliency to strengthen the security posture of an environment. With cyberattacks becoming increasingly common and widespread, hardening alone cannot provide the resources companies need to bounce back from both successful and unsuccessful compromise attempts by threat actors. However, with thorough logging and monitoring and strategies to protect a business' most critical functions, companies can place themselves in the best position possible to defend themselves from threats, wherever they originate.

Exploitation is the fourth stage of the Cyber Kill Chain® – by encouraging awareness and building protection and resiliency into their environments, companies have an opportunity to stop cyberattacks just as they begin. For more information on cybersecurity and resources to prevent and respond to breaches, visit https://lodestone.com/contact/.

This article is the fourth in Lodestone's seven-part series that explores Lockheed Martin's Cyber Kill Chain® framework. Explore examples of companies facing cyber adversaries and learn strategies to combat malicious activity at every step in the process. Look for another spotlight on the first Wednesday of each month. For additional details and a full schedule of upcoming releases, visit https://lodestone.com/insight/introducing-our-spotlight-series/.

Lodestone Security is a wholly owned subsidiary of Beazley plc. Lodestone provides computer security and cybersecurity consulting services. Lodestone does not provide insurance services and client information obtained by Lodestone is not shared with Beazley claims or underwriting. Likewise, client information obtained by Beazley claims or underwriting is not shared with Lodestone.

www.lodestone.com
320 E. Main Street
Lewisville, TX 75057

6