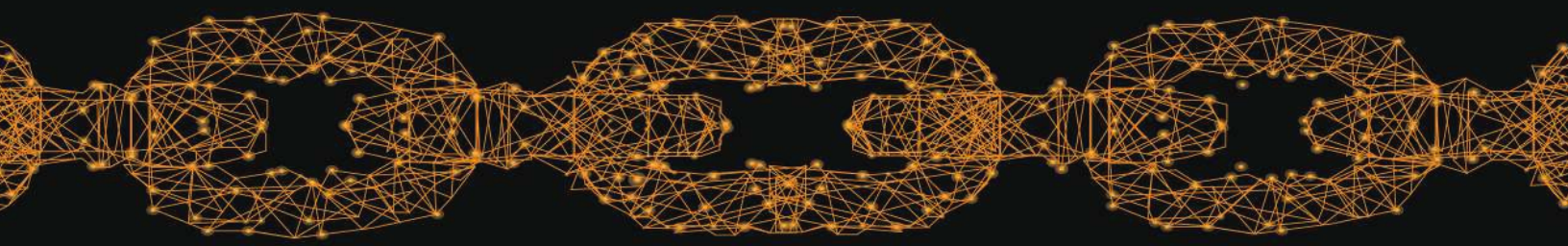
Lodestone

Mastering the Cyber Kill Chain

Step Two: Weaponization



STEP TWO: WEAPONIZATION

"Knowledge is power"—this famous adage, rooted in Latin origins, rings true today in ways its originators could never have imagined when it was first recorded thousands of years ago. The success or failure of an attack hinges on the intersection of the information attackers have gleaned about a potential target, and their ability to translate that into a weapon to use against them.

This process, Weaponization, is the second 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 first step, Reconnaissance, attackers study their potential victims to learn about potential weaknesses in their environments. These efforts have varying levels of sophistication, depending on whether the attackers are common opportunists looking for a small payday, or an advanced threat actor being driven by a powerful nation-state.

Weaponization represents the second half of preparing a cyberattack. Attackers consider the information gained from the reconnaissance phase and begin collecting and developing tools to exploit it. This can include the generation of malware or configuring existing malware through public or private channels and configuring it to address specific vulnerabilities in a prospective victim's environment.

FROM KNOWLEDGE TO POWER

Attacker strategy during the Weaponization phase is strongly influenced by the original motivation behind selecting the target. If a wide scan across the Internet happened to pinpoint a vulnerable target, the end goal, and the tools needed to achieve it may differ greatly from a specific, hand-picked target.

The previous entry in this series, Mastering the Kill Chain—Step One: Reconnaissance, introduced three hypothetical businesses of various sizes: The Second Breakfast, a small brunch spot that relies little on technology; Fhloston Paradise, a spa retreat for the rich and famous with a handful of locations; and Cash Williams, a retail giant that sells outdoor goods, including chainsaws, through a complex infrastructure.

The smallest of the three examples, The Second Breakfast, has a small attack surface but few resources to devote to security. As a result, an attacker performing the Reconnaissance step was able to identify a few unpatched, outward-facing systems. In addition, their website provides many specific details, including the format of

employees' email addresses (e.g., First.Last@secondbreakfast.com) and the full names of long-time employees.

Fhloston Paradise, the hypothetical medium-sized business, takes additional measures to protect the confidentiality of its high-profile clients. However, a recent email dump from a vendor the company worked for in the past revealed details about Fhloston Paradise locations. In addition, an attacker exploring the company website was able to identify a "Contact Us" page that included a form with a scripting error.

The largest company, Cash Williams, has been gaining a lot of media attention with its growing success. As a result, an attacker simply searched the Internet to locate promotional articles on the company's partnerships with other vendors, identifying what brands of equipment they use, and personal details on the company's executives through their social media profiles, such as LinkedIn.

PREPARING SECOND BREAKFAST

Operators of small businesses like The Second Breakfast may think that there is little return on investing in security, as they are too small to be a valuable target to attackers, this is often simply not the case. Opportunistic attacks using commodity malware are on the rise, with attackers using searches for Internet-connected devices or Internet-wide scans to locate easy targets. These targets can become practice for inexperienced attackers or unwittingly looped into a larger attack.

An attacker that has performed reconnaissance on The Second Breakfast and identified some unpatched, Internet-facing systems, may consider it as an opportunity to add to an existing botnet. A botnet is a group of external-facing devices that have been placed in the control of an attacker using malware. Botnets can be used to perform denial-of-service attacks, steal credentials, or send spam without the knowledge of the legitimate owners of the devices involved.

To force The Second Breakfast's vulnerable devices to join the botnet, the attacker could use known vulnerabilities for the unpatched systems to infect them. The malware used to infect other members of the botnet could be reconfigured to exploit the known vulnerability and install the malware on The Second Breakfast's systems. From there, the malware could use the same functions it does in other systems to connect to attacker command-and-control (C2) servers.

TARGETING FHLOSTON PARADISE

Malware generation for Weaponization is often an automated process that combines an exploit to infect a system with malware that affects the system once compromised. This malware may be created in-house by the attackers that use them or purchased or obtained from other attackers through public or private channels.

In the case of Fhloston Paradise, an attacker that has identified a scripting error in the company's website may find an opening to use a cross-site scripting attack. Cross-site scripting attacks use unprotected or misconfigured forms on benign or trusted websites to inject malicious code. By injecting code into data that gets stored in an internal system—in this case, contact information for prospective customers of Fhloston Paradise that attempt to contact them through a website—an attacker may be able to use the system as an entry point to spread malware within the target's environment.

WEAPONS AGAINST CASH WILLIAMS

Large-scale operations like Cash Williams are more likely to be targets themselves, as they can offer more valuable payouts for attackers. An attacker with reconnaissance information on Cash Williams may see an opportunity to compromise the account information of many individuals at once, using it to steal as much money as possible before they are detected and ejected from the environment.

To prepare, an attacker might begin planning a phishing campaign to steal a large sum of money that Cash Williams pays to one of its vendors each quarter. By scouring LinkedIn, the attacker could compile a list of employees that are in or adjacent to the accounting department that likely handles such payments. In addition, the attacker could use information about the Chief Financial Officer (CFO) and prepare the content of an email in which they pose as the CFO.

Weaponization for social engineering attacks may include developing scripts or drafting emails that are as convincing as possible to trick legitimate employees into following attacker instructions, such as updating the routing number of the bank account where payments for a vendor are usually sent.

WARDING OFF WEAPONIZATION

Similar to Reconnaissance, protecting an environment against Weaponization may seem near impossible—and indeed, weaponization cannot be detected as it happens. However, there are ways to prepare and study the artifacts of weaponization from past attacks. Sharrone Berry-Davis, a Senior Consultant in Lodestone's proactive Security Consulting group, has been "on both sides of the table" as a penetration tester and in his current role.

Berry-Davis states that a key factor in defending against Weaponization is both internal and external awareness. This includes a company being fully aware of its own attack surface, and how it might change over time. He emphasizes that while there is no environment that is perfectly secure, there are ways companies can compensate for nicks in its digital armor. "Look at the whole of everything. If you know where you're vulnerable, you know where to put additional protections."

In addition, some advanced persistent threat (APT) groups target specific industries. Companies in these industries can take advantage of information sharing with other companies and government entities regarding indicators of attacks that have become common in recent times. While some companies hesitate out of fear of revealing weaknesses, this information sharing can help industries become stronger together.

Berry-Davis also recommends the following strategies to harden an environment against Weaponization:

- Fund and support internal security efforts.
    - External advice from hired consultants can help convince executives of the importance of investing in security.
    - Dedicate a couple of individuals at a minimum to maintaining patches and ensuring the environment is kept up to date.
    - Automated resources like antivirus (AV) and security incident and event management (SIEM) can identify what is normal for an environment and alert on anomalies or specially configured indicators.
- Promote company-wide security awareness.
    - Perform quarterly vulnerability assessments, in which personnel scan the company's own environment for external-facing vulnerabilities and manually validate them.

- Annually, perform a penetration test by hiring a third party or assigning internal personnel to attempt to actually exploit the vulnerabilities detected in the assessments or that can be identified externally.
- Train all personnel and periodically send fake phishing emails to encourage employees to identify and report suspicious behavior. For attackers that cannot gain a foothold into the environment using a vulnerability, targeting a company's people with a social engineering campaign is often consider the next solution.

Both The Second Breakfast and Fhloston Paradise could defend against attackers weaponizing information they have gained by supporting security efforts. Vulnerability scans are capable of identifying vulnerabilities such as scripting errors in a website, and keeping all resources patched and up to date renders vulnerabilities based on old versions moot.

Additionally, by keeping personnel aware of potential attacks via security awareness training, companies like Cash Williams can decrease the likelihood of any planned social engineering attacks being effective.

Weaponization is the second stage of the Cyber Kill Chain®—by understanding their own vulnerabilities and preparing personnel, companies have the chance to weaken or eliminate attackers' ability to effectively weaponize information they collect about their environments. For more information on cybersecurity and resources to prevent and respond to breaches, visit https://lodestone.com/contact/.

This article is the second 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/.

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