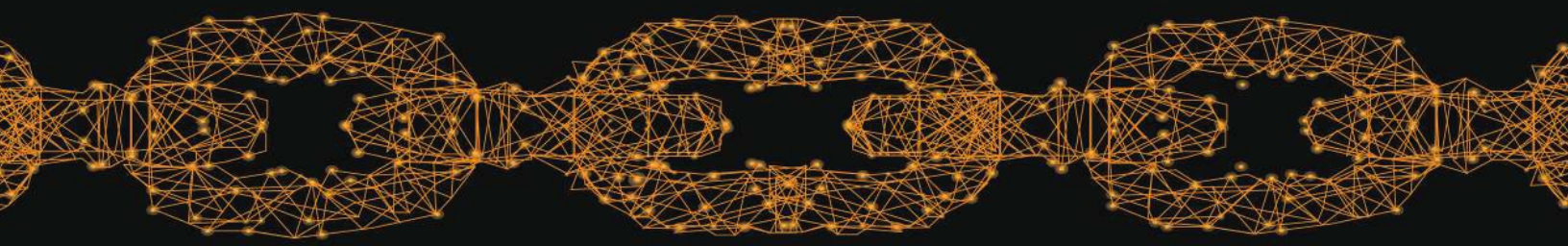
Lodestone

Mastering the Cyber Kill Chain

Step Five: Installation



STEP FIVE: INSTALLATION

"We're in." This line, one of the favorite cliches of hacking in Hollywood, is often uttered as fingers fly across a keyboard and colorful graphics dart across the screen. While this is, of course, classic dramatization, in it lies a grain of truth: once a threat actor is able to penetrate a victim's environment, they become all the more dangerous and more difficult to shake. This is often caused by the threat actor embedding themselves into the systems they were able to compromise to maintain their hard-earned, unauthorized access.

Installation is the fifth 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, and Exploitation is attempted to launch a cyberattack.

This step comes into play if the threat actors' attempt at exploitation was successful enough to provide a foothold into the environment – even if a single user account was all that could be compromised. Systems can be fickle, and unknowns within an environment could cause a threat actor to be booted out of the network by chance or by design. As a result, many threat actors make it a priority to establish a beachhead on an account or system they have been able to compromise, to allow them to easily re-enter the environment if necessary.

INSTALL TACTICS

The tools of installation at a threat actor's disposal once in a victim's network come in two flavors: malware files and file-less malware. The former is what comes to mind for most when picturing a cyberattack, where a "bad" file infects a system and is spread. The reality, however, is more complex: even if a threat actor only needs a malware file to run at intervals or at a specific time to maintain persistence, plopping a strange file on a system can easily trigger red flags from an antivirus (AV) solution or astute personnel. Steps must be taken to place malware where it is unlikely to be found, such as in a startup folder or scheduled as a task in Windows. File-less malware avoids this issue by being embedded into a system's operations, such as the Windows Registry, or having its code injected into existing, legitimate code. The end goal is typically to establish a backdoor into the system that can allow

threat actors to maintain their access for an extended period of time and more easily bring additional malware into an environment to compromise additional systems.

Each entry in this series, Mastering the Kill Chain, has explored the effect of a different step in the Cyber Kill Chain® on 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 small business example, The Second Breakfast, has a limited attack surface but few resources to designate for security. As a result, an opportunistic threat actor 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. The malware was triggered by a command from threat actor to run.

Fhloston Paradise, a medium-sized business, takes additional measures to protect the confidentiality of its high-profile clients. However, after using reconnaissance to identify a “Contact Us” page with a form that included a scripting error, the threat actor weaponized the vulnerability with a custom script that delivered a ransomware package into the environment. While the ransomware portion of the malware must be run last, as it will encrypt and effectively lock out systems, other portions are focused on stealing as much sensitive data as possible before the threat actor makes their presence known.

The largest example, Cash Williams, has been gaining a lot of media attention with its growing success. Threat actors easily collected a wealth of information about the company and its organization during the reconnaissance phase thanks to the company’s recent boom. 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. After tricking the employee into executing the file, the threat actor now has a starting point in the environment from which they can work to further infiltrate the environment.

SETTLING IN FOR SECOND BREAKFAST

Owners of small businesses like The Second Breakfast may feel protected, to an extent, by the idea that their environments are of little value to threat actors, and therefore provide little incentive to attempt a cyberattack. However, this is a false sense of security: a small business is a prime target for a novice hacker, or "script kiddie" using pre-packaged malware, or as part of a larger-scale attack. In this example, The Second Breakfast's external-facing systems are being targeted by threat actors to be used as part of a botnet that forces compromised networks to use their resources for nefarious purposes at the command of the threat actor.

Combining The Second Breakfast's resources into a larger botnet requires a threat actor to maintain access to compromised systems for an extended period of time, while other victim networks are added to the botnet or the larger attack, such as denial-of-service attacks or virtual currency mining, can be set into motion. As such, the threat actor might look to establish persistence during the Installation step by hiding malware files in system directories and creating a scheduled task that triggers the malware to re-establish its connection to the botnet at set intervals of time. This provides the threat actor with a way back into the environment if they are somehow disconnected.

CHECKING INTO FHLOSTON PARADISE

Ideally, medium-sized businesses have more resources to devote to security and maintaining visibility into the current states of their environments. However, companies like Fhloston Paradise with sensitive, protected information such as Personally Protected Information (PII), credit card information, or Health Insurance Portability and Accountability Act (HIPAA) information can be particularly tempting targets for threat actors. For this example, the private information about its clients is exactly what the threat actors are after.

Ransomware has become an increasingly common cybersecurity threat and involves threat actors encrypting numerous or key systems within a victim's environment and demanding a fee to provide the decryption key needed to recover the information. A less-discussed aspect of ransomware, however, includes the exfiltration of sensitive data from these systems before the actual ransomware is launched. The threat actors then have the opportunity to sell the information for a profit or may use it as an additional bargaining chip to blackmail its victims for more money to prevent its public release.

For Fhloston Paradise, with the ransomware package already delivered, the threat actors may use the Installation step to set up a beachhead on a particularly useful system. Current ransomware often establishes persistence by using Windows' PsExec function, a legitimate tool used to execute code on remote systems that can be used to run malicious code instead. This activity can buy threat actors time to dig into the environment and search for additional systems and servers to compromise, steal information from, or both.

CAMPING OUT AT CASH WILLIAMS

While large companies have the disadvantage of having similarly large, complex environments, they benefit from having the personnel and resources to dedicate to a full security team that can have a deep understanding of the business' network and knowledge of what normal, healthy operations look like. Cyberattacks can still come from a number of different angles, including through the social engineering of company employees who may be less aware of the dangers of phishing and other threat actor tactics. In the case of Cash Williams, this is exactly what has proven to be the break in their armor: a threat actor has posed as a member of the IT team and convinced an employee to install and run malware disguised as a legitimate program.

The malware that was successfully delivered and executed within Cash Williams' network included the means for the threat actor to establish a connection via Remote Desktop Protocol (RDP), another legitimate tool that can be used for malicious purposes. With RDP allowing the threat actor to perform actions as if they were sitting at that workstation and using the mouse and keyboard themselves, they have the opportunity to run diagnostics or set up a web shell that instructions can be fed into even if the RDP connection is lost. The threat actor may also discover new endpoints to connect to or key file shares associated with critical operations within the company. It is even possible that the compromised employee unwisely stored the passwords for all of the Cash Williams accounts they manage in a file on their desktop, to which the threat actor now has access.

KEEPING INSTALLATION OUT

Installation serves as the phase in the Cyber Kill Chain® in which a successful cyberattack enables a threat actor to begin embedding themselves more deeply into a victim's environment. The goal of this phase is typically to establish persistence, or a backdoor into the environment that the threat actor can use to maintain their unauthorized access to a network without having to retrace their steps if they are

accidentally disconnected or booted off of a system by a remediation attempt. The strongest defense against the Installation step is one that balances maximizing a company's visibility into and understanding of its own environment with practical limitations, like resource allocation and funding. "Work within your budget to create some type of detection system that fills the gaps in your AV," says Mike Wirtz, a Senior Consultant in Lodestone's Forensic Investigations practice. Otherwise, "make sure you're investing in [next-generation] AV."

With over a decade of experience in cybersecurity from the Department of Defense to the public sector, Wirtz brings his talents to Lodestone as a post-incident case lead that investigates cyberattacks to provide clarity and knowledge to companies in the midst of some of their most difficult moments. As an expert in malware analysis, Wirtz keeps his finger on the pulse of trends in cyberattacks through open-source intelligence and disassembling and examining code used by actual threat actors in the wild. One of the most common mistakes he has observed by companies is purchasing useful monitoring tools like AV or security information and event management (SIEM) systems but failing to set up and test them correctly. "Be more proactive than reactive. Most of these [threats] are fairly easy for these products to detect, they just need to be configured correctly and be looking for them."

Wirtz emphasizes that even for steps like Installation, which occur when a threat actor has already penetrated an environment, "an ounce of prevention is worth a pound of cure." He recommends that companies equip themselves to effectively detect threat actor activity by giving themselves the advantages through avenues such as:

- Investing in robust AV, SIEM, and other security products that are configured specifically for the environments they monitor.
- Regularly testing security products in place to identify any gaps in network visibility.
- Gaining an in-depth understanding of baseline activity in an environment, including what normal, baseline behavior looks like.
- Keeping up with cyber security news and alerts released by government agencies like the United States Computer Emergency Readiness Team (US-CERT) and the Cybersecurity and Infrastructure Security Agency (CISA), paying special attention to threats specific to the industry the company operates in.

In the hypothetical scenarios described above, preparation with wide visibility into their environments and robust, well-configured monitoring tools could have helped these companies quickly detect the presence of threat actors and address cyberattacks before malware could be further embedded into their systems. Even for a small company like The Second Breakfast, understanding what activity would be considered unusual in their environment could allow personnel to easily recognize potentially malicious behavior.

For companies that have detected a threat actor during the Installation step, Wirtz recommends reaching out to a professional response team. Isolate the system or systems in question, taking care to preserve data that could be critical to a digital forensics and incident response (DFIR) investigation. Wirtz adds, “Engage your incident response plan. If you don’t have one, you should make one.”

Installation is the fifth stage of the Cyber Kill Chain® – by focusing on being proactive rather than reactive, companies have an opportunity to catch threat actors within their environments before they become even greater threats. For more information on cybersecurity and resources to prevent and respond to breaches, visit https://lodestone.com/contact/.

This article is the fifth 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