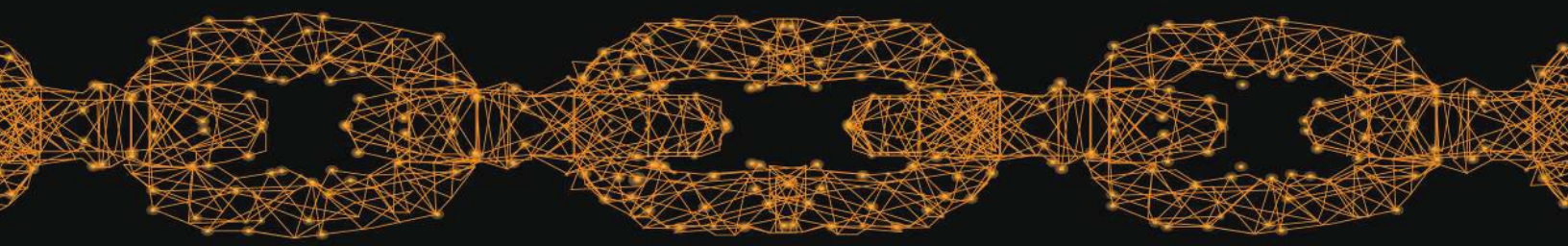
Lodestone

Mastering the Cyber Kill Chain

Step Six: Command and Control



STEP SIX: COMMAND AND CONTROL

As 80s synth-pop darlings Tears for Fears famously sang, “Everybody wants to rule the world.” Stripped of the supervillain antics terms like “world domination” bring to mind, this is a sentiment that motivates every threat actor. Whether it is through ransomware, botnets, or other malware, the ideal outcome for a threat actor is taking unauthorized command of as many systems and as much data as possible. While the specifics may differ between the humble script kiddie and the money-motivated hacker or nation-state-driven Advanced Persistent Threat (APT), control is the ultimate goal.

Command and Control (C2) is the sixth step in Lockheed Martin’s Cyber Kill Chain®, a framework that outlines the common steps attackers take during a security event or incident. This vicious cycle begins with Reconnaissance, Weaponization, and Delivery, when information about potential victims is collected and transformed into tools that attempt to exploit weaknesses in vulnerable environments. Depending on the success of that Exploitation, threat actors may be able to move to the Installation step and set the stage for even more malicious activity.

If undetected, the successful establishment of a base of operations allows a threat actor to initiate the second to last stage of the Cyber Kill Chain®: creating channels that can be used to remotely control compromised systems. These channels are designed to allow commands to be received from the outside world, enabling threat actors to maintain their hold over target environments if they lose their previously obtained access by accident or design. Remote-control capabilities open a myriad of avenues for escalating malicious activity or branching out anew, all at the expense of the victim.

ASSUMING DIRECT CONTROL

As Lockheed Martin states in its description of the Cyber Kill Chain, the C2 step represents “the defender’s last best chance to block the operation,” and one of the final phases of an active cyberattack. While, in practice, it often overlaps with the previous phase, Installation, C2 focuses on establishing a channel not merely for persistence, but to allow the threat actor to force systems to execute remote commands. This often requires a two-way mode of communication, such as Domain Name Service (DNS), web, or email protocols, that results in systems sending information to a threat-actor-controlled external network and receiving commands to carry out within the targeted environments. Note that the external network the threat actor uses, referred to as a C2 server, may not actually belong to the threat actor, but instead belong to another victim’s network and repurposed for malicious use.

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 local eatery with a handful of systems; Fhloston Paradise, a resort favored by the rich and famous and with multiple locations; and Cash Williams, an online-based retail giant focused on outdoor goods, including chainsaws.

The Second Breakfast, a small business with a single location, has few systems in its network but similarly limited resources to use for security. A threat actor scanning the Internet identified an unpatched, public-facing system and exploited it to install malware for a botnet. The threat actor was able to spread the malware to a few other connected systems. The threat actor is poised to launch a botnet that will force The Second Breakfast's systems to join a group of compromised systems from other compromised networks to target additional victims.

The medium-sized example, Fhloston Paradise, is a luxury health retreat and resort with wealthy clientele. A major contribution to the popularity of its locations is the additional measures it takes to protect the confidentiality of the client information stored in its databases. A threat actor researched Fhloston Paradise as a potential lucrative target and identified a scripting error on the business' website. The threat actor exploited this vulnerability to install ransomware on a number of the systems on the Fhloston Paradise network, with plans to use the malware to steal sensitive data and force the business to pay a ransom to regain access to their data.

Finally, Cash Williams is a fictional online retail giant with a complex infrastructure that allows customers to purchase outdoor goods and receive them through a rapid delivery system. Recent media coverage about the company's growing success attracted the attention of a threat actor that has researched and prepared custom malware to target the business' environment. After posing as a member of the Cash Williams Information Technology (IT) team, the threat actor convinced a legitimate employee to execute the malware and install it in the network.

SEIZING SECOND BREAKFAST

It is essential that small businesses like The Second Breakfast are aware that they are not safe from cyberattacks because they have equally small environments: all targets are fair game to threat actors. Not only are they prime targets for novice hackers using pre-packaged malware, but even a handful of systems can add value and computing power to a large-scale attack being orchestrated by a threat actor. In this hypothetical example, this large-scale attack is a botnet, in which compromised networks from a number of different targets are forced to redirect their resources to malicious activities such as denial-of-service (DoS) attacks or mining cryptocurrency.

In the previous step, the threat actor established a backdoor into The Second Breakfast's environment by hiding malware files in system directories and creating a scheduled task that triggers the malware to re-establish its connection at set intervals of time. The C2 step takes this further by using additional malware or malware features to establish a connection between the system and a C2 server controlled by the threat actor. With this channel successfully created, not only can the threat actor re-enter the environment if they are kicked off – they can also ping the system for availability and resource information and send commands for systems to carry out, including assisting with cyberattacks on other organizations.

PUPPETEERING FHLOSTON PARADISE

The success of many businesses, including the fictional Fhloston Paradise, hinges upon the ability to appropriately manage and protect sensitive information such as Personally Protected Information (PII), credit card information, or Health Insurance Portability and Accountability Act (HIPAA) information. Since a failure to prevent this data from falling into the wrong hands has especially serious repercussions, including fines, the loss of key certifications, and even legal consequences, a threat actor may consider companies with large amounts of this information to be particularly valuable targets for cyberattacks such as ransomware.

The main focus of ransomware is to encrypt as many business-critical systems as possible with a key known only by the threat actor, effectively locking a business out of its own data. The threat actor then contacts the victim to demand payment in exchange for the decryption key. In this case, a threat actor is poised to begin the encryption process after exploiting a misconfiguration in the Fhloston Paradise website to deliver and spread malware throughout the business' environment.

A less well-known, but common additional step in a ransomware attack includes the exfiltration of critical data for blackmailing purposes. Ransomware groups often claim to have collected large volumes of a victim's data, occasionally providing examples of the files they have taken as proof and demanding additional payment to prevent the public release of this information. The successful execution of the C2 step in this context, therefore, equips the threat actor with the means to not only launch the encryption process, but to command systems to access and exfiltrate sensitive data from within Fhloston Paradise's network.

COMMANDEERING CASH WILLIAMS

Large companies have prominent advantages and disadvantages as a result of their size: while their environments can be complex and difficult to monitor, these organizations often have the resources to dedicate a full security team. If this security team is remote or not well-known to all employees, however, threat actors can leverage this lack of communication for a variety of malicious activities, including social engineering – in this particular case, the threat actor has broken through Cash Williams' defenses by social engineering a legitimate employee and tricking them into installing and running malware disguised as a legitimate program.

After establishing persistence via a Remote Desktop Protocol (RDP) connection, the threat actor was able to discover new endpoints and key file shares. A channel was set up via a web shell to support C2, allowing compromised systems to communicate with the C2 server and receive commands from the threat actor without the need for the threat actor to re-enter the environment. A well-established C2 channel can provide the threat actor with full control of several key Cash Williams systems to carry out any number of more advanced cyberattacks.

TAKING BACK CONTROL

The C2 step of the Cyber Kill Chain® represents one of the final opportunities to combat a cyberattack in progress. While successful Installation allows a threat actor to deeply embed themselves into an environment, C2 is where threat actors may truly take the reins of full portions of their target's infrastructure. While a dire situation, that is not time to give up the fight, however, says Josh Sudbury, the Managing Director of Lodestone's Forensic Investigations team. "There is no point in the incident response lifecycle where [organizations] shouldn't be worried about detection, mitigation, and containment." Sudbury emphasizes that "any environment that has been compromised likely has some form of C2 malware in the environment," as "the C2 is the malware that creates a tunnel from the threat

actor's system to the target system." Organizations must work as quickly as possible to disrupt the conduit that the threat actor will rely on to successfully complete the cyberattack and even carry out additional attacks.

The leader of Lodestone's Forensic Investigations practice, Josh Sudbury has over two decades of experience across the varying fields of technology. As a digital forensics and incident response (DFIR) expert, he has provided guidance to companies in the midst of some of the largest data breaches in the world. He emphasizes that in the ever-changing world of cybersecurity, while "there is no silver bullet … there's no one solution to it all," there are steps that organizations can take to respond to cyberattacks, including those in their final stages. "[Even] if the threat actor is already in the environment, you still want to work on blocking them, containing them, and mitigating the situation." Insufficient containment can create a back-and-forth battle for control: threat actors that become aware of a company's remediation efforts have often been observed shifting their strategies to hamper such efforts and maximize damage.

Sudbury recommends that companies invest in both antivirus (AV) and endpoint detection and response (EDR) tooling to maintain the highest levels of visibility into their own environments as possible. Fighting the fight against threat actors depends on businesses being able to fully see and understand the battlefield. AV and EDR tooling can provide a number of advantages, including:

- Detection of threats using repositories of known malware and malware binaries.
- Identifying suspicious behavior within an environment using catalogued heuristics.
- Behavioral analysis that identifies normal behavior within an environment.
- Automated alerting and response, including blocking malicious activity or quarantining malware, in the event that dangerous deviations from a network's normal behavior are detected.

The three companies in the hypothetical scenarios described above can provide themselves the best advantages possible by ensuring that they maintain visibility into and an understanding of their environments; this includes implementing what AV and EDR tooling they can afford. As companies scale, support for internal IT teams becomes increasingly critical. While a small company like The Second

Breakfast may have to outsource IT, they should understand what their relationship is with the third party and have a plan built around an organized response that reflects how responsibility is divided between both parties. Medium and large companies must work closely with their IT teams to set up sufficient resources, visibility, architecture, and segmentation.

Sudbury recommends that companies work with a third-party security company that specializes in DFIR to facilitate their technological needs and ensure that they are in the best position possible to combat cyberattacks. “Work closely with [consultants] to determine where risks might exist. Focus on backups and a response plan on what to do, who to call, and how to organize yourself around responding to an incident.”

C2 is the sixth stage of the Cyber Kill Chain® – by staying resilient in the face of an active cyberattack and equipping themselves with the appropriate tooling, companies can disrupt cyberattacks in progress to help minimize the damage. For more information on cybersecurity and resources to prevent and respond to breaches, visit https://lodestone.com/contact/.

This article is the sixth 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