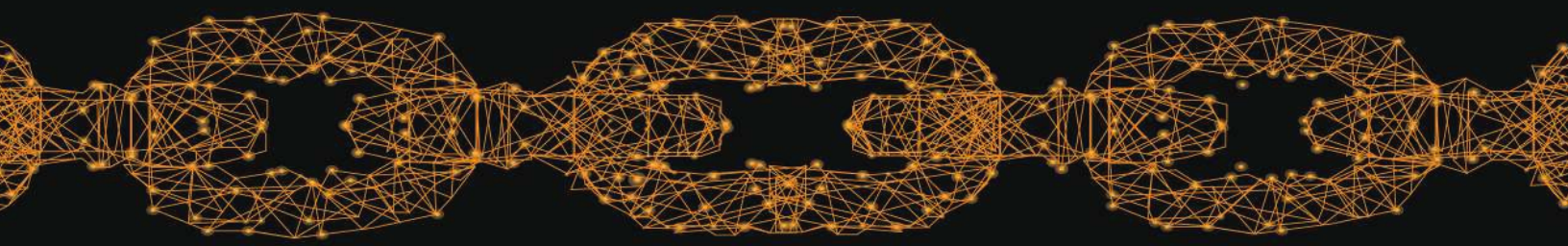
Lodestone

Mastering the Cyber Kill Chain

Step Seven: Actions on Objectives



STEP SEVEN: ACTIONS ON OBJECTIVES

Let's face it – we're spending most of our lives living in a hacker's paradise. Over the past decades, the world's technological advancement has exploded. We are more connected than ever, with conveniences and ways of life that our ancestors never could have dreamt of. However, we have not escaped the growing pains: rapid technological advancements have forged the way forward, but security often struggles to catch up. Even savvy organizations scramble to close gaps within their environments' armor, while a threat actor may only need to successfully exploit one to achieve their final objectives.

Actions on Objectives is the final phase 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 perform Installation and Command and Control (C2) setup to expand their influence and maintain their hold on a victim's environment.

Once a threat actor has a strong grasp on all or a portion of a system or environment, the time has come to reap the rewards of their unsavory efforts. This is represented by the final stage of the Cyber Kill Chain®: accomplishing the goal of their mission. This can vary tremendously based on the individual or group behind the cyberattack; threat actors may have myriad motivations, from financial gain to political motivation to a simple desire to sow discord. As a result, their ultimate aim may be to collect and exfiltrate valuable data, collect user credentials, or destroy a network altogether.

ACTING UP

The final step in the Cyber Kill Chain® is where a threat actor's motivations are most likely to become known. With a firm foothold established in the victim's environment, the threat actor has the relative freedom to do as they wish using the access and tools they have gained. In the case of spyware, this may be as simple as ongoing reconnaissance within an environment, capturing keystrokes and gathering more intelligence and sensitive information from behind the scenes. In other scenarios, a threat actor may seek to modify or corrupt data without the victim's knowledge to sabotage their business.

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 restaurant with a few systems; Fhloston Paradise, a medium-sized resort group catering to the rich and famous; and Cash Williams, a massive online retail giant that sells outdoor equipment.

The Second Breakfast is a tiny local eatery with a handful of systems and little to no resources for security. In the mind of the business' owner, they aren't a target because they don't have much of value to those big-time hackers that turn up in the news. However, a threat actor scanning the Internet identified one of their unpatched, public-facing computers and exploited it to install malware for a botnet. It was spread to the other systems on the Second Breakfast's network and launched, forcing them all to help additional compromised systems from other victims launch denial-of-service (DoS) and other attacks at the threat actor's command.

The medium-sized example, Fhloston Paradise, is a chain of luxurious health retreats and resorts with wealthy and famous clientele. Its management knows the value of the additional measure it takes to protect the confidentiality of its customers, and Fhloston Paradise's small Information Technology (IT) has tirelessly combed through the network for any potential gaps. Unfortunately, they missed on – a scripting error on the business' website. A threat actor was able to exploit this vulnerability to enter the environment, gather and steal critical data, and launch a ransomware attach that encrypted key Fhloston Paradise systems and effectively put their business at a standstill. Now, the threat actor is reaching out to the organization with ransom demands.

Finally, fictional online retail giant Cash Williams has a complex infrastructure and dedicated IT team to help manage it. However, recent media coverage about the company's success has attracted the attention of many threat actors. Monitoring and other good security practices warded off several of these attempts, but one threat actor was able to impersonate a member of the IT team and trick a legitimate employee into installing custom malware into the environment. After establishing persistence via a Remote Desktop Protocol (RDP) connection, the threat actor is poised to perform any number of malicious actions within a target-rich environment.

BURNING SECOND BREAKFAST

A critical consideration for small businesses like The Second Breakfast is that their size does not render them exempt from cyberattacks and security concerns. Many threat actors, especially novice hackers, are willing to take what they can get, even if this means compromising an environment with only a few systems. There is still value to be gained from exploiting small businesses, including the ability to incorporate their resources into larger-scale attacks, or redirect them into malicious activities such as mining cryptocurrency without the owner's knowledge.

In this example, a threat actor has established a foothold in The Second Breakfast's environment by hiding malware files in system directories and using scheduled tasks to re-establish malicious connections. In addition, a channel has been set up between the environment and the threat actor's Command and Control (C2) server, enabling them to issue commands even when they aren't directly logged in to The Second Breakfast's environment. Now, the threat actor is able to force The Second Breakfast's systems to join their botnet and redirect their resources towards attacking others. Not only can this cause problems using the systems for their intended purposes, but it can also implicate The Second Breakfast in malicious activity they knew nothing about if the victim of a DoS attack traces the systems involved back to their Internet Protocol (IP) addresses.

TROUBLE IN FHLOSTON PARADISE

The fictional Fhloston Paradise has found its success in its discretion. The rich and famous flock to their handful of resort locations, which also offer "holistic healing" services. As a result, the business has a large database that stores sensitive information such as credit card information, Personally Identifiable Information (PII), and even some data that is covered under the Health Insurance Portability and Accountability Act (HIPAA). Despite the small IT team they enlisted to monitor their environment, a threat actor identified a vulnerability in their website and has exploited it to access Fhloston Paradise customer information.

While the main focus of this threat actor, who is a member of a ransomware group, is to encrypt as many systems as possible in an attempt to effectively lock Fhloston Paradise out of its own network, they were also aware of the business' reputation. As a result, once the threat actor had established themselves within the environment, they took time to identify, package (i.e., compress), and exfiltrate as much seemingly valuable data as possible. After exfiltrating the data, they ran the

ransomware. As a result, the ransomware group can reach out to Fhloston Paradise with two sources of ransom demands: payment to receive the decryption keys for the systems, and payment to prevent the ransomware group from releasing Fhloston Paradise's sensitive customer information to the public.

CASH (WILLIAMS) AND GRAB

Security at large companies can be a double-edged sword; these businesses often have the resources to dedicate to monitoring tools and internal IT teams, but also have complex environments that make it difficult to maintain visibility. In the example of Cash Williams, the company has implemented some protections and employs a reasonably sized IT team. However, due to the number of employees and locations, many employees aren't familiar with one another, especially when it comes to new hires. As a result, a threat actor impersonating a new member of the IT team was able to call a legitimate Cash Williams employee and convince them to download custom malware and execute it on their work computer. From there, the malware automatically spread to numerous systems within the environment and established web shell connections to external C2 servers.

In this scenario, the Actions on Objectives step could take a number of different forms, depending on the threat actor involved. By establishing a strong foothold in the environment, any number of malicious activities could be performed. A financially motivated threat actor may attempt to manipulate routing numbers in financial transactions so that payments to a third-party provider of Cash Williams are sent to a bank account they control instead. A threat actor with a political motive may attempt to locate controversial information or release emails of high-ranking individuals at the company. Others may simply be looking to create chaos, and destroy backups, wipe systems, and attempt to bring the business' operations to a standstill.

RESISTANCE IS NOT FUTILE

As the final step of the Cyber Kill Chain®, the implications of a threat actor reaching the Actions on Objectives step are dire: they have succeeded with their cyberattack and need only to reap the rewards. Companies, however, still have a chance to fight back through efforts to detect and block threat actor activity as quickly as possible. As Lockheed Martin states, "the longer an adversary has [Actions on Objectives] access, the greater the impact. Depending on when a company is able to intervene, the effects of the cyberattack can be mitigated. This may include recognizing ransomware-related activity and mitigating its effects in time to prevent any

encryption from actually occurring, isolating systems that have been compromised from the rest of the network, or terminating suspicious external communications, such as those from C2 channels, to interrupt threat actor activity.

The Managing Director of Lodestone Europe, Adam Harrison has overseen hundreds of incident response cases and supported organizations across the globe in almost every sector in their efforts to prevent and respond to cyberattacks. He states that even if a cyberattack has succeeded, detecting and responding to as much of the malicious activity as quickly as possible can still make a difference for a company. "When [an incident is] in that phase, or after that phase, they key is acting with haste – you don't want to rush things, but at the same time … [the threat actor] may be one action from exfiltrating data or dropping ransomware." Based on Harrison's experience, current trends in digital forensics and incident response (DFIR) indicate that ransomware is what a majority of organizations experiencing a cyberattack are likely to encounter. While the Actions on Objectives step can happen quickly, there might also be a lull as threat actors position themselves within the environment to best carry out their end goals; this provides victims with the opportunity to strike back and minimize the damage a threat actor is able to do to an environment.

Harrison recommends that companies that suspect a cyberattack against their environment has succeeded execute their incident response plans (IRPs) immediately and make use of endpoint detection and response (EDR). IRPs, which would ideally be created and tested ahead of time, should provide immediate guidance to personnel on mitigation activities like identifying and resetting compromised credentials and attempting to locate and remove any backdoors into the company's network. In addition, seeking the help of an experienced third party, such as Lodestone, can make a tremendous difference. "For most people, finding a malicious actor in their environment could be a first-in-a-career type of event," Harrison states. "Leaning into it and getting expert assistance is going to be valuable."

DFIR organizations are experienced in assisting organizations experiencing confirmed or suspected cyberattacks day in and day out. "Incident response is often a second job for everyone within an organization," Harrison says. "[Third parties] can bolster their capability." When a threat actor has reached the Actions on Objectives step, timing becomes especially critical. Even if the threat actor has already achieved their goals, DFIR groups can still assist organizations with preventing recurrence and answering key questions, such as:

- How did the threat actor get to this stage?
- What access might the threat actors still have (e.g., C2, malware)?
- What was the method of exploitation, and how could it have been detected earlier?
- What defenses can be built up to prevent recurrence?

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.

The three hypothetical businesses described previously still have an opportunity to fight back against the threat actors within their environments, even at the last step in the Cyber Kill Chain®. While small companies like The Second Breakfast are likely to have limited incident response capabilities, they have the advantage of being able to gain visibility into their environments more easily. Meanwhile, medium-sized companies like Fhloston Paradise and large companies like Cash Williams can take advantage of their internal capabilities to attempt to isolate malicious activity. All three companies can minimize damage and stop threat actors as quickly as possible by working closely with internal or third-party IT resources and employing DFIR experts to help them respond thoroughly and efficiently.

Actions on Objectives is the seventh and final stage of the Cyber Kill Chain® – even if a cyberattack has succeeded, hope isn't lost for companies that fight back against threat actors active within their environments and take steps to minimize 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