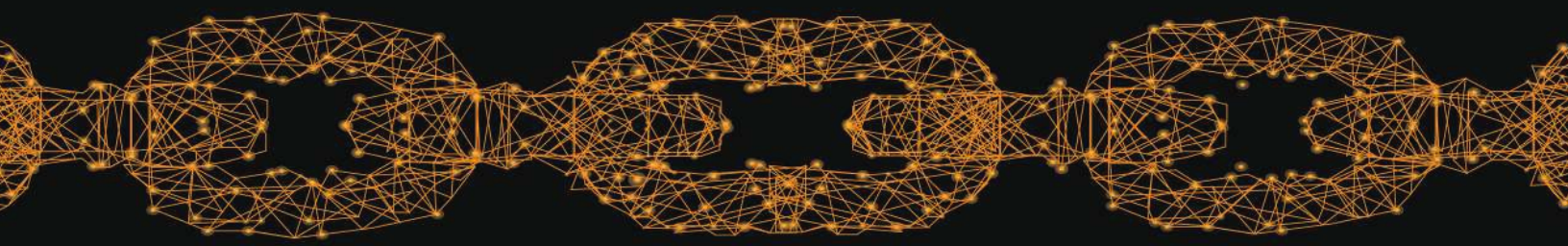
Lodestone

Mastering the Cyber Kill Chain

Step Three: Delivery



STEP THREE: DELIVERY

Signed, sealed, delivered – you're theirs. It's a much less romantic notion than the original line from Stevie Wonder's classic, but an increasingly common occurrence in an increasingly computer-driven world. Attackers craft weapons to send to unsuspecting victims, setting the stage to launch cyberattacks that can cripple critical infrastructure, compromise sensitive data, and generally wreak havoc.

Delivery is the third 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 two 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.

While cyberattacks can be anything from painstakingly planned to pure opportunism, each begins with an attempt to place malicious tools or files within the boundaries of a target's environment. Delivery may be closely controlled via an attempt to place malware on a vulnerable web server, for example, or released as a phishing email or decoy website that works to trick any user that happens to visit into downloading malware under the guise of a benign tool.

WHAT'S IN THE BOX?

Attackers have two primary options for the execution of the Delivery phase: hacking people or hacking computers. Even with security awareness training and an understanding of cyberattacks, a single instance of human error can be the weak link that breaks the chain of an otherwise strong security posture. Computers, however, provide more flexibility in what time of day a delivery attempt can occur, and aren't influenced by fickle emotional factors like bad mornings or late nights that could render them uncooperative.

Each entry in this series, Mastering the Kill Chain — Step One: Reconnaissance, 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 attacker performing the

Reconnaissance step was able to identify a handful of unpatched, outward-facing systems. During the Weaponization phase, the attacker obtained an exploit for known vulnerabilities in these unpatched systems that could force them to join a botnet, or group of external-facing devices used to perform denial-of-service attacks, steal credentials, or send spam without the knowledge of the legitimate owners of the devices involved.

Fhloston Paradise, a medium-sized business, takes additional measures to protect the confidentiality of its high-profile clients. However, an attacker exploring the company website during Reconnaissance was able to identify a "Contact Us" page that included a form with a scripting error. As part of the Weaponization phase, the attacker customized a widely available malicious script to exploit this error and drop a ransomware package into the environment.

The largest example, Cash Williams, has been gaining a lot of media attention with its growing success. As a result, an attacker performing Reconnaissance was able to easily locate information such as the company's partnerships with other vendors and details about employees and executives through their social media profiles. The attacker has planned to Weaponize this information by using it to perform a phishing campaign with the intent to trick employees into downloading malicious files directly into the company's environment.

SENT TO SECOND BREAKFAST

Even if there appears to be little of value to steal from a small business like The Second Breakfast at a glance, these companies are not exempt from becoming targets of a cyberattack. Attackers often understand that security resources for businesses of that size are limited, and that their systems may be useful as part of a larger-scale attack or a chance opportunity for an inexperienced attacker to hone their skills. External-facing resources can be effectively taken over by attackers and used as part of a botnet to perform denial of service attacks, mine virtual currency, or other similarly malicious activity as part of a group of other compromised networks.

In previous steps, attacker was able to use reconnaissance to identify Internet-facing unpatched systems The Second Breakfast manages, and weaponized this knowledge by obtaining code for a botnet that could be placed in a victim's environment. In

the Delivery phase, the attacker puts these plans into action, attempting to delivery malware by exploiting known vulnerabilities in systems with outdated tools or software. Their success results in the installation of malware on all of The Second Breakfast's external systems that, for now, lies dormant. The malware has been configured to await instructions from an attacker command-and-control (C2) server and activate itself when prompted.

A PACKAGE FOR FHLOSTON PARADISE

A business like Fhloston Paradise that has significant amounts of private information about its clients may find itself an especially desirable target for ransomware and blackmail campaigns. As a rumored rehabilitation facility that serves wealthy customers and celebrities, Fhloston Paradise would be in deep trouble should the names of its customers be released.

An attacker that has observed scripting error in the company's website during reconnaissance may see a prime opportunity to access valuable information and extort money from the victim to prevent its public release. During the Weaponization phase, they customized the code for a widely known cross-site scripting attack such that the malware could inject malicious code into the Fhloston Paradise environment through its website. When triggered, this malware will operate as ransomware and perform activities such as accessing and exfiltrating information, establishing persistence in the environment, and encrypting critical data on the system in an effort to force the company to pay a ransom and meet the attackers' demands.

CALLING CASH WILLIAMS

A large company like Cash Williams may have a strong security setup that includes monitoring and automated responses but is still particularly vulnerable if its personnel do not possess an awareness of potential events, attacks, or other security issues.

An attacker planning to use a phishing campaign to steal money from Cash Williams obtained a list of employees in finance-related departments as part of its reconnaissance. During weaponization, the attacker prepared a script to follow during conversations with employees and malware to provide persistence in the environment once an employee has downloaded the malware.

To deliver this malware, the attacker uses their script and calls various employees at the company, insisting that they are an IT representative or another trusted

individual that needs assistance. By playing off the good will and inexperience of others, attackers may convince them to install malware that provides persistence onto their systems and set the stage for their next step.

DELIVERY DENIED

Delivery represents the first phase in the Cyber Kill Chain® where a cyberattack is put into action. As a result, companies have an opportunity to directly defend against it by observing attacker behavior within their own environments. This can reveal critical information such as the attackers intent, what information they appear to have, what the goal of their attack appears to be, and indicators such as Internet Protocol (IP) addresses that can be used to attribute activity to the attacker. A company's ability to block an attack at this preliminary stage is a strong indicator of effectiveness in a security plan, says Jeff Bowie, a Consultant in Lodestone's proactive Security Consulting group. "It's all about awareness and preparedness."

Bowie used his first computer at only 8 years old, kicking off a life-long interest in physical and computer security. His focus as a consultant is penetration testing and scanning, both key factors in the assessment of client preparedness to face off with potential attackers in the wild. Every environment is unique, like a fingerprint, according to Bowie. Identifying and addressing weaknesses regularly can help clients keep their environments healthy and strong, similar to a person getting regular check-ups at a doctor's office.

Bowie states that having multiple layers of security is critical to blocking a cyberattack during the Delivery phase, and includes preparation such as:

- Security awareness training.
- Systems and firewalls with up to date and custom settings to best suit the needs of the company.
- Endpoint detection monitoring and response, as well as other similar solutions that are reviewed by dedicated personnel in near-real time.
- Regular testing of processes, backups, and emergency response plans.

In the hypothetical scenarios described above, patching and penetration testing could have helped The Second Breakfast and Fhloston Paradise detect and resolve the outdated systems and website misconfigurations that made delivery possible for their attackers. In addition, regular phishing tests could have helped promote awareness of social engineering within Cash Williams, making personnel more prepared to combat attackers' first attempts at delivery.

It is critical to empower not only companies, but their personnel to take an active role in stopping cyberattacks, Bowie says. By performing phishing and penetration testing at least every six months, companies can safely simulate the experience of an actual attack to ensure that its response strategies on all levels are as effective and actionable as possible.

Delivery is the third stage of the Cyber Kill Chain® – by engaging in regular testing and building employees' confidence in detecting and responding to social engineering attempts, companies have an opportunity to stop cyberattacks at their earliest stages. 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/.

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