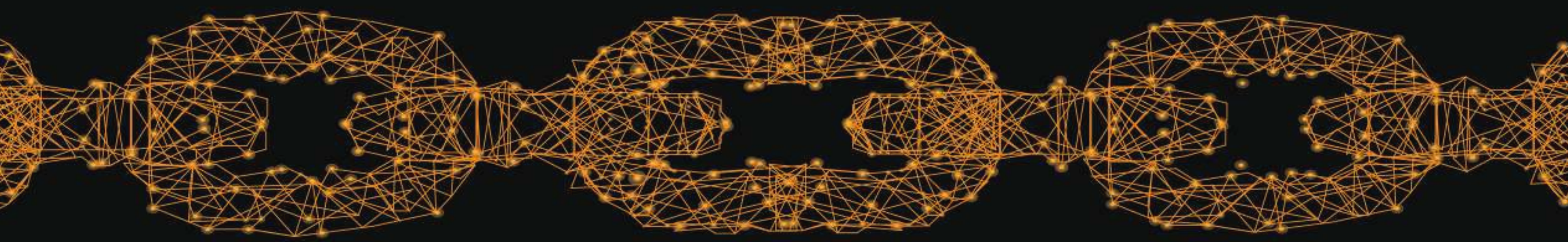
Lodestone

Mastering the Cyber Kill Chain

Step One: Reconnaissance



STEP ONE: RECONNAISSANCE

Is someone peeking through your (digital) window? In the world of cybersecurity, this is known as reconnaissance – a common first step for the vast majority of cyberattacks.

Lockheed Martin establishes reconnaissance as the first step in its Cyber Kill Chain®, a framework that outlines the common steps attackers take during a security event or incident. Reconnaissance is generally defined as the information gathering that occurs before an attack. This could include gathering technical information, such as information about network topology and systems, including what operating systems (OSs), applications, and services are running in a target's environment. This may also involve organizational information, including information on employees, the target organization itself, and the organization's business partners. In general, knowledge is indeed power – the more information an attacker is able to gain about their target, the more likely they are to be able to carry out a successful and fast-moving attack.

> Reconnaissance is generally defined as the information gathering that occurs before an attack. |

In security, reconnaissance is separated into two categories: active and passive reconnaissance. In active reconnaissance, attackers play a direct role in gathering information about a target or target environment. This could appear as a combination of manual and automated tools that are run against any portion of an environment that is accessible via the Internet. Passive reconnaissance, while less invasive, is often more difficult to detect and dangerous to underestimate. This could include information from web searches or data gathered from the target's own website.

SELECTING A TARGET

Attackers are driven by a number of motivations when selecting a target. These could include promoting a political agenda or social change, monetary gain, or simply a desire to stir up trouble.

Consider three popular (and hypothetical) businesses of varying 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 Second Breakfast hasn't made itself a target for any obvious reasons, but as a small, local business, it places little focus on security and has some poor practices in place. As a result, an attacker collecting information about the restaurant may identify it as an easy opportunity to cause some trouble.

Fhloston Paradise, on the other hand, is suspected by the paparazzi of being a celebrity rehabilitation facility disguised as a spiritual retreat. Some particularly unsavory members of the press pool their money together in secret to hire an expert hacker to infiltrate Fhloston Paradise's environment and dig up some juicy secrets.

A million-dollar company with customers across the United States, Cash Williams stores vast amounts of data, including the addresses and credit card information of its customers. An Advanced Persistent Threat (APT), a group of experienced attackers, identifies the company as an ideal candidate for a large-scale ransomware attack in which malware is used to encrypt critical files and systems. The APT will provide the keys to decrypt the systems, but only for an exorbitant fee.

All of these examples begin with the same step: reconnaissance. Whether active or passive and targeted at a large, mid-sized, or small company, the information gathered during this step provides attackers insight into their target and their target's environment. Think of this as a robber "casing the place" and getting to know the surroundings before stealing from a jewelry store.

> Think of reconnaissance as a robber "casing the place" and getting to know the surroundings before stealing from a jewelry store.

In the sections below, take a glimpse into the first link in the Cyber Kill Chain® for three real-world examples and pull back the curtain on cyberattacks – and how to help stop them in their tracks.

PREPARING SECOND BREAKFAST

In the example of a small business like The Second Breakfast, the Internet-accessible portion of the environment reachable by attackers, also known as the "attack surface," is small. An attacker performing active reconnaissance by scanning The Second Breakfast's outward-facing systems may find that some of the systems have publicly known vulnerabilities that were addressed in a recent patch but have yet to be applied due to the businesses having no information technology (IT) personnel. With this information, an attacker could identify a particular exploit that would be effective in gaining control of a business-critical server the target runs.

An attacker performing passive reconnaissance on The Second Breakfast may glean information from the restaurant's website, such as the names of its employees and the format used for the restaurant's email addresses (e.g., First.Last@secondbreakfast.com). With this information, an attacker could attempt to impersonate someone from the restaurant who is an actual employee or make password guessing attempts using the email addresses of employees as usernames.

For many small businesses, especially given the current trend of opportunistic attacks using commodity malware, parts of the Cyber Kill Chain® may seem obsolete. Reconnaissance in those cases is often limited to searches for Internet-connected devices or Internet-wide scanning to identify low-hanging fruit ripe for a cyberattack. While a small company like The Second Breakfast may not have the high profile or security budget of a large company like Cash Williams, they are still in danger of becoming victims by failing to place sufficient emphasis on security. Without keeping up with best practices, small companies risk making themselves easy targets.

TROUBLE IN FHLOSTON PARADISE

As a mid-sized company with high-profile clients, Fhloston Paradise has taken additional measures to protect the confidentiality of its customers. An active scan of the Fhloston Paradise attack service shows that the vast majority of the environment is locked down; however, an information request form on their website contains a scripting error. An attacker might note this scripting error as a potential point of entry into the full environment if exploited successfully.

Though information on Fhloston Paradise's specific locations and the contact information of its staff is omitted from the website for privacy, thorough passive reconnaissance may reveal key information that was inadvertently leaked in third-party pages or even on map services. An attacker could find an information dump on the Internet that contains a handful of emails from Fhloston Paradise personnel that, though seemingly benign, reveal the address of one of the facilities and the corporate signature all Fhloston Paradise employees are required to use.

STALKING CASH WILLIAMS

A large-scale operation like Cash Williams that relies more heavily on technology would have a wide attack surface. An attacker performing active reconnaissance by scanning the public-facing portions of the environment may be able to identify several web applications with exploitable vulnerabilities or a security server that is inadvertently accessible to external devices for Remote Desktop Protocol (RDP) or similar connections. Though often better equipped for larger businesses, Cash Williams' IT team may struggle to differentiate particularly targeted or successful active reconnaissance against the environment, as scanning attempts from automated bots in the wild are common across the Internet.

An attacker gathering information on Cash Williams through passive reconnaissance could perform Internet searches to find promotional articles on the company's partnerships with other vendors to identify what brands of equipment they use, and even personal details on the company's executives by studying their social media profiles, such as LinkedIn. This could help attackers tailor an attack to the specific combination of software and hardware the target company uses, or personal details that make social engineering more convincing, allowing them to perform a social engineering attack in which an employee is convinced to approve a money order or similar by an attacker impersonating an executive.

RESISTING RECONNAISSANCE

Protecting against reconnaissance may seem impossible at first glance, but there are multiple ways to harden an environment against would-be foes, according to Lodestone Managing Principal Allyn Lynd. With over 25 years of experience in cybersecurity, including in the Federal Bureau of Investigations (FBI) Lynd has seen his share of reconnaissance, and even performed it himself as part of penetration testing.

Lynd recommends a twofold approach to addressing reconnaissance by addressing both active and passive reconnaissance either internally or with the assistance of experienced third-party vendors and consultants. To address passive reconnaissance, awareness is key. Companies can effectively perform reconnaissance on themselves to maintain an accurate understanding of their attack surfaces, enabling personnel to better defend them. In the case of active reconnaissance, log reviews and the use of tools such as intrusion detection systems (IDSs) can be used to pinpoint subtle traces that may be left behind by active reconnaissance. Disconnections between what a company believes is public knowledge and what actually is public knowledge can be a source of major security gaps.

In addition, Lynd recommends that companies adopt the following strategies to improve resistance to reconnaissance:

- Create and foster a culture of security awareness within the organization
    - Perform phishing tests and ask employees to routinely take security training.
- Limit what information the company makes available.
    - Do not provide public information beyond what is necessary to meet business needs.
    - Limit what employees post on social media related to the company.

For both the examples of The Second Breakfast and Cash Williams, reducing available information and maintaining awareness about what is publicly available could have prevented attackers from hacktivists to APTs from gaining the information necessary to successfully compromise their environments.

Reconnaissance is the first step in the Cyber Kill Chain® – by preparing defenses against the earliest stages of an attack, companies have the chance to stop breaches and the attackers behind them in their tracks before they can truly begin. For more information on cybersecurity and resources to prevent and respond to breaches, visit https://lodestone.com/contact/.

This article is the first 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

6