INFO & INSIGHTS

DISRUPTING THE ATTACK LIFECYCLE AT EVERY STAGE

When cyber attackers strategize their way to infiltrate an organization's network and exfiltrate data, they follow the series of stages that comprise the attack lifecycle.[1] For attackers to successfully complete an attack, they must progress through each stage. Blocking adversaries at any point in the cycle breaks the chain of attack. To protect a company's network and data from attack, prevention must occur at each stage to block the attackers' ability to access and move laterally within the organization or steal sensitive data. The following are the different stages of the attack lifecycle and steps that should be taken to prevent an attack at each stage.

1 **Reconnaissance:** During the first stage of the attack lifecycle, cyber adversaries carefully plan their method of attack. They research, identify and select targets that will allow them to meet their objectives. Attackers gather intel through publicly available sources, such as Twitter, LinkedIn and corporate websites. They will also scan for vulnerabilities that can be exploited within the target network, services, and applications, mapping out areas where they can take advantage. At this stage, attackers are looking for weaknesses based on the human and systems perspective.

- Perform continuous inspection of network traffic flows to detect and prevent port scans and host sweeps.
- Implement security awareness training so users are mindful about what should and should not be posted – sensitive documents, customer lists, event attendees, job roles and responsibilities (i.e., using specific security tools within an organization), etc.

2 **Weaponization and Delivery:** Attackers will then determine which methods to use in order to deliver malicious payloads. Some of the methods they might utilize are automated tools, such as exploit kits, spear phishing attacks with malicious links, or attachments and malvertizing.

- Gain full visibility into all traffic, including SSL, and block high-risk applications. Extend those protections to remote and mobile devices.

[1] Defined by Lockheed Martin as the Cyber Kill Chain®

- Protect against perimeter breaches by blocking malicious or risky websites through URL filtering.
- Block known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti-malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking.
- Detect unknown malware and automatically deliver protections globally to thwart new attacks.
- Provide ongoing education to users on spear phishing links, unknown emails, risky websites, etc.

3 **Exploitation:** In this stage, attackers deploy an exploit against a vulnerable application or system, typically using an exploit kit or weaponized document. This allows the attack to gain an initial entry point into the organization.

- Block known and unknown vulnerability exploits on the endpoint.
- Automatically deliver new protections globally to thwart follow-up attacks.

4 **Installation:** Once they've established an initial foothold, attackers will install malware in order to conduct further operations, such as maintaining access, persistence and escalating privileges.

- Prevent malware installation, known or unknown, on the endpoint, network and cloud services.
- Establish secure zones with strictly enforced user access controls and provide ongoing monitoring and inspection of all traffic between zones (Zero Trust model).
- Limit local admin access of users.
- Train users to identify the signs of a malware infection and know how to follow up if something occurs.

5 **Command and Control:** With malware installed, attackers now own both sides of the connection: their malicious infrastructure and the infected machine. They can now actively control the system, instructing the next stages of attack. Attackers will establish a command channel in order to communicate and pass data back and forth between the infected devices and their own infrastructure.

- Block outbound command-and-control communications as well as file and data pattern uploads.
- Redirect malicious outbound communication to internal sinkholes to identify and block compromised hosts.

- Block outbound communication to known malicious URLs through URL filtering.
- Create a database of malicious domains to ensure global awareness and prevention through DNS monitoring.
- Limit the attackers' ability to move laterally with unknown tools and scripts by implementing granular control of applications to allow only authorized applications.

6 **Actions on the Objective:** Now that the adversaries have control, persistence and ongoing communication, they will act upon their motivations in order to achieve their goal. This could be data exfiltration, destruction of critical infrastructure, to deface web property, or to create fear or the means for extortion.

- Proactively hunt for indicators of compromise on the network using threat intelligence tools.
- Build bridges between the security operations center (SOC) and the network operations center to put the right prevention-based controls in place.
- Monitor and inspect all traffic between zones and enforce user access controls for secure zones.
- Block outbound command-and-control communications as well as file and data pattern uploads.
- Block outbound communication to known malicious URLs through URL filtering.
- Implement granular control of applications and user control to enforce file transfer application policies on the enterprise, eliminating known archiving and transfer tactics and limiting the attackers' ability to move laterally with unknown tools and scripts.

Advanced attacks are very complex in that, in order for an adversary to succeed, they must progress through every stage of the attack lifecycle. If they cannot successfully take advantage of vulnerabilities, then they cannot install malware and will not be able to obtain command and control over the system.

Disrupting the attack lifecycle relies on not only the technology but the people and the process. The people must receive ongoing security awareness training and be educated in best practices to minimize the likelihood of an attack progressing past the first stage; and there must be processes and policies in place for remediation should an attacker successfully progress through the entire attack lifecycle.

Cybersecurity is asymmetric warfare — an attacker must do everything right in order to succeed, but a network defender needs to only do one thing right to prevent an attack, of which they have multiple opportunities. To learn more about disrupting the attack lifecycle and how Palo Alto Networks provides prevention capabilities at each stage, read **Breaking the Attack Lifecycle.**