GAINING THE ADVANTAGE

Applying Cyber Kill Chain® Methodology to Network Defense

**LOCKHEED MARTIN**

THE MODERN DAY ATTACKER

Cyberattacks aren't new, but the stakes at every level are higher than ever. Adversaries are more sophisticated, well-resourced, trained, and adept at launching skillfully planned intrusion campaigns called Advanced Persistent Threats (APT). Our nation's security and prosperity depend on critical infrastructure. Protecting these assets requires a clear understanding of our adversaries, their motivations and strategies.

Adversaries are intent on the compromise and extraction of data for economic, political and national security advancement. Even worse, adversaries have demonstrated their willingness to conduct destructive attacks. Their tools and techniques have the ability to defeat most common computer network defense mechanisms.
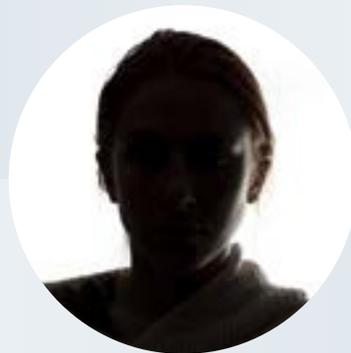
SOPHISTICATED   WELL-RESOURCED   MOTIVATED
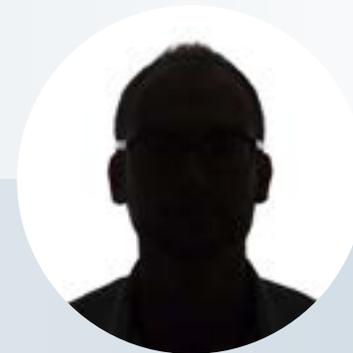
THE LOCKHEED MARTIN CYBER KILL CHAIN®

The Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for the identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.

Stopping adversaries at any stage breaks the chain of attack! Adversaries must completely progress through all phases for success; this puts the odds in our favor as we only need to block them at any given one for success. Every intrusion is a chance to understand more about our adversaries and use their persistence to our advantage.

The kill chain model is designed in seven steps:

- ▶ Defender's goal: understand the aggressor's actions

- ▶ Understanding is Intelligence

- ▶ Intruder succeeds if, and only if, they can proceed through steps 1-6 and reach the final stage of the Cyber Kill Chain®.

1

2

3

4

5

6

7
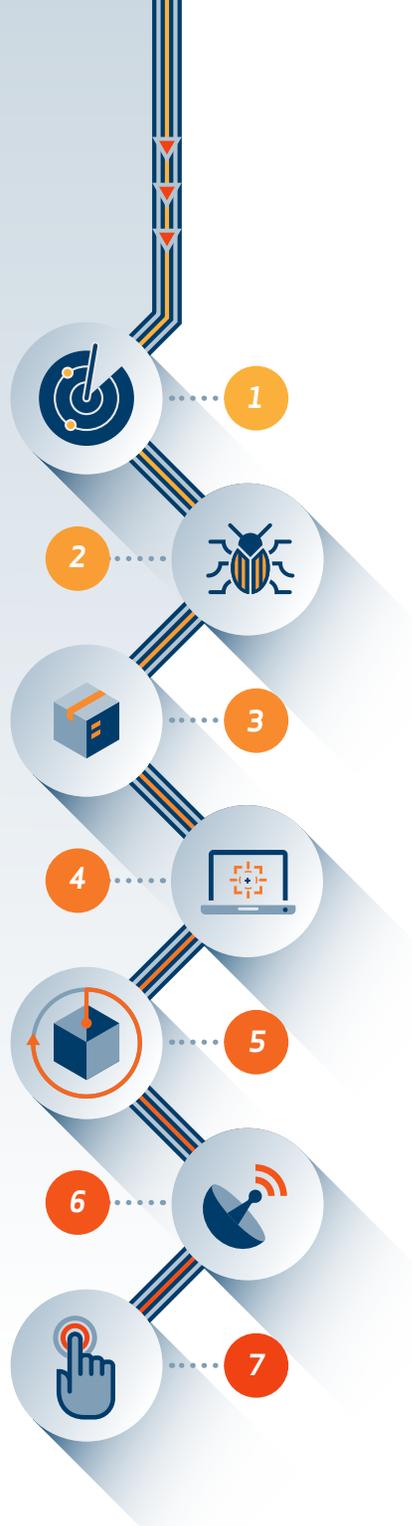
RECONNAISSANCE *Identify the Targets*

1

ADVERSARY

The adversaries are in the planning phase of their operation. They conduct research to understand which targets will enable them to meet their objectives.

▶ Harvest email addresses

▶ Identify employees on social media networks

▶ Collect press releases, contract awards, conference attendee lists

▶ Discover internet-facing servers

DEFENDER

Detecting reconnaissance as it happens can be very difficult, but when defenders discover recon – even well after the fact – it can reveal the intent of the adversaries.

▶ Collect website visitor logs for alerting and historical searching.

▶ Collaborate with web administrators to utilize their existing browser analytics.

▶ Build detections for browsing behaviors unique to reconnaissance.

▶ Prioritize defenses around particular technologies or people based on recon activity.

WEAPONIZATION *Prepare the Operation*

2

ADVERSARY

The adversaries are in the preparation and staging phase of their operation. Malware generation is likely not done by hand – they use automated tools. A "weaponizer" couples malware and exploit into a deliverable payload.

▶ Obtain a weaponizer, either in-house or obtain through public or private channels

▶ For file-based exploits, select "decoy" document to present to the victim.

▶ Select backdoor implant and appropriate command and control infrastructure for operation

▶ Designate a specific "mission id" and embed in the malware

▶ Compile the backdoor and weaponize the payload

DEFENDER

This is an essential phase for defenders to understand. Though they cannot detect weaponization as it happens, they can infer by analyzing malware artifacts. Detections against weaponizer artifacts are often the most durable & resilient defenses.

▶ Conduct full malware analysis – not just what payload it drops, but how it was made.

▶ Build detections for weaponizers – find new campaigns and new payloads only because they re-used a weaponizer toolkit.

▶ Analyze timeline of when malware was created relative to when it was used. Old malware is "malware off the shelf" but new malware might mean active, tailored operations.

▶ Collect files and metadata for future analysis.

▶ Determine which weaponizer artifacts are common to which APT campaigns. Are they widely shared or closely held?

DELIVERY *Launch the Operation*

3

ADVERSARY

The adversaries convey the malware to the target. They have launched their operation.

- ► Adversary controlled delivery:
  - ► Direct against web servers
- ► Adversary released delivery:
  - ► Malicious email
  - ► Malware on USB stick
  - ► Social media interactions
  - ► "Watering hole" compromised websites

DEFENDER

This is the first and most important opportunity for defenders to block the operation. A key measure of effectiveness is the fraction of intrusion attempts that are blocked at delivery stage.

- ► Analyze delivery medium – understand upstream infrastructure.
- ► Understand targeted servers and people, their roles and responsibilities, what information is available.
- ► Infer intent of adversary based on targeting.
- ► Leverage weaponizer artifacts to detect new malicious payloads at the point of Delivery.
- ► Analyze time of day of when operation began.
- ► Collect email and web logs for forensic reconstruction. Even if an intrusion is detected late, defenders must be able to determine when and how delivery began.

EXPLOITATION *Gain Access to Victim*

ADVERSARY

The adversaries must exploit a vulnerability to gain access. The phrase "zero day" refers to the exploit code used in just this step.

- Software, hardware, or human vulnerability
- Acquire or develop zero day exploit
- Adversary triggered exploits for server-based vulnerabilities
- Victim triggered exploits
  - Opening attachment of malicious email
  - Clicking malicious link

DEFENDER

Here traditional hardening measures add resiliency, but custom capabilities are necessary to stop zero-day exploits at this stage.

- User awareness training and email testing for employees.
- Secure coding training for web developers.
- Regular vulnerability scanning and penetration testing.
- Endpoint hardening measures:
  - Restrict admin privileges
  - Use Microsoft EMET
  - Custom endpoint rules to block shellcode execution
- Endpoint process auditing to forensically determine origin of exploit.

4
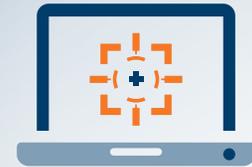
INSTALLATION *Establish Beachhead at the Victim*

5

ADVERSARY

Typically, the adversaries install a persistent backdoor or implant in the victim environment to maintain access for an extended period of time.

- ▶ Install webshell on web server
- ▶ Install backdoor/implant on client victim
- ▶ Create point of persistence by adding services, AutoRun keys, etc.
- ▶ Some adversaries "time stomp" the file to make malware appear it is part of the standard operating system install.

DEFENDER

Endpoint instrumentation to detect and log installation activity. Analyze installation phase during malware analysis to create new endpoint mitigations.

- ▶ HIPS to alert or block on common installation paths, e.g. RECYCLER.
- ▶ Understand if malware requires administrator privileges or only user.
- ▶ Endpoint process auditing to discover abnormal file creations.
- ▶ Extract certificates of any signed executables.
- ▶ Understand compile time of malware to determine if it is old or new.
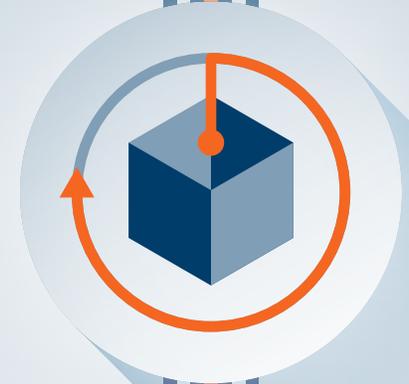
COMMAND & CONTROL (C2) *Remotely Control the Implants*

6

ADVERSARY

Malware opens a command channel to enable the adversary to remotely manipulate the victim.

- Open two way communications channel to C2 infrastructure

- Most common C2 channels are over web, DNS, and email protocols

- C2 infrastructure may be adversary owned or another victim network itself

DEFENDER

The defender's last best chance to block the operation: by blocking the C2 channel. If adversaries can't issue commands, defenders can prevent impact.

- Discover C2 infrastructure thorough malware analysis.

- Harden network:
  - Consolidate number of internet points of presence
  - Require proxies for all types of traffic (HTTP, DNS)

- Customize blocks of C2 protocols on web proxies.

- Proxy category blocks, including "none" or "uncategorized" domains.

- DNS sink holing and name server poisoning.

- Conduct open source research to discover new adversary C2 infrastructure.

ACTIONS ON OBJECTIVES *Achieve the Mission's Goal*

7

ADVERSARY

With hands-on keyboard access, intruders accomplish the mission's goal. What happens next depends on who is on the keyboard.

▶ Collect user credentials

▶ Privilege escalation

▶ Internal reconnaissance

▶ Lateral movement through environment

▶ Collect and exfiltrate data

▶ Destroy systems

▶ Overwrite or corrupt data

▶ Surreptitiously modify data

DEFENDER

The longer an adversary has CKC7 access, the greater the impact. Defenders must detect this stage as quickly as possible by using forensic evidence – including network packet captures, for damage assessment.

▶ Establish incident response playbook, including executive engagement and communications plan.

▶ Detect data exfiltration, lateral movement, unauthorized credential usage.

▶ Immediate analyst response to all CKC7 alerts.

▶ Forensic agents pre-deployed to endpoints for rapid triage.

▶ Network package capture to recreate activity.

▶ Conduct damage assessment with subject matter experts.

ANALYSIS: *Identifying Patterns*

Analysis of multiple intrusion kill chains over time draws attention to similarities and overlapping indicators. Defenders learn to recognize and define intrusion campaigns and understand the intruder's mission objectives.

Identify patterns: what are they looking for, why are they targeting me?

This will help identify how to best protect yourself from the next attack. You can't get ahead of the threat unless you understand the campaign.

RECONSTRUCTION: *Prevent Future Attacks*

Cyber Kill Chain® analysis guides understanding of what information is, and may be, available for defensive courses of action. Stay focused on your threat landscape with vigilance.

RESILIENCE: *Defend against Advanced Persistent Threats*

The antidote to APT is a resilient defense. Measure the effectiveness of your countermeasures against the threats. Be agile to adapt your defenses faster than the threats.

JUST ONE MITIGATION BREAKS THE CHAIN

- ▶ The defender has the advantage with the Cyber Kill Chain® solution. All seven steps must be successful for a cyber attack to occur.

- ▶ The defender has seven opportunities to break the chain.

CONCLUSION

- ▶ Defenders CAN have the advantage:
  - ▶ Better communicate and mitigate risks
  - ▶ Build true resilience
  - ▶ Meaningfully measure results
- ▶ Getting Started: Remember there is no such thing as secure, only defendable.
  - ▶ Start by thinking differently when you make changes to your processes, investments, metrics, communications with your team and leadership, staffing models, and architectures.
  - ▶ Know your threats...it's not just about network defense anymore. it's about defending much more like your platforms and mobile users.

1

2

3

4

5

6

7
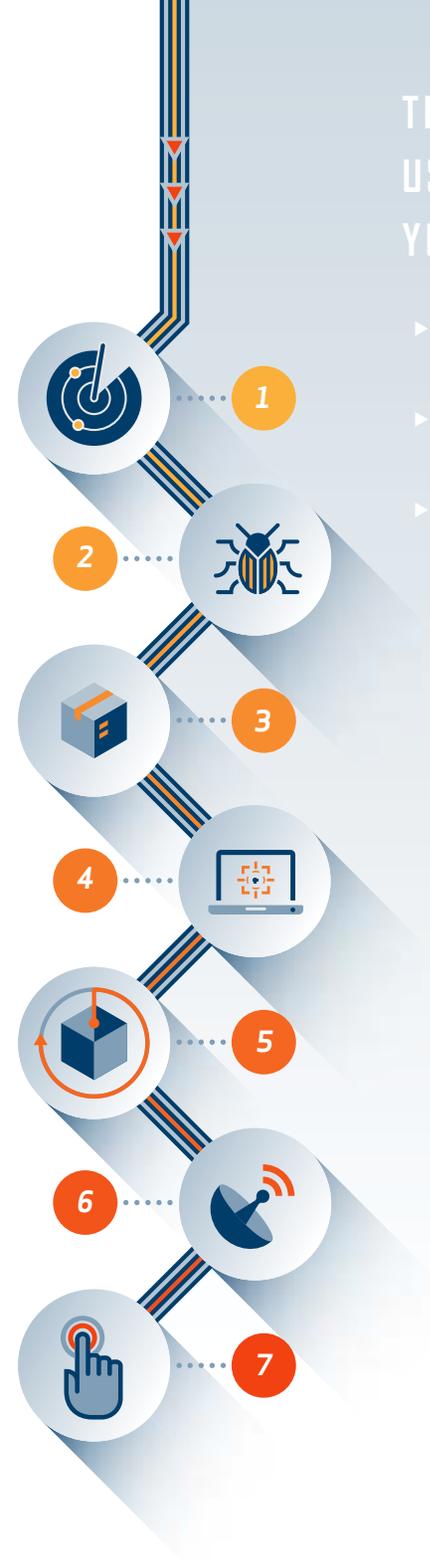
RESOURCES

White Paper

Video

Article

cyber.security@lmco.com
855-LMCYBER
855-562-9237

Connect