Kill chain

The term **kill chain** was originally used as a military concept related to the structure of an attack; consisting of target identification, force dispatch to target, decision and order to attack the target, and finally the destruction of the target.[1] Conversely, the idea of "breaking" an opponent's kill chain is a method of defense or preemptive action.[2] More recently, Lockheed Martin adapted this concept to information security, using it as a method for modeling intrusions on a computer network.[3] The cyber kill chain model has seen some adoption in the information security community.[4] However, acceptance is not universal, with critics pointing to what they believe are fundamental flaws in the model.[5]

Contents

The military kill chain

F2T2EA

One military kill chain model is the "F2T2EA", which includes the following phases:

- Find: Identify a target. Find a target within surveillance or reconnaissance data or via intelligence means.

- Fix: Fix the target's location. Obtain specific coordinates for the target either from existing data or by collecting additional data.
- Track: Monitor the target's movement. Keep track of the target until either a decision is made not to engage the target or the target is successfully engaged.
- Target: Select an appropriate weapon or asset to use on the target to create desired effects. Apply command and control capabilities to assess the value of the target and the availability of appropriate weapons to engage it.
- Engage: Apply the weapon to the target.
- Assess: Evaluate effects of the attack, including any intelligence gathered at the location.

This is an integrated, end-to-end process described as a "chain" because an interruption at any stage can interrupt the entire process.[6][7]

Previous terminology

The "Four Fs" is a military term used in the United States military, especially during World War II.

Designed to be easy to remember, the "Four Fs" are as follows:

- Find the enemy – Locate the enemy
- Fix the enemy – Pin them down with suppressing fire
- Fight the enemy – Engage the enemy in combat or flank the enemy – Send soldiers to the enemy's sides or rear
- Finish the enemy – Eliminate all enemy combatants

Proposed terminology

The "Five Fs" is a military term described by Maj. Mike “Pako” Benitez, an F-15E Strike Eagle Weapons Systems Officer who served in the United States Air Force and the United States Marine Corps.

Designed to update the Kill Chain to reflect updated, autonomous and semi-autonomous weapon systems, the "Five Fs" are described in IT’S ABOUT TIME: THE PRESSING NEED TO EVOLVE THE KILL CHAIN [8] as follows:

- Find encapsulates the unity of effort of Joint Intelligence Preparation of the Operating Environment, matching collection assets to commander’s intent and targeted areas of interest. This inevitably leads to detections, which may be further classified as an emerging target if it meets the intent.
- Fix is doctrinally described as “identifying an emerging target as worthy of engagement and determines its position and other data with sufficient fidelity to permit engagement.”
- Fire involves committing forces or resources (i.e., releasing a munition/payload/expendable)
- Finish involves employment with strike approval authorities (i.e., striking a target/firing directed energy/destructive electronic attack). This is similar to a ground element executing maneuvers to contact but then adhering to prescribed rules of engagement once arriving at the point of friction.
- Feedback closes the operational OODA Loop with an evaluative step, in some circumstances referred to as "Bomb Damage Assessment."

North Korean nuclear capability

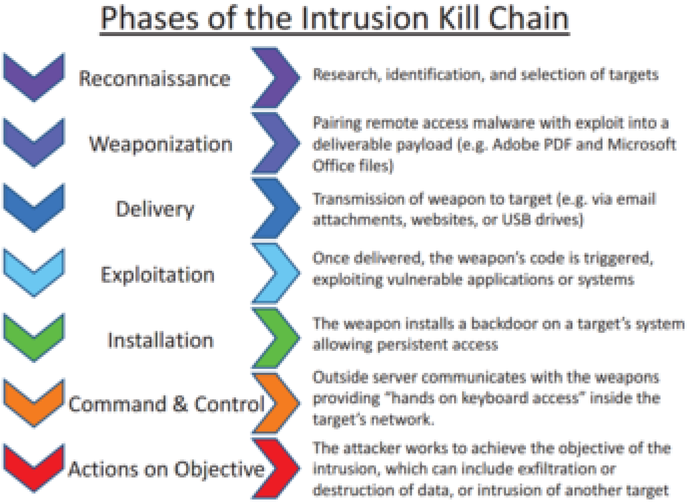
A new American military contingency plan called "Kill Chain" is reportedly the first step in a new strategy to use satellite imagery to identify North Korean launch sites, nuclear facilities and manufacturing capability and destroy them pre-emptively if a conflict seems imminent. The plan was mentioned in a joint statement by the United States and South Korea.[9][10]

The cyber kill chain

Attack phases and countermeasures

Computer scientists at Lockheed-Martin corporation described a new "intrusion kill chain" framework or model to defend computer networks in 2011.[6] They wrote that attacks may occur in phases and can be disrupted through controls established at each phase. Since then, the "cyber kill chain" has been adopted by data security organizations to define phases of cyberattacks.[12]

A cyber kill chain reveals the phases of a cyber attack: from early reconnaissance to the goal of data exfiltration.[13] The kill chain can also be used as a management tool to help continuously improve network defense. According to Lockheed Martin, threats must progress through several phases in the model, including:


Phases of the Intrusion Kill Chain
Reconnaissance
Research, identification, and selection of targets
Weaponization
Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery
Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation
Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation
The weapon installs a backdoor on a target's system allowing persistent access
Command & Control
Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective
The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Intrusion kill chain for information security[11]

1. Reconnaissance: Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.
2. Weaponization: Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
3. Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)
4. Exploitation: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.
5. Installation: Malware weapon installs access point (e.g., "backdoor") usable by intruder.
6. Command and Control: Malware enables intruder to have "hands on the keyboard" persistent access to target network.
7. Actions on Objective: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.

Defensive courses of action can be taken against these phases:[14]

1. Detect: determine whether an attacker is poking around
2. Deny: prevent information disclosure and unauthorized access
3. Disrupt: stop or change outbound traffic (to attacker)
4. Degrade: counter-attack command and control
5. Deceive: interfere with command and control
6. Contain: network segmentation changes

A U.S. Senate investigation of the 2013 Target Corporation data breach included analysis based on the Lockheed-Martin kill chain framework. It identified several stages where controls did not prevent or detect progression of the attack.[11]

Alternative kill chains

Different organizations have constructed their own kill chains to try to model different threats. FireEye proposes a linear model similar to Lockheed-Martin's. In FireEye's kill chain the persistence of threats is emphasized. This model stresses that a threat does not end after one cycle.[15]

1. Reconnaissance
2. Initial intrusion into the network
3. Establish a backdoor into the network
4. Obtain user credentials
5. Install various utilities
6. Privilege escalation/ lateral movement/ data exfiltration
7. Maintain persistence

MITRE maintains a kill chain framework known as MITRE ATT&CK® (https://attack.mitre.org/). The framework models tactics, techniques and procedures used by malevolent actors and is a useful resource for both red teams and blue teams. Pentesters can emulate this behavior during an engagement to represent real-world scenarios and help their customers determine the effectiveness of defensive countermeasures.[16] The ATT&CK framework has 4 main matrices: PRE_ATT&CK, Enterprise, Mobile and ICS. The Enterprise Matrix has categories for Windows, macOS, Linux and Cloud. The Enterprise Windows categories are:

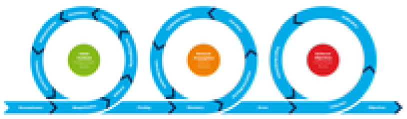
1. Initial Access - Used to gain an initial foothold within a network
2. Execution - Technique that results on the execution of code on a local or remote system
3. Persistence - Method used to maintain a presence on the system
4. Privilege Escalation - Result of actions used to gain higher level of permission
5. Defense Evasion - Method used to evade detection or security defenses
6. Credentialed Access - Use of legitimate credential to access system
7. Discovery - Post-compromise technique used to gain internal knowledge of system
8. Lateral Movement - Movement from one system over the network to another
9. Collection - Process of gathering information, such as files, prior to exfiltration
10. Command and Control - Maintaining communication within targeted network
11. Exfiltration - Discovery and removal of sensitive information from a system
12. Impact - Techniques used to disrupt business and operational processes[17]

Critiques of the cyber kill chain

Among the critiques of Lockheed Martin's cyber kill chain model as threat assessment and prevention tool is that the first phases happen outside the defended network, making it difficult to identify or defend against actions in these phases.[18] Similarly, this methodology is said to reinforce traditional perimeter-based and malware-prevention based defensive strategies.[19] Others have noted that the traditional cyber kill chain isn't suitable to model the insider threat.[20] This is particularly troublesome given the likelihood of successful attacks that breach the internal network perimeter, which is why organizations "need to develop a strategy for dealing with attackers inside the firewall. They need to think of every attacker as [a] potential insider".[21]

The unified kill chain

A unified version of the kill chain was developed to overcome common critiques against the traditional cyber kill chain, by uniting and extending Lockheed Martin's kill chain and MITRE's ATT&CK framework. The unified kill chain is an ordered arrangement of 18 unique attack phases that may occur in end-to-end cyber attacks, which covers activities that occur outside and within the defended network. As such, the unified kill chain improves over the scope limitations of the traditional kill chain and the time-agnostic nature of tactics in MITRE's ATT&CK. The unified model can be used to analyze, compare and defend against end-to-end cyber attacks by advanced persistent threats (APTs).[22]



The unified kill chain consists of 18 unique attack phases that can occur in advanced cyber attacks.

References

1. "Kill Chain Approach" (https://web.archive.org/web/20130613233413/http://cno.navylive.dodlive.mil/2013/04/23/kill-chain-approach-4/). *Chief of Naval Operations*. April 23, 2013. Archived from the original (http://cno.navylive.dodlive.mil/2013/04/23/kill-chain-approach-4/) on June 13, 2013.
2. Jonathan Greenert; Mark Welsh (May 17, 2013). "Breaking the Kill Chain" (https://foreignpolicy.com/2013/05/17/breaking-the-kill-chain/). *Foreign Policy*. Retrieved June 30, 2016.
3. Higgins, Kelly Jackson (January 12, 2013). "How Lockheed Martin's 'Kill Chain' Stopped SecurID Attack" (http://www.darkreading.com/attacks-breaches/how-lockheed-martins-kill-chain-stopped-securid-attack/d/d-id/1139125). *DARKReading*. Retrieved June 30, 2016.
4. Mason, Sean (December 2, 2014). "Leveraging The Kill Chain For Awesome" (http://www.darkreading.com/attacks-breaches/leveraging-the-kill-chain-for-awesome/a/d-id/1317810). *DARKReading*. Retrieved June 30, 2016.
5. Myers, Lysa (October 4, 2013). "The practicality of the Cyber Kill Chain approach to security" (http://www.csoonline.com/article/2134037/strategic-planning-erm/the-practicality-of-the-cyber-kill-chain-approach-to-security.html). *CSO Online*. Retrieved June 30, 2016.
6. Lockheed-Martin Corporation-Hutchins, Cloppert, and Amin-Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains-2011 (http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf)
7. Air Force Magazine, Tirpak-2000 (http://www.airforcemag.com/MagazineArchive/Pages/2000/July%202000/0700find.aspx)
8. Benitez, Mike (May 17, 2017). "IT'S ABOUT TIME: THE PRESSING NEED TO EVOLVE THE KILL CHAIN" (https://warontherocks.com/2017/05/its-about-time-the-pressing-need-to-evolve-the-kill-chain/). *War on the Rocks*. Retrieved April 28, 2020.
9. Sanger, David E. (July 6, 2017). "Tiny Satellites From Silicon Valley May Help Track North Korea Missiles" (https://www.nytimes.com/2017/07/06/world/asia/pentagon-spy-satellites-north-korea-missiles.html). *The New York Times*. Retrieved July 7, 2017.
10. "06/30/17 - Joint Statement between the United States and the Republic of Korea I U.S. Embassy & Consulate in Korea" (https://kr.usembassy.gov/063017-joint-statement-united-states-republic-korea/). *U.S. Embassy & Consulate in Korea*. 2017-06-30. Retrieved 2017-07-07.

11. U.S. Senate-Committee on Commerce, Science, and Transportation-A "Kill Chain" Analysis of the 2013 Target Data Breach-March 26, 2014 (http://www.public.navy.mil/spawar/Press/Documents/Publications/03.26.15_USSenate.pdf) Archived (https://web.archive.org/web/20161006082550/http://www.public.navy.mil/spawar/Press/Documents/Publications/03.26.15_USSenate.pdf) October 6, 2016, at the Wayback Machine
12. Greene, Tim. "Why the 'cyber kill chain' needs an upgrade" (http://www.networkworld.com/article/3104542/security/why-the-cyber-kill-chain-needs-an-upgradesecurity-pros-need-to-focus-more-on-catching-attackers-aft.html). Retrieved 2016-08-19.
13. "The Cyber Kill Chain or: how I learned to stop worrying and love data breaches" (https://blog.varonis.com/the-cyber-kill-chain-or-how-i-learned-to-stop-worrying-and-love-data-breaches/). 2016-06-20. Retrieved 2016-08-19.
14. "Archived copy" (https://web.archive.org/web/20180910164459/http://gauss.ececs.uc.edu/Courses/c6055/pdf/attackpatterns.pdf) (PDF). Archived from the original (http://gauss.ececs.uc.edu/Courses/c6055/pdf/attackpatterns.pdf) (PDF) on 2018-09-10. Retrieved 2017-05-15.
15. Kim, Hyeob; Kwon, HyukJun; Kim, Kyung Kyu (February 2019). "Modified cyber kill chain model for multimedia service environments" (https://doi.org/10.1007/s11042-018-5897-5). *Multimedia Tools and Applications*. **78** (3): 3153–3170. doi:10.1007/s11042-018-5897-5 (https://doi.org/10.1007%2Fs11042-018-5897-5). ISSN 1380-7501 (https://www.worldcat.org/issn/1380-7501).
16. Nutting, Ray (2019). *CompTIA PenTest+ certification all-in-one exam guide (PT-001)*. New York: McGraw-Hill Education. p. 75. ISBN 978-1-260-13594-7.
17. Nutting, Ray (2019). *CompTIA PenTest+ certification all-in-one exam guide (PT-001)*. New York: McGraw-Hill Education. p. 76. ISBN 978-1-260-13594-7.
18. Laliberte, Marc (September 21, 2016). "A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack" (http://www.darkreading.com/attacks-breaches/a-twist-onthe-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952). *DARKReading*.
19. Engel, Giora (November 18, 2014). "Deconstructing The Cyber Kill Chain" (http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542). *DARKReading*. Retrieved June 30, 2016.
20. Reidy, Patrick. "Combating the Insider Threat at the FBI" (https://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf) (PDF). *BlackHat USA 2013*.
21. Devost, Matt (February 19, 2015). "Every Cyber Attacker is an Insider" (https://www.oodaloop.com/osint/cyber/2015/02/19/every-cyber-attacker-insider/). *OODA Loop*.
22. Pols, Paul (December 7, 2017). "The Unified Kill Chain" (https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf) (PDF). Cyber Security Academy.

External links

- "Lockheed Martin Cyber Kill Chain" (http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html).
- "The Unified Kill Chain" (https://www.csacademy.nl/en/csa-theses/february-2018/104-the-unified-kill-chain). Cyber Security Academy.
- "MITRE ATT&CK" (https://attack.mitre.org/).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Kill_chain&oldid=966792699"

This page was last edited on 9 July 2020, at 07:02 (UTC).