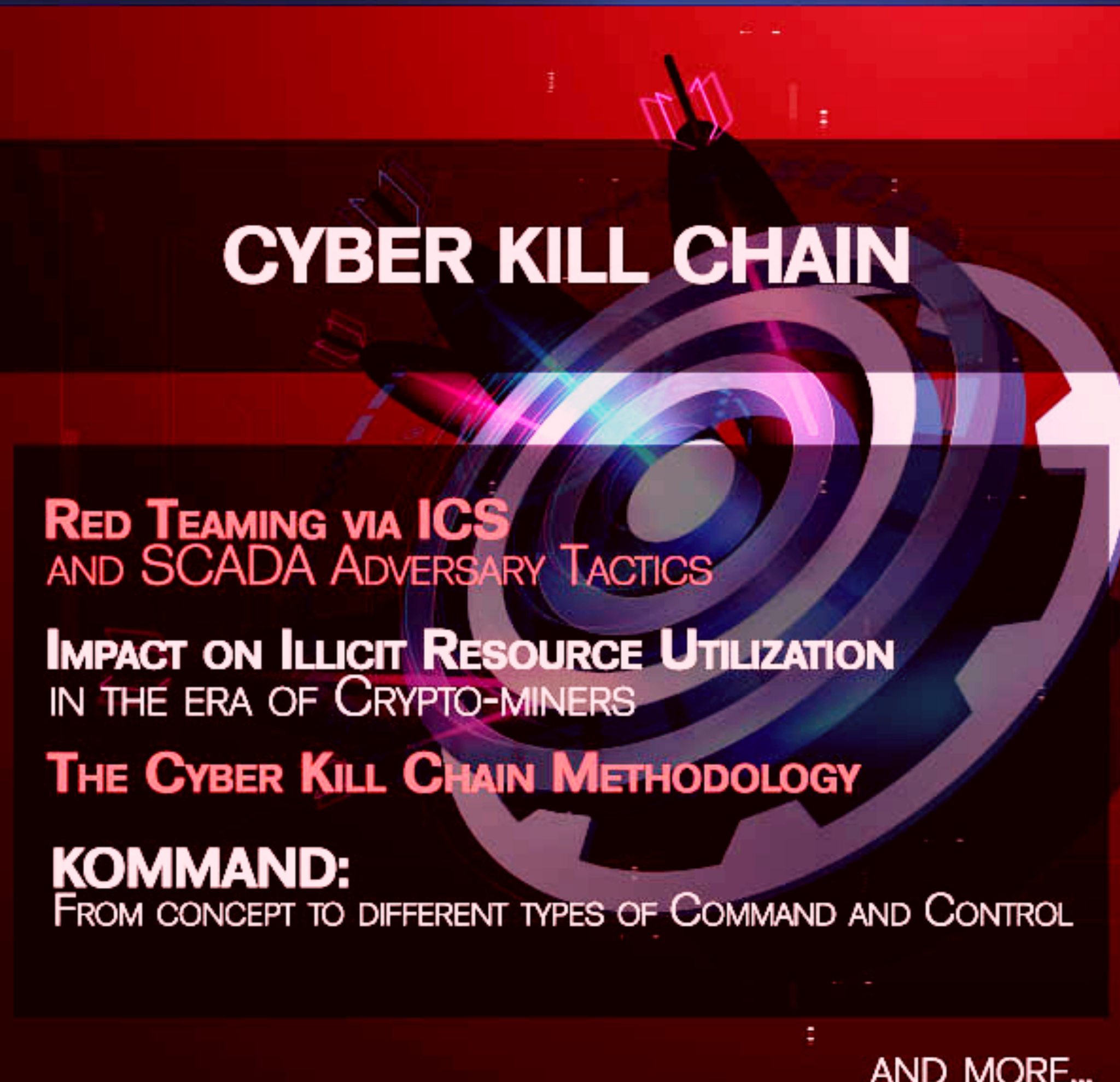
hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.16, NO. 02



CYBER KILL CHAIN

Red Teaming via ICS and SCADA Adversary Tactics

Impact on Illicit Resource Utilization in the era of Crypto-miners

The Cyber Kill Chain Methodology

KOMMAND: From concept to different types of Command and Control

AND MORE...

Dear Readers!

Our February issue is dedicated to the cyber kill chain methodology. Inside you'll find various articles, case studies and tutorials that will help you improve your hacker's work routine. Here's what's inside.

To warm up we start with The Cyber Kill Chain by Syed Peer - a brief introduction to the methodology, prevention and drawbacks, explaining how the cyber kill chain provides a clear way to build a cyber security regime.

Later we drift off to KOMMAND: From concept to different types of command and control, from which you'll learn what are command and control servers and how important they are to Red Teamers and pentesters.

Staying on the topic of Red Teaming, we have Red Teaming via ICS and SCADA Adversary Tactics and the title speaks pretty much for itself â€“ this article will help you learn how to create a safe and reliable Red Teaming ICS environment.

Later on, we have Impact on Illicit Resource in the Era of Crypto-miners, that explains what cyber kill chain means during times of increased number of cybercrimes, and how to protect yourself from cyberattacks. To help you improve your skills and work environment, we also prepared Automating with Mitre ATT&CK with Python, in which you'll learn how to automate the process of exploring threats with multiple tools, i.e. Recon-ng and Nmap.

If you're still hungry for some Red Teaming, we also have Red Team vs Blue Team, in which the author explains how both teams work together in order to provide better security.

We also prepared articles on other topics that may gain your interest. Bruce Williams in Cybersecurity Management explains how different views of businesses on cybersecurity may change the work routine and how this view depends on the business mindset. If you're looking for a more offensive topic, check out Attack with Websploit Tool.

We also have something really fresh for you - an article about the newest Kali Linux release, Kali 2021 - Pentesting with Empire & Starkiller by Daniel Dieterle.

Last but not least we will briefly touch the topic of data security and privacy in AWS and Azure, and wireless sensor network security for IoT systems.

As you can see, this month's edition is very diverse, it's important to us to provide you all kinds of knowledge, and we hope you'll enjoy reading this edition as much as we did while preparing it for you.

Stay safe!
Hakin9 Editorial Team

Contents

THE CYBER KILL CHAIN

SYED PEER

The author is a seasoned 20-year IT professional having worked in Fortune 400 companies across diverse verticals from Social Media to Banking to Cyber Security with experience managing Software Development, Engineering and Cyber Security teams.

"If you know the enemy and know yourself,
you need not fear the result of a hundred battles.
If you know yourself but not the enemy,
for every victory gained you will also suffer a defeat.
If you know neither the enemy nor yourself,
you will succumb in every battle."

— Sun Tzu, The Art of War

Introduction

In its relatively few years of its existence, the modern internet as we know it today has been on an exponential tear over the last decade. The need for speed, the adoption of ever faster components and servers and the rollout of high-speed broadband and 4G/5G networks have meant a whole new generation of applications, use cases and billions of happy customers. In fact, the next great revolution in the "Internet of Things" (IoT) will bring about a whole new meaning to the phrase "connected world" as it will encompass anything and everything that can (and will) be connected to the web. As if we were not already overwhelmed with this firehose of information, everyone from your CEO to HR to your washing machine and toaster – all will soon want to send you a notification.

As with all technologies, though, we need to take the good with the bad. The rise in internet strengths and capabilities has been shadowed equally by the increase in nefarious activity and a new breed of cyber criminals empowered with the latest hardware and software tools that make terms like "identity fraud", "ransomware", "malware" (everywhere) and "Denial of Service" (DDOS) commonplace in our daily lives and part of the 21st Century vernacular.

Background

Like so many things we take for granted as standard fare these days that have their origins in solutions within other industries (e.g. modern Project Management and Critical Path come to mind from Aerospace), so too was the case with the original "Kill Chain". Lockheed Martin, a major defense contractor for the US Military (DOD), was instrumental in deriving the "Kill Chain" model based upon its military use case. Being a military defensive concept in principle and execution, the "Cyber Kill Chain" that originated at Lockheed focuses on the attacker's perspective and the different stages identified in the process and required threats to be addressed to counter these types of attacks.

The original military framework was modeled to identify the threat (or malicious attacker), prepare for an attack mechanism, engage the enemy and ultimately to bring about the destruction of the threat. Based upon historical military campaigns on record and known adversarial strategies, the Cyber Kill Chain tries to anticipate the logical steps taken by the attacker and to recognize and identify a best-case defense approach. It is part of a larger process called "*Intelligence Driven Defense*".

Cyber Kill Chain Methodology

The Cyber Kill Chain framework is differentiated from other approaches based upon its seven core stages that try to encompass the whole breadth of an attacker's work plan from the initial reconnaissance, to surreptitious (lateral) movement across the target territory (or network) and retrieving valuable (data) assets (exfiltration).

The Cyber Kill Chain has become an essential part of an organization's Cyber security strategy and helps them to better understand and predict how an attacker works and thinks in order to select the appropriate tools and strategies to counter the attack or address any on-going attacks and ultimately to limit the chances of an expensive data breach.

Having decided on a "value target" organization (or individual), the Cyber Kill Chain is comprised of the following seven logical stages:

- **Stage #1 – RECONNAISSANCE (Identifying the target)**: This initial stage is focused on harvesting as much information as possible on the identified "value" target. Employee email addresses, affiliations, joint ventures with sister companies and, if possible, corporate and IT staffing levels and network administrator information from Social Media platforms. At this stage, all information is good information. It enables the attacker to create a useful profile of the target by triangulating information from disparate sources. This stage may take weeks or even months to complete but the more time expended on this stage builds a more accurate profile and increases the likelihood of a successful breach in the future.

- **Stage #2 – WEAPONIZATION (Preparation for the attack)**: Having identified a vulnerability or exploit at the "value target", this next stage involves the attacker preparing the necessary toolkit to use for the attack. The choice of tools will essentially depend on the motives for the attack, such as malware/ransomware (e.g. Norsk Hydro Aluminum) or whether to extract valuable information (e.g. Equifax, Verizon) or render the target inoperable or cause permanent damage (e.g. Aramco, Stuxnet). The attack vector may be a newly re-engineered version of an earlier attack binary used effectively before but with specific bells and whistles added - suited especially for the target organization. This re-engineering effort helps in evading any existing controls in place at the target but its sophistication depends on the attacker's skill and funding. With the approach and malicious motive being so broad, almost anything and everything is game for consideration by the attacker.

- **Stage #3 – DELIVERY (Introduction to the target)**: This stage involves the execution of the actual attack on the target with the sole intent of delivering a malicious payload. At this stage "radio silence is bliss" as the attacker attempts to infiltrate the target defenses stealthily with only the intent to seed the payload without fanfare

and noise or raising the alarm bells of any existing monitoring controls. The methods employed quite regularly are by means of email attachments (spear phishing with malicious code embedded into a pdf document) or website redirection for credentials theft (cross site scripting) or removable media, such as memory stick/CD ROM. From the defender's perspective, the arrival of this weaponized bundle at their doorstep affords the first and most important checkpoint to address and block or neutralize the threat with its internal defenses and tools.

☑ **Stage #4 – EXPLOITATION (Detection of security flaws/vulnerability)**: This stage involves making use of a newly discovered vulnerability to execute errant code on the target system with the intent to remotely manipulate at a later stage in the Cyber Kill Chain. We can say that the target system has been "technically compromised" at this stage. After the successful delivery to the target host system, this stage executes the intruder's code. This stage will likely exploit either an operating system or application vulnerability, or leverage stolen users' elevated credentials with necessary permissions to allow their code to run.

☑ **Stage #5 – INSTALLATION (Setup the backdoor):** This stage involves the setup of a remote access Trojan or backdoor to allow the attacker continued persistent access to the target host environment. This process is done with stealth and often with active participation of the target user with the necessary administrative privileges to enable and run the malicious attacker's code within the target host environment.

☑ **Stage #6 – COMMAND AND CONTROL (C2) (Remote control of target)**: Attackers open a channel to an external internet Control Center (C2) server to orchestrate further actions from the outside. This is the last opportunity defenders at the target may have to block access to the outside by means of denying attackers rights to execute commands, etc. This setup is established manually mostly by means of using internal resources with necessary administrative privileges. Once the channel is established, the attacker quickly establishes command and control over multiple workstation nodes on the network in an effort to mask malicious behavior across multiple machines so as not to raise suspicion for recorded anomalies in the logs. Once completed successfully, the attacker will have access to execute any binaries on the host target system.

☑ **Stage #7 – ACTIONS ON OBJECTIVES (Achieving intruder goals)**: Compromised systems lend themselves to all manner of encryption, exploitation and exfiltration whether that be intellectual property theft, engineered sabotage or plain data harvesting. At this stage, the attacker has successfully infiltrated the host system and has all necessary tools and access privileges to steadily dig deeper and become fully entrenched.

Courtesy Lockheed-Martin

Prevention

Let's briefly address each stage and defender mitigation options available:

1. **RECONNAISSANCE:** Defenders should establish next generation firewalls to enforce perimeter defense. Monitor for vulnerable entry points and establish endpoint security and log suspicious activity. Setup a Desktop Support dedicated email handle for routing all suspicious emails received by users to the IT Security function. Discourage users from advertising their company emails on social networks, messages or self-registration on

websites. Pay special attention to mailboxes of critical staff and senior management to prevent email spoofing and credential theft. Advise management on restricting publicly available company data such as ERP Systems or application upgrades and the like.

2. **WEAPONIZATION:** Establish Employee Awareness programs for Cyber Security internally. This should follow a standard annual frequency with tips and guides for users identifying weaponized communications. Celebrate Cyber Security Month every October to ingrain the security mantra throughout the organization. Establish spam filters and attachment sandboxed analysis to quarantine suspicious malware attachments. Enhance mail detection tools used internally for all inbound traffic. Only allow authorized portable media (such as company issued USB sticks) or provide Self-Service Help Desk Kiosks for users to validate external supplied USB media before attaching to network connected nodes or from contractor laptops.

3. **DELIVERY:** Defenders should protect against phishing attacks especially for critical senior members or those with elevated privileges. Administrators should be forced to use multi-factor authentication for Server Farm access and their passwords routinely refreshed on an agreed schedule. Monitor for anomalies in user login behavior and log their times and locations. Investigate new files and folder creation for unusual activity. Keep patch management cycles up to date with latest vendor approved releases. Discourage use of departmental "shares" and group servers that auto connect at login. Establish as standard policy the running of Penetration Tests by externally approved providers to identify risk and vulnerabilities proactively.

4. **EXPLOITATION:** Defenders should maintain devices and application software patches up to date whenever possible. Use reliable anti-virus protection at all endpoints. Establish a Host Based Intrusion Prevention Systems (HIPS) to alert or block common installation pathways. Conduct regularly scheduled vulnerability scanning with an industry leading tool (e.g. Nessus from Tenable). Establish server build hardening procedures and scripts (e.g. Ansible, Puppet) before releasing servers to common users and departmental business owners.

5. **INSTALLATION:** Implement network segmentation and virtual LANS to effectively isolate groups and individual systems from cascading intrusion spread. Prohibit and eliminate shared User Accounts across the organization and correctly implement Group Membership to accommodate user needs. Enforce password security best practices and complex password regimes to avoid trivial brute force success. Establish "Zero Trust Security" to mitigate compromised reach and further damage across the network

6. **COMMAND AND CONTROL (C2):** Establish a regime of continuous scanning for threats. Utilize intrusion detection systems to alert the organization of potential new applications trying to gain access to the network. Hackers will typically complete the C2 stage via a beacon over an external network pathway using the HTTP or HTTPS protocols. When available, analyze malware for red flags of Command and Control (C2) infrastructure.

7. **ACTIONS ON OBJECTIVES:** Having reached this stage the attacker's mission has already been accomplished or is currently underway at the target environment. The attacker's motives may be varied based on intent and the target organization will need to take appropriate actions to counter. Best practice suggests taking steps to detect signs of exfiltration and employ necessary Data Loss Prevention tools to alert and reduce the loss

exposure. Run analysis reports from the tool to analyze every alert raised. Fallback to your Incident Response Procedure to follow clear communication guidelines and escalation routes as necessary.

Drawbacks

Although widely adopted in spirit across the industry, the Cyber Kill Chain has some detractors who have raised some valuable criticisms.

- ☑ While revolutionary in its own time, the focus on perimeter defense and the outsider attack threats are considered outdated when confronted by the very real modern-day insider threat scenarios. Insider threats were not factored into the framework at the time of its inception whilst these are quite prevalent today and an everyday occurrence.

- ☑ Consequently, the Cyber Kill Chain postulates that during the Weaponization, Delivery and Installation stages the malicious payload is crafted as malware or a virus specific to the organization and needs to be dropped into the target network. For insider threats, though, stages 2, 3 and 4 then become irrelevant.

- ☑ The current broad adoption of cloud infrastructures and associated architecture has largely eliminated the "castle and moat" legacy approach and thinking for cyber security.

- ☑ The first two stages of the Cyber Kill Chain (namely Reconnaissance and Weaponization) are beyond the line-of-sight of an organization and difficult to detect outside of the standard monitoring tools already in place.

- ☑ The first iteration of the Cyber Kill Chain model appeared in 2011 and many see this as both dated and not easily adaptable to the rigorous needs of defending against modern day Advanced Persistent Threats (APTs) in cyber security.

- ☑ Current thinking suggests that additional stages need to be folded into the framework such as Obfuscation/Anti-Forensics, and Denial of Service before the final stage. Moreover, the modern expert view is that the Cyber Kill Chain is circular in nature and that reaching the final stage is not the end of the threat.

Conclusion

While not a single tool or application in itself, the Cyber Kill Chain still provides an organization a clear pathway to build out their Cyber Security regime. The Cyber Kill Chain identifies the different stages and can help in the selection of appropriate tools. It continues to provide a baseline for the security strategy, which can be tweaked and supplanted as per the specific needs of an organization.

References:

- Lockheed-Martin: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- Norsk Hydro: https://www.infosecurity-magazine.com/news/norsk-hydro-outage-destructive/
- ARAMCO: https://money.cnn.com/2015/08/05/technology/aramco-hack/
- EQUIFAX: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html