Challenges and Countermeasures in Disrupting the Cyber Kill Chain

Hammaz Ahmed

Department of Professional Studies, Saint Louis University

CYBR-5000: Cybersecurity Principles

Jeff Robertson. Teacher

October 4, 2023

Abstract

The paper will start off by giving a briefing on the background of cybersecurity and move on to discuss the "Cyber Kill Chain" structure, which was originally introduced by Lockheed Martin, and since then has become a crucial framework in understanding and guarding against cyberattacks. This model studied APTs and identified 7 phases that most APTs follow during their course of attack. This research paper provides an Analysis of the entire Cyber Kill Chain and a detailed Analysis of the *Delivery step*. The study starts by explaining each of the steps involved in the Cyber Kill Chain and providing instances of each stage. Eventually, it goes on to provide in-depth scrutiny of the Delivery phase, providing real-world scenarios and how organizations successfully or unsuccessfully countered the attacks that used the Cyber Kill Chain framework. In summary, this paper will conclude writings and underscore the Overview of the Cyber Kill Chain, Historical Analysis, Different phases, Real-world scenarios, Threat actor behaviors, Defensive strategies, Limitations and Criticisms, and some Future Trends. In the end, this paper also states a few pieces of advice that I as a consultant would give to the CISO/CIO of an organization to mitigate the Delivery step of the Cyber Kill Chain.

Keywords: Cyber Kill Chain, APTs (Advanced Persistent Threat), CISO/CIO.

Challenges and Countermeasures in Disrupting the Cyber Kill Chain

Need for Cyber Security

Organizations today spend a significant amount of money on securing their networks and internal infrastructure**.** According to Rosenbaum (2021), Microsoft is *quadrupling* its cybersecurity investment to $20 billion in the next five years. Even small businesses are spending quite a bit on protecting their security and data. In today's digital realm, cybersecurity has its own place.

Protection of Sensitive data: Data is considered the digital gold. It can include PII (*Personally Identifiable Information*), date of birth, credit card numbers, health-related information, and much more. These credentials are to be protected or else it will be a breach of privacy and the organization will lose its reputation.

Prevention of Financial Loss: Loss of data and other valuable information can lead to severe consequences including *financial loss*. This could lead the company to have dire ramifications.

National Security: Government agencies and contractors often contain sensitive information that, if leaked, can have serious consequences. This information can include militant and defense information, data related to politics, and much more.

Business Continuity: Once an organization has been breached it cannot function properly any longer. It might even have to completely shut down until all the issues have been resolved and there's no more threat. This has severe repercussions for its reputation and financial well-being.

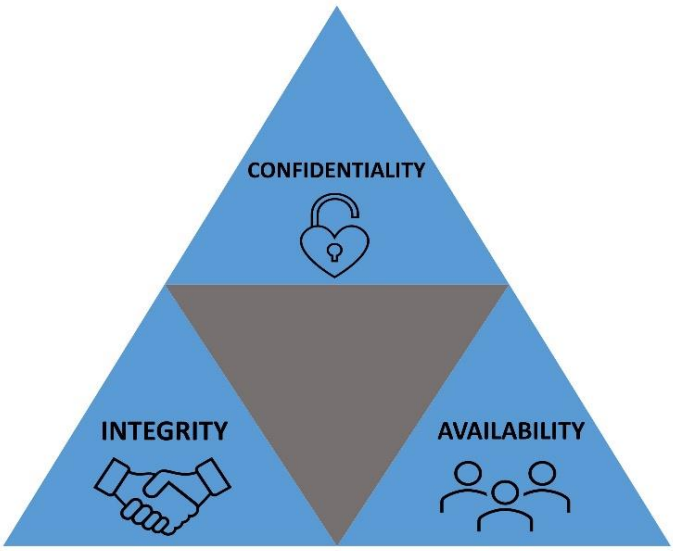
Background and context of Cyber Threats:

Cybersecurity began in the 1970s when researcher *Bob Thomas* created a computer program called "*Creeper*" that could move across ARPANET's network, leaving a breadcrumb trail wherever it went. The first example of an antivirus program was written in the year 1973 called the *Reaper,* which chased and deleted Creeper (Bhadwal, 2023).1997 was the birth year of commercial malware examining antiviruses. The Creeper was designed as an experimental program and affected the TENEX operating system. It displayed a message "*I'm the creeper,*

catch me if you can." Creeper was also a worm which means it was spreading across the network without the user's knowledge. In 1977 the CIA Triad constitutes *Confidentiality, Integrity, and Availability* and is shown in Figure 1. It was introduced (Ruthberg and McKenzie, 1977). The CIA triad is the pillar of today's cybersecurity.

Figure 1

The CIA Triad



It was not until the late 2000s that criminal organizations started to heavily fund professional cyber-attacks (GeeksforGeeks, 2022). *Cyber threats* refer to malicious activities that target computer systems, networks, and digital infrastructure with the intent to compromise their security, steal sensitive information, or disrupt operations. These threats include Malware, Phishing, DDoS, and many more.

Figure 2

Cyber Threats in 2023

Some of the biggest moments in Cyber Security history in the last 10 years are stated below:

1. 2011: Sony's PlayStation Network and Sony Pictures suffer multiple attacks.
2. 2012: Global Payment System Data Breach
3. 2014 and 2014: Target and Home Deport Credit Card Stolen.
4. 2014: Sony Dealt Another Blow with Attack on Sony Pictures Entertainment.

Cyber Kill Chain:

A Kill chain is a systematic process to target and engage an adversary to create desired effects. U.S. military targeting doctrine defines the steps of this process as find, fix, track, target, and engage (Hutchins et al., 2014). The cyber kill chain is a framework that was developed by *Lockheed Martin*. It is widely used to understand and counteract cyberattacks by dividing them into different stages of a lifecycle. The idea behind the kill chain is to make it difficult for the attacker to gain access to a system.

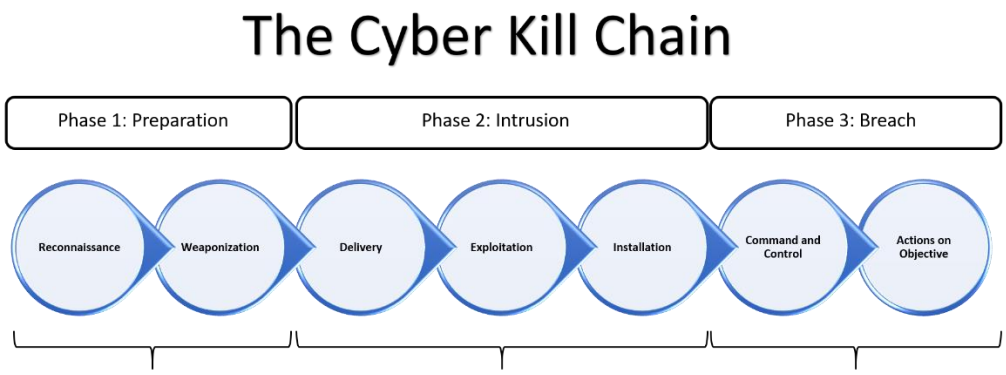
Advanced Persistent Threats (APTs):

An *Advanced Persistent Threat* is a highly sophisticated and protracted cyber-attack wherein an infiltrator clandestinely establishes a long-term presence within a network, with the objective of quietly stealing sensitive data over a long duration (CrowdStrike, 2023). Some main objectives of APTs can include Cyber Espionage, E-Crime, and Hacktivism. Examples of used APTs include GOBLIN PANDA(APT27), FANCY BEAR(APT28), Cozy Bear(APT29), Ocean Buffalo(APT32), and many more.

The *Lockheed Martin* Cyber Kill Chain introduced a popular model that studied APTs and identified the 7 phases they follow during the course of their attack. Figure 3 gives an overview of the cyber kill chain steps.

Figure 3

Cyber Kill Chain



Reconnaissance: This is the initial and most important phase of the APT life cycle. It consists of several crucial steps required for the overall process. Reconnaissance involves the comprehensive and detailed collection of information about the target to the greatest extent possible. APT actors spend a lot of time on this step to carry out the plan. Diligent reconnaissance of the target yields valuable insights that enable the threat actor to gain a deeper understanding of the organization they are targeting. This aids them to have a better grasp of the business processes, technology, and the inside infrastructure. Wrightson (2105) stated that the

information from Reconnaissance is used to create a scheme of the victim's IT system to find vulnerabilities that could be exploited and gain access to their systems by bypassing the security controls. Gathering information on non-technical assets of the target is equally significant. There are other methods for attackers to gather valuable information which can include details on employees' job roles, their functions, and online activities. Reconnaissance can itself be divided into 2 more steps: *pre-exploitation* and *post-exploitation*. Pre-exploitation involves gathering information about the target while post-exploitation is done after a strong foothold has been established on the target (Wrightson, 2015).

Table 1

Reconnaissance Techniques used by Threat actors.

Reconnaissance Methodology	Type of Reconnaissance	Techniques Used
1. Target Identification and Selection.	Passive	Domain names, whois, records from RIPE, ARIN.
2. Target Profiling.		
a) Target Social Profiling.	Passive	Social Networks, Public Documents, and Corporate Websites.
b) Target System Profiling.	Active	Ping sweeps, Finger printing, Port scanning.
3. Target Validation	Active	Spam messages, Phishing, and mails.

Weaponization: This is one of the key steps in the APT's life cycle. In this step, the attacker's main goal is to gain access to the vulnerable system. Once the vulnerability is found using the previous step, those identified *weak points* are exploited. The threat actor creates a malicious *payload*(data) which can be comprised of malware, viruses, or any exploit code that is used to target the weak and vulnerable spots in those systems. Weaponization can take place in many different formats. Victims can be manipulated into accessing a website or portal that is

malicious. One of the easiest ways can be when the threat actor hides superficially legitimate files and tricks the victim into downloading them. Something called an exploit kit is used more often. It can be defined as a toolkit cyber criminals use to attack vulnerabilities in systems so they can distribute malware or perform other malicious activities. Adobe Flash exploit kits were extremely popular in the past, with the phaseout of the software causing a steep decline in exploit kit deployment. More recent studies see a shift towards Microsoft product exploits (Driscoll, 2020). One can use certain steps in order to protect and shield themselves against this weaponization step. Patching and updating are the most important. Many systems are exploited

when they don't have the current running software. Since weaponization can be done when the victim downloads a malicious file, implementing email security is very crucial. The web is also used for blocking suspicious websites.

Table 2

Exploit kits and their timeline

EXPLOT KIT	2014	2015
ANGLER	• Infected PoS Systems • Delivered CryptoWall, TeslaCrypt, CryptoLocker Ransomware • Dropped the DRIDEX Malware • Delivered the CryptXXX Ransomware	
BLACKHOLE	• Spread Zeus P2P variant "Gameover"	
MAGNITUDE	• Linked to Malicious ads on Yahoo sites	• Exploited a patched Adobe Flash Player flaw. • Delivered CryptoWall ransomware
SUNDOWN	• Delivered card scraping Kasidet worm.	• Employs use-after free vulnerabilities in Adobe Flash

		player.
SWEET ORANGE	• Included in a Malicious YouTube and campaign.	

Delivery: This step is built upon the previous step of weaponization. The primary objective of this phase is to deliver the malicious code to the target system. This will aid the attacker in having a strong grip. This stage involves the use of cyber weapons and tools. We will be discussing some methods which are used frequently. First and foremost is phishing. This is the most common method of delivering malicious code. It can include malicious attachments. The purpose of the threat actor is to trick the user into downloading these files or clicking on a link that looks legit. A method called Drive-by-downloads is also quite routine. Bad actors use legitimate websites, or they make one that looks real. Once the user accesses these sites, the malware is automatically executed without their knowledge.

Exploitation: Exploitation is the step that follows the previous three. This is the stage where bad actors prey on vulnerabilities. These exploits and vulnerabilities are the ones that were discovered in the reconnaissance phase and eventually deployed in the next phase which was Delivery. Let's discuss some of the proactive measures we can use to avoid this part of the cyber kill chain. Patching and updating can fix a lot of security problems. This step is no different. One can implement stricter access controls which means limiting access to and modifying sensitive data. Network segmentation is crucial since it can help to desert systems which makes it difficult for the attacker to move easily across the network.

Installation: Once the threat actors successfully exploit the victims and gain access to their network the installation phase starts. This is done by transferring the malware to the victim's computer to exfiltrate data. Some of the strategies used in this phase can include Trojan Horses, Backdoors, and Command-line interface. Fortunately, there are some ways we can avoid this phase of the cyber kill chain. Organizations can use training and awareness. Employees can be taught about the dangers that come with opening random emails that can contain malicious files. Email security measures like DMARC (Domain-based Message, Authentication, Reporting, and Conformance and DKIM (Domain-keys Identified Mail) can be kept in place. Web filtering and software patching are some other ways to avoid the malicious installation phase.

Command and Control: This step is often referred to as the C2 stage. Once the malware or something similar has been installed on the victim's system the threat actors start to communicate with the malware. This can be established by setting up a command-and-control server that can send instructions to the malware. Covert channels are generally used here to avoid detection. Covert channels can be defined as an unintended or unauthorized intra-system channel that enables two cooperating entities to transfer information in a way that violates the system's security policy but does not extend the entities' access authorization. Another key term "Obfuscation" is used here. It means the threat actor makes it look like there's no threat present now by covering their tracks.

Actions on Objectives: This is the last step in the cyber kill chain. After the collecting victim's information, developing malware, and installing it in their computer it's time for the threat actor to take action. Which includes DDOS attacks, Ransomware, and many more. These attacks are among the many used by malicious actors. Plans should be made beforehand to tackle this step. There should be a well-defined incident response plan to quickly detect, contain, and recover from the breach. New plans can be made after the incident took place, hence learning from the mistakes.

Table 3

Overview of Cyber kill chain stages

Stage	Description	Key points
1. Reconnaissance	Gather information on Target	• Research Targets. • Identify weakness. • Collect intel.
2. Weaponization	Develop or secure malicious code	• Create malware. • Weaponize code. • Prepare for attack.
3. Delivery	Send malicious payload to target	• Phishing emails. • Malicious links. • Infected files.
4. Exploitation	Exploit vulnerabilities to gain	• Vulnerability exploitation.

	access	• Gain initial access.
5. Installation	Establish a foothold on the target system	• Install Malware. • Establish control mechanisms.
6. Command and Control	Establish remote control over compromised systems	• Set up C2 channels. • Communicate with malware.
7. Actions on Objectives	Achieve the threat actor's goal.	• Data Manipulation. • System Disruption. • Achieve Goal. • Financial Gain.

Detailed Analysis of Delivery Phase

Each step in the Cyber Kill chain has its own significance to the overall process, yet some are considered more lethal or impactful than others. The third step, Delivery, is one of them. What makes this step critical is the amount of damage it can inflict upon the victim. Most of the cyber-attacks out there need some kind of interaction with the victim. Examples include downloading unsafe PDF's, visiting malicious websites, and redirecting sites. This step can act as a double-edged sword. While it's in progress, it is possible for the malicious code to leave traces behind, and by applying the digital forensics method it can be traced back to the original source or the hacker. To avoid this problem Delivery step is carried out mostly using paid anonymous applications, malicious websites, and hacked or compromised email accounts.

While delivering a payload, multiple delivery methods are also used because no single method can guarantee 100% success. Failed attacks are also useful since they can be a source of information from the victim's system (Yadav and Rao, 2015).

Table 4

Delivery methods and their characteristics.

Delivery Mechanisms	Characteristics
1. Email Attachments	Email content and attachments are made intriguing for download.
2. Phishing Attacks	Personally Identifiable Information and Sensitive data can be extracted using these attacks.
3. Drive By Download	The victim is forced to download malicious content and files like PDF, word files, and software setup guides.
4. USB/Removable Media	Unknown USB media is inserted inside the system without proper identification
5. DNS Cache Poisoning	Forged or fake DNS is injected into cache of a DNS resolver.

Defining each Mechanism:

Email attachments belong to the most common and easiest method in the Delivery step. This step demands the malicious attachments be sent to the victim with the hope that they download it. The attachment looks normal on the surface, but it contains hidden malicious code. Once executed the delivery of malicious code into the target system is done. These files can be executable Word files, PDFs, and ZIP archives. Malicious files like Java Script(.js), VB script(.vbs), power shell (.ps1) can also be attached to email and sent to the victim. Executable files like e.g., exe, .dll can execute malware once they are opened. Another crafty method is by using Archived files. Threat actors compress files into ZIP or RAR so that the malicious code is not easily detectable and can hide itself properly. URLs are also a pretty common form of delivery method. Since they look intriguing and can be easily executed with just one click without any form of download. Steps can be taken by organizations to avoid this method of delivery. Employees should be trained in identifying emails coming from untrusted sources and

scanning every file they are downloading. Deploying best security practices is important, which can include software updates and using antivirus software.

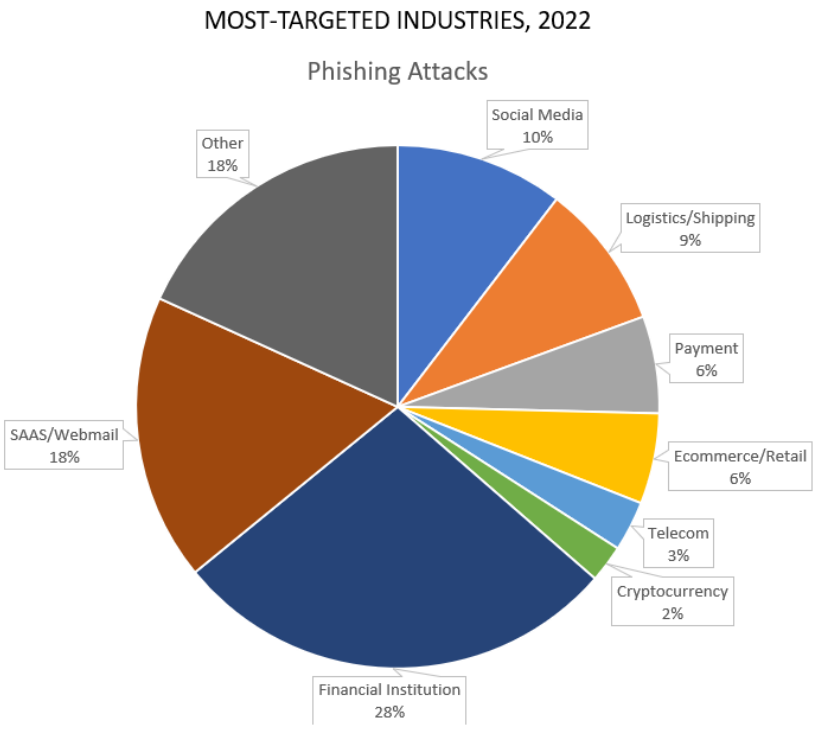
Common signs of Malicious emails:

- Being Cautious while opening emails.
- Emails showing signs of urgency.
- Improper opening remarks and generic greetings.
- Unknown senders.

Phishing Attacks: Phishing email statistics suggest that nearly 1.2% of all emails sent are malicious which in number translates to 3.4 billion phishing emails sent every day. Extortion of over 33 million records is expected to occur by 2023 with ransomware or phishing attacks occurring every 11 seconds (James, 2023). Phishing attacks are extremely common. They have different types of ways around the target. The figure below shows the most targeted industries in 2022.

Figure 4

The industries that experienced the highest level of focus in 2022



Spear Phishing: This involves a malicious actor acquiring personal information about a particular person and crafting their emails and messages accordingly. Spear Phishing is used on high-value targets like CEOs and stakeholders. Threat actors use samples of legitimate messages that were earlier sent by the organization and tailor them to wheel in the target. To best protect ourselves from phishing attacks one should

- Not open suspicious emails, links, and attachments.
- Utilize multi-factor authentication.

Vishing: This attack falls under Phishing and uses automated voice or one generated by AI to fool the victims. AI can be used to mimic the voices of close friends and family members in order to trick the victim. AI can even understand NLP (Natural Language Processing) which makes the voice mimic more persuasive.

We can prevent vishing by:

- Identify Pressure and Scare Tactics.
- Ignore calls from unknown numbers.
- Be wary of any caller that asks for sensitive information like PII and credit card details.

Figure 5

Mechanism used by attackers using Vishing

Other forms of Phishing can include Smishing which uses fake text messages and tricks victims to reveal sensitive information. Pharming redirects targets to fraudulent websites even though they think they are opening a legitimate one. Whaling is similar to spear-phishing in the sense that both utilize targeted attacks, social engineering, and impersonation. Whaling is more like a subset of spear phishing where the attacker only goes for high-value target. Angler Phishing which takes place on social media platforms. Phishing attacks continue to evolve with new methods coming every now and then. The best way to avoid being a victim is to be wary of people asking for PII and other personal details. Below are some statistics given by Rushton, 2023 on Phishing:

- 83% of all companies experience phishing attacks every year.
- There was a 345% increase in unique phishing sites between 2020 and 2021.
- There were 300,497 phishing attacks reported to the FBI in 2022.
- Each phishing attack costs $4.91 million, on average.

Drive-by-Download: A drive-by download is a download that occurs without the user's action or knowledge. It usually triggers a vulnerability in a browser to download an unknown file (Ibrahim & Heramni, 2019). Since drive-by-downloads are silent in nature and happen without the user's knowledge, they are hard to detect. Threat actors use Compromised Websites that look like legit websites at the surface but are injected with malicious code. Another method that is quite commonly used is Exploit Kits. These software packages exploit vulnerabilities are website plugins. Regardless, of the different methods used one can use precautions and ways to potentially detect a Drive-by-Download.

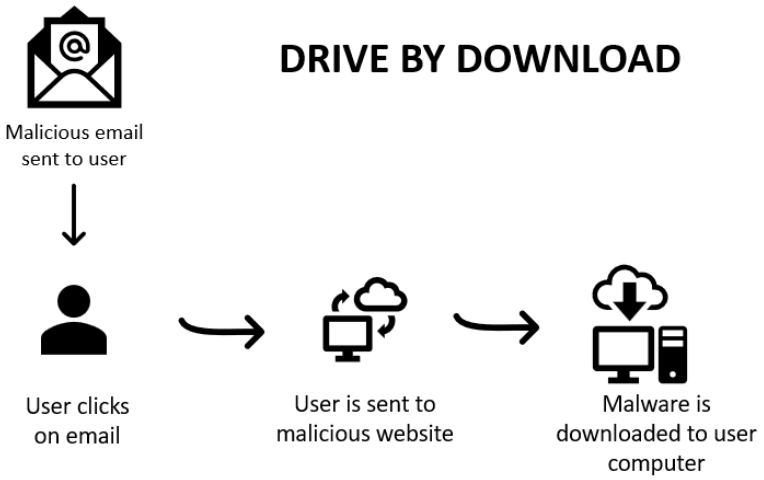
- Antivirus and Anti-Malware: These are software that can conduct regular scans and notify us if there are any suspicious files in our system.
- Web browser settings: Most current web browsers are designed in a way to detect and avoid drive-by downloads. We need to make sure the browser is configured correctly and can block websites that are malicious and end up causing drive-by downloads.

- Browser Extensions: NoScript(Firefox), ScriptSafe(Chrome), WOT(Chrome, Edge, Firefox) are some of the Browser extensions that can help users avoid drive-by-download.
- Sandboxing: Using an isolated environment or Sandbox while browsing can reduce the risk of drive-by downloads.

The below graphic demonstrates the mechanism involved with drive-by downloads.

Figure 6

Mechanism used in Drive by Download



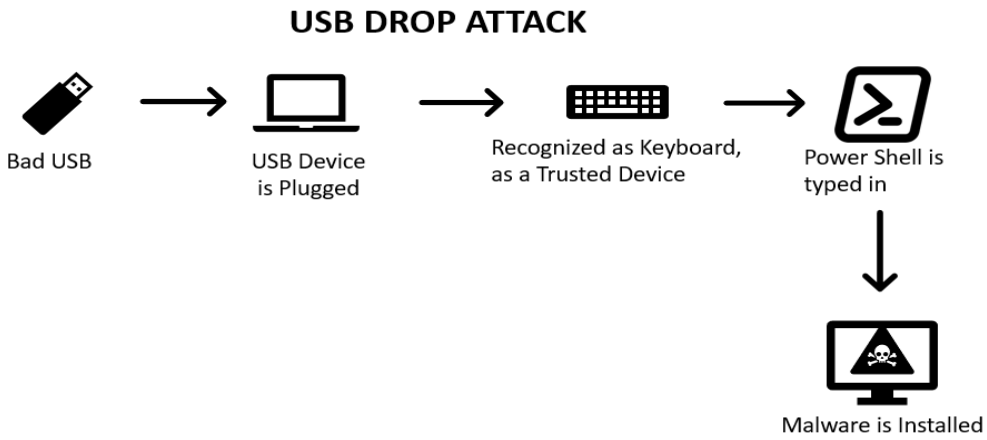
USB/Removable Media: This method belongs to somewhat of a physical delivery of malicious malware or code. The main goal of this method is to inject Malware into the victim's system. The method of Auto-Run and Auto-Play can be utilized here. The system tends to run some processes once a USB is plugged in and attackers place the malicious file in those parts so the malware script is executed as soon as the USB is plugged in. Device Emulation is also used where attackers emulate or imitate other devices like keyboards and mouse and once these are plugged in the malware script is executed. Organizations can implement several things to avoid these threats.

- Implement USB policies: Companies should implement strict policies on USB and removable devices. Only scanned devices should be logged into a system.

- Endpoint security controls: These controls can block malicious activities from an external device like a USB.

Figure 7

USB drop attack mechanism



DNS Cache Poisoning: This method belongs more on the tricky side of what threat actors use to compromise a system. It works by manipulating the Domain Name System (DNS) and captures users' network traffic by redirecting them to malicious websites. The steps to DNS Poisoning are discussed below:

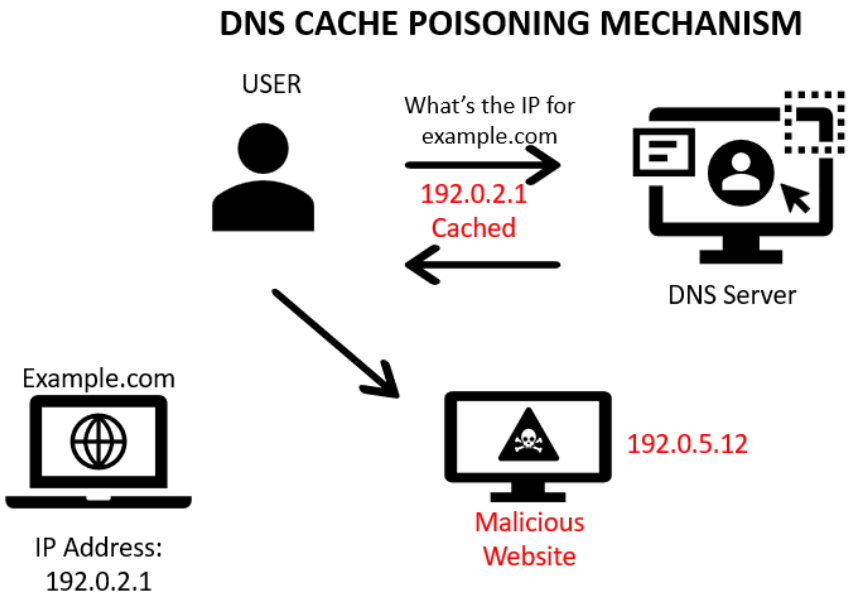
- Identification of vulnerable DNS servers.
- Threat actor sends forged requests to the server.
- The DNS server might accept the request if it does not have weak security measures.
- End-users try to access the usual-looking websites but in turn get sent to the malicious website. The cache has been previously forged, redirecting the user to the false website.
- These users are subjected to various attacks like Phishing, data theft, and much more.

DNS poisoning can have adverse consequences. To protect ourselves from this, we can use DNSSEC (DNS Security Extension). It protects the user by digitally signing the data to confirm its authenticity. Using firewalls is also crucial since we can cut out traffic even further hence reducing the risk of DNS Poisoning. Using DNS over HTTPs or DNS over TLS is

important. These protocols encrypt DNS requests therefore making it tougher for attackers to manipulate it.

Figure 8

Manipulating DNS cache to enter malicious data



Mitigating the Delivery Phase:

First, let's talk about who a CISO/CIO is and what are their roles in an organization. The terms stand for Chief Information Security Officer and Chief Information Officer respectively. Tillson (2023) described the role of CISO as "Someone responsible for ensuring that the organization's data is secure and ensuring that the organization complies with relevant regulations and that it can respond to cyber incidents effectively". Depending on the organization, the CISO can report to different authorities. Usually, they report to the CIO, but there's been an upward trend of the CISO reporting directly to the CEO of that organization or the Board of Directors.

There are several ways we can personally advise the CISO of a company to reduce or mitigate the overall risk of the Delivery phase in the Cyber Kil Chain. Some of them are:

Advanced Email Filtering: Heaps of cyber-attacks are carried out through hoax and malicious emails. Email filtering that uses *machine learning*, *artificial intelligence*, and *advanced threat intelligence* can assist in blocking spam mail in a more sophisticated and automated way. Some of the current in-demand tools to achieve these tasks include *Mail Channels*. This is a cloud-based spam filtering tool that has features like reports, analytics, fraud detection, and much more. It is priced at $59.99 a month. *Xeams* is a tool that has been in the market since 2002 and hence has a lot of so-called perfect features. The features include email routing, reports, mass email manager, encryption, and fraud detection. This tool pledges to remove 99.99 % of spam emails. The pricing is *$20* a user every year. *TopSec Email Security* is famous both in the business and federal agencies. It has features like audit logs, email recovery, block lists, and much more. What's different about this tool is that the company provides training and consulting on various security measures. There is no set price for this and a quote can be achieved from the company directly.

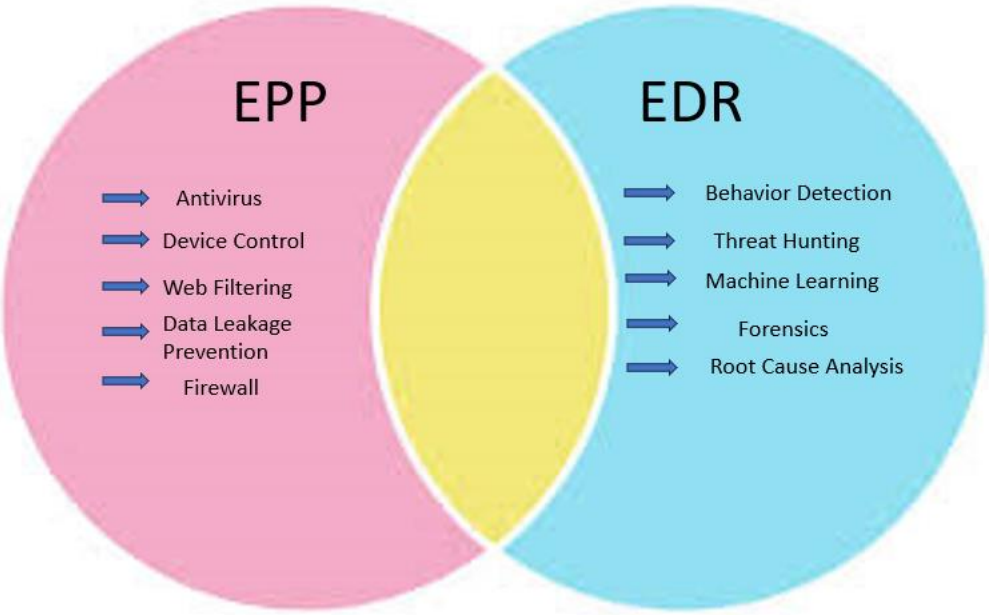
So, in conclusion to my first advice to a CISO, I would suggest selecting a comprehensive Email Security Posture. Implementing AI and Behavioral Analysis can be very beneficial. The use of DMARC (Domain-Based Message Authentication, Reporting, and Conformance) is extremely vital. Customize policies that can help to define set criteria and expectations based on the organization's needs.

EPP (Endpoint Protection Plan) and EDR (Endpoint Detection and Response) To protect our systems and organization from the Delivery phase we need to make sure our endpoint devices are also secured. EPP is a detailed solution that is deployed on endpoint devices to do so. These utilize cloud data for advanced monitoring and remote remediation. EPP was developed to identify threat actors that were able to bypass the usual endpoint security. In order to implement EPP in the most efficient way the CISO can implement the following steps. *Evaluating needs and selecting the right EPP*: Depending on the organization they can have contrasting threat landscapes. So, choosing the correct EPP that complements our organization is crucial. *Comprehensive Coverage:* The chosen EPP should have varied options for the type of threats it can handle. It must include malware, Threat analysis, Zero-day exploits, and others. *Centralized Management:* An EPP that has centralized management allows an organization for easy deployment and monitoring. *Behavioral Analysis:* This is very important since it can detect

atypical behavior and emerging threats. *Combining EPP with EDR.* It provides advanced protection and response capabilities. EDR can aid in suspicious activities in real time by analyzing data from network traffic and system logs. It is also used for Behavioral Analysis, Incident response and threat detection. Utilizing both EPP and EDR serves us in proper endpoint security.

Figure 9

Key Difference Between EPP and EDR

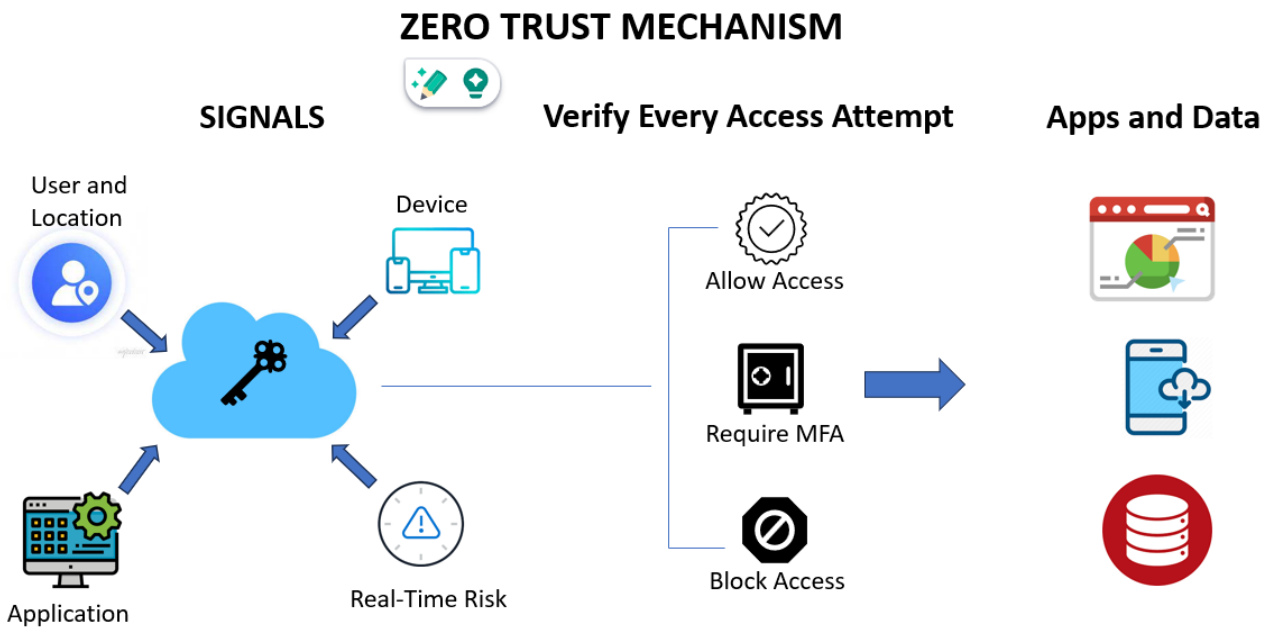


Zero Trust Model: The CISO should implement a Zero Trust Model if it's not already in place. This security model believes in the fact that trust can never be assumed, and authentication is always *preferred and required*. This approach has several benefits since the overall attack surface is significantly minimized. There is an enhanced security posture since no user is trusted by default. It improves *Network segmentation* since the network is divided into smaller fragments hence the roles and responsibilities are further segmented. This makes it difficult for the attacker to navigate through the network. Insider threats are reduced significantly since continuous monitoring is taking place, and any abnormal behavior is detected in real time. The Zero-trust model aligns with regulatory rules and compliance standards hence obtaining the legal industry-

specific rules. Furthermore, MFA (Multi-factor Authentication) and least privilege should be put into since this help mitigate several problems. MFA can have something you know like passwords, PINs, and security questions, something you have that is smart cards or tokens, something you are which includes biometrics, and something you do that is behavioral factors. Least privilege means giving access to end users that helps them to do their task but also at the same time not giving them too much access. This also helps in segmentation since people can be held responsible in a more convenient way.

Figure 10

Trustless approach or no-trust model



Reference

Bedell, C., Loshin, P., & Hanna, K. T. (2022, September 13). *What is a computer worm and how does it work?* Security. https://www.techtarget.com/searchsecurity/definition/worm

Bhadwal. (2023). *The history of cyber security: A detailed guide [infographic]*. KnowledgeHut. https://www.knowledgehut.com/blog/security/history-of-cyber-security

CrowdStrike. (2023, February 28). *What is an Advanced Persistent Threat?* https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

Forrester, N. (2021, September 11). *A brief history of cyber-threats - from 2000 to 2020*. SecurityBrief New Zealand. https://securitybrief.co.nz/story/a-brief-history-of-cyber-threats-from-2000-to-2020#:~:text=2000%2D2004%20%E2%80%94%20The%20Worm%20Era&text=First%2C%20there%20was%20the%20ILOVEYOU,to%20%2415%20billion%20in%20damages

GeeksforGeeks. (2022a, June 22). *History of cyber security*. GeeksforGeeks. https://www.geeksforgeeks.org/history-of-cyber-security/

Ibrahim, S., Herami, N. A., Naqbi, E. A., & Aldwairi, M. (2020a). Detection and analysis of drive-by downloads and malicious websites. *Communications in Computer and Information Science*, 72–86. https://doi.org/10.1007/978-981-15-4825-3_6

James, N. (2023, August 4). *81 phishing attack statistics 2023: The ultimate insight*. Astra Security Blog. https://www.getastra.com/blog/security-audit/phishing-attack-statistics/

Rosenbaum. (2021, September 8). *Microsoft has a $20 billion hacking plan*. CNBC. https://www.cnbc.com/2021/09/08/microsofts-20-billion-and-cybersecuritys-big-spending-problem.html

Rushton, J. (2023, July 3). *50+ phishing statistics you need to know – where, who & what is targeted*. Techopedia. https://www.techopedia.com/phishing-statistics#:~:text=Phishing%20Statistics%20Highlights&text=83%25%20of%20all%20companies%20experience,corporations%20%244.91%20million%2C%20on%20average

Sophos. (2021, February 2). *What the last 20 years of cyberthreats have taught us*. Channel Futures. https://www.channelfutures.com/from-the-industry/what-the-last-20-years-of-cyberthreats-have-taught-us

Tillson. (2023, June 12). *Evolution of the ciso role*. Cyber Defense Magazine. https://www.cyberdefensemagazine.com/evolution-of-the-ciso-role/

Wrightson. (2015). *Reconnaissance*. Azeria. (n.d.). https://azeria-labs.com/reconnaissance/

Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. *Communications in Computer and Information Science*, 438–452. https://doi.org/10.1007/978-3-319-22915-7_40