**I. Introduction**

This report will be detailing the MITRE ATT&CK Framework (MAF) tactics, and will point out which tactics and their relevant techniques were used in the Cynical Health cyberattack. The Cynical Health cyberattack allowed attackers to gain access to internal systems for a significant period of time, and used multiple angles of attack. Through investigating the attack, we can understand how attackers launch a targeted attack.

**II. MITRE ATT&CK Framework Overview**

The MAF is an evolution of the cyber kill chain, which mainly involves the upgrade of acknowledging that attackers rarely execute their attacks in linearly, orderly fashion – and rather execute each prong of attack whenever they can. The MAF’s purpose is to provide foundational cyber security knowledge to the world, and provide a comprehensive method of describing an cyber-attack.

**III. Mapping the Attack to the MITRE ATT&CK Framework**

Provide a detailed analysis of each tactic in the MITRE ATT&CK Framework

For each tactic, identify the techniques that the Cynical Health attackers used

Explain the purpose of each technique in the overall attack

Discuss any instances where a tactic was used multiple times or not at all

This section of the report will describe each MAF tactic in more detail, before explaining what techniques from the tactics were used in the Cynical Health attack. The techniques will be resourced from the attack.mitre.org website.

**Reconnaissance** is a vital part of an attack, where the attacker will collect information about the target through various means. Passive techniques will get information about the target without directly engaging with them, such as searching through their social media or looking them up on websites (public or closed sourced websites). Active techniques will directly engage with the target such as through scanning ports or phishing. This information gained will then be used to help execute attacks, and/or also to find and prioritize assets within the target.

Although reconnaissance techniques are not alluded to in the Cynical Health attack, there are likely several reconnaissance techniques used in this attack. The attacker likely used the techniques:

Gather Victim Host Information – to find the victim was running windows (although they could have had an executable for each operating system, or it could have been an assumption).

Gather Victim Identity Information – the adversary may have searched the victims social media to find the employees email/discover that they were new to the job so might provide an easier “in” to the network.

Gather Victim Network Information – the attacker may have searched accessible data sets, to gain information about the Cynical Health’s network.

Gather Victim Org Information – here the attacker would have found the value of the companies data which would be used to justify the attack.

Search Closed Sources, Open Technical Databases, Open Websites/Domains and victim owned websites will also likely have been some techniques that the attacker will have used to scope out the target.

**Resource Development** is a tactic where the adversary will acquire resources needed to facilitate an attack on a specific target. Physical resources such as computers, servers or memory drives will be acquired, as well as software resources, such as email accounts used to impersonate people, reverse shell programs, and other malicious software tools. Each attack will require different resources, as extracting data from a network (largely requiring software tools and social engineering) is a completely different attack compared to denial of service attacks (requiring a large amount of hardware).

Obtain Capabilities or Develop Capabilities – the attackers will have either obtained people with software skills to use tools such as ASPXSPY, or have developed the capabilities to use it themselves. As well, once they explore the network that they have infiltrated, they may have had to obtain either the code to exploit the Remote Code Execution, or have developed the capabilities to write it themselves (through reading other exploits, the exchange server documentation, etc.). they also obtained their C2 Server.

Stage Capabilities – this technique describes setting up a capability for later use. In the Cynical Health case, the adversaries would have set up the web resource for which the email containing the malicious code would have had a link to, to download the malware.

**Initial Access** is the first method that an attacker may use to gain access to, or foothold to the target network.

Phishing - The attackers used a phishing email with an attachment about employee benefits to deliver malware to the victim's personal laptop.

External Remote Services - The attackers used a known vulnerability in the on-premise Microsoft Exchange server to perform Remote Code Execution (RCE) and gain access to the server.

**Execution** is when the adversary is running the malicious code to either – explore a network, or steal some data.

User Execution – through sending the email with the attachment, the user inadvertently executed the malicious code in the attachment.

Command and Scripting interpreter – although it does not say how they executed the majority of the commands, It was likely done through a command shell, PowerShell or some other shell available on the windows network.

**Persistence** is when the attacker is trying to maintain their hold on the network, even through system restarts, password changes among other things.

**Privilege Escalation** is when the attacker is trying to achieve a higher level of security clearance from a lower level (e.g. getting root user access from a general user access).

Exploitation for Privilege Escalation – the attackers exploited a known software vulnerability in attempt to elevate privileges. In this case they used a known vulnerability in Microsoft Exchange Server, through performing Remote Code Execution which lead to an escalation

**Defence Evasion** is the adversary trying to avoid being detected. Through disabling security, encrypting malware or other similar techniques, the attacker can obfuscate their presense to avoid detection.

Rootkit – the attackers used Fire Chilli Rootkit, which is a program used to hide malicious programs or processes from the user, in order to remain undetected to continue attacks.

**Credential Access** the attacker is trying to steal usernames and passwords – through methods such as keylogging or credential dumping. Through getting access to systems through real credentials will be a lot harder to detect, as they will be access codes already validated by the systems, and if the adversary gets access to administrative credentials, they could have a worse impact on the system.

OS Credential dumping – the system stores a variety of credentials in the LSASS, from which the adversary’s tried to dump the memory in effort to dump the domain passwords (and succeeded). From here they are able to privilege escalation, data theft or lateral movement (in this case, they got administrative credentials, so was privilege escalation).

**Discovery** the attacker will move around and explore the network, in order to gain more information abou the environment, as well as be able to spot opportunities for potential attack points.

Software Discovery – the attackers will move around the system in search for vulnerable software which may lead to privilege escalation. In the cynical health attack, the adversarys used the software discovery technique to find out about the Microsoft exchange server with the remode code execution vulnerability. From there they coud use the vulnerability for privilege escalation.

Network Service Discovery – retrieve a listing of services running on hosts, in hopes of discovering software vulnerabilities. Cynical health attack saw that the adversaries completed multiple scans on a patched SQL instance.

**Lateral Movement** is when an attacker needs to move through the network to reach their objective. Quite often the point of access is not the final destination, and the attacker will have to pivot across multiple systems before reaching their target.

Exploitation of Remote Service – in this attack Powercat was used. Powercat is a useful tool to secure a reverse TCP connection, and can be used to establish a connection from a compromised machine to the attackerse machine. Powercat was found (amough other remote shell tools) on the exchange server, likely to establish the remote connection for the attacker.

Internal Spearfishing – sometimes additional information is required to gain access to further systems, and spearfishing while already inside the system is called internal spearfishing. In this instance, the attackers needed some credential information from the manager of a SQL database, to gain access to the data, and did so through this method.

**Collection** describes adversaries collecting information that will help them in achieving their final goal – usually before stealing the data.

Email Collection – where attackers will target emails specifically, as emails frequently have sensitive information in them. In this case the attackers collected data from the mailbox on the exchange server.

Data From information repositories – mining data specifically from information repositories. Here the attackers used collection tactic and pulled data from the SQL database information repository.

**Command and Control** has a few techniques that adversaries will likely use to communicate with systems that are under their control within the network.

Encrypted channel – attackers will employ an encryption algorithm to conceal their traffic from the user or anti-malware. In this example, the attackers encrypted the SQL data before sending it to their C2 server.

**Exfiltration** is when the attackers are in the act of stealing the data.

Data Transfer Size Limits - The attackers in Cynical Health both split and compressed the data to likely minimize the amount of extra traffic that was going on in the system.

**Impact** is the attacker is trying to manipulate, destroy or otherwise alter the normal data flow in the system. In this attack there was no impact on the data, as the attackers were likely trying to remain undetected, so did not want to leave any trace of their presence

**IV. Conclusion**

The report discusses the use of the MITRE ATT&CK Framework (MAF) to investigate the Cynical Health cyberattack, which allowed attackers to gain unauthorized access to the internal systems for a significant period of time. The report provides a detailed analysis of each tactic in the MAF, identifies the techniques used by the attackers, explains the purpose of each technique in the overall attack, and discusses any instances where a tactic was used multiple times or not at all. The report also explains that the MAF is an evolution of the cyber kill chain and provides a comprehensive method of describing a cyber attack.

To improve cybersecurity, organizations should adopt a layered defence approach with multiple security controls. Regular vulnerability assessments can help identify and address critical weaknesses. Organizations should also develop a security awareness training program to minimize the risk of human error and strengthen the overall security posture.