Edmund Reisser

CS462

Susan Zehra

April 15, 2024

CS462 Term Project

In a world dominated by the use of technology and the internet, it is a wonder how any individual can avoid being online. Businesses use the internet to advertise their products and services, while individuals use the internet to order packages, stay up to date with current events, message and communicate with family and friends, and even more recently have moved to taking their primary, secondary, and higher education classes online. With all of the advancements in technology, there does inevitably come risks with all of these rewards. There are sadly those who would see the advancements in technology as a way to execute and commit crimes on a larger scale online, these individuals are known as Cyber Adversaries. These Cyber Adversaries use many different means to achieve their goal of stealing data online such as through the use of ransomware, vulnerabilities, and phishing attempts to name a few. For the purpose of this blog, we will be going over a recent cyber attack through the use of ransomware and SQL injection vulnerability on the MOVEit Transfer databases.

Before we can dive into the attack itself, we must first understand and clarify any confusion on what these different definitions mean. So what is a Cyber Attack, and what types are there?

A cyber attack, as defined by Cisco, is a “malicious and deliberate attempt by an individual or organization to breach the information system of another individual or

organization" (*CISCO*). The unfortunate reality is that any individual who utilizes the internet is susceptible to these types of attacks.

Ransomware, as defined by the FBI, is a "type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return" (*Ransomware*). Ransomware is a type of malware that can be downloaded through websites, files, and even images in some cases. The best way to avoid these are to be careful on what websites you visit, what files you download, and to keep your systems and anti virus software up to date.

A Zero-Day vulnerability as defined by CSO, is a "security flaw for which the vendor of the flawed system has yet to make a patch available to affected users" (*Zero Days explained*). These vulnerabilities were released alongside the MOVEit software at the day of launch and have gone unnoticed for the lifetime of the software until now. These vulnerabilities are worrisome for companies as after these types of vulnerabilities are discovered, the targeted companies have only a little bit of time to minimize the scale of the attack before their systems are compromised beyond salvage. That is to say if these companies have any idea that they have been attacked at all, depending on the demands from the hackers, or if these malicious actors want to create a way to compromise and steal more data in the future.

Now that the definitions have been clarified, we can delve into the main topic for this blog, the MOVEit Ransomware attack that happened between the months of May and June of 2023. According to CISA (the Cybersecurity & Infrastructure Security Agency) a group named CL0P, also known as TA505, found a vulnerability inside of the file transfer system known as the MOVEit Transfer solution (MTF) and this group exploited the discovered vulnerability with a SQL injection (*CISA*). A SQL injection attack is a type of code insertion of the SQL query

through the input data from a user to the application. With a successful injection of this code, OWASP (The Open Worldwide Application Security Project) states that “can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system” (*SQL Injection*). With this unfettered access to systems that these individuals should not have access to, these malicious actors could theoretically steal all of the companies data, copy it, delete it, or anything else they could come up with in order to either make money or even take down these companies if they so wished. The downside of the discovered vulnerability is that the SQL injection can range in degrees of severity depending on the skill of the group who is exploiting it. So a malicious actor with only a basic knowledge of the skills required to hack could only do minimal damage, while a seasoned hacker could use this to have a huge and severe impact on the companies involved. On the other hand, the positive aspect is that the vulnerability only affects the platforms that require the interaction with a type of SQL database. According to OWASP, the SQL Injection is one of the more common issues with websites. It is an easily detectable flaw, which also means that it can be an easily exploited flaw (*SQL Injection*).

Getting back to the subject at hand, the group known as CL0P was found to have breached a number of federal agencies and while it was not a vast penetration of, as the Washington Post describes it “Cabinet-level departments”, the data that was stolen may be used to orchestrate future attacks against these same agencies (*Washington Post*). The attack itself was considered to be a SQL injection of a zero-day vulnerability, now known as CVE-2023-34362. NIST (the National Vulnerability Database) categorizes this vulnerability as 9.8 score on a 10 score base and classifies it as of a Critical Severity. The description given for this attack by NIST

is that the vulnerability could allow for an individual who does not have authorized access to be able to gain access to the MOVEit Transfer database through engines such as MySQL, Microsoft SQL Server, or even Azure SQL (*NIST*).

LEMURLOOT was the method of attack by CL0P, as they used this vulnerability to install this web shell. According to CISA, the web shell imports different libraries of information, including those such as "MOVEit.DMZ.ClassLib," "MOVEit.DMZ.Application.Files," and "MOVEit.DMZ.Application.Users". By doing so, CL0P was able to interact with the MOVEit software and create randomly generated 36 character passwords so that the group could access and authenticate themselves on the company servers (*CISA*). This attack works by interacting with the request for HTTP containing a "header field named X-siLock-Comment, which must have a value assigned equal to the password established upon the installation of the web shell" (*CISA*). By doing so, the group can create administrative accounts that look legitimate while also having the ability to delete accounts they may want to appear to look like.

The MOVEit file transfer program is sold by Progress Software, and according to their website is used by the 30 largest companies in the world, 70% of the Fortune 500 use their services, and has an active developer community of three and a half million plus individuals (*MOVEit*). The company's mission is to provide a way for other companies to handle sensitive data and to be able to encrypt and send them to individuals or groups depending on the needs of the company. The effects of the attack can stretch and grow according to the actions taken by the afflicted companies. According to the Washington Post, Progress had apparently identified the vulnerability and released a software patch in late May (*Washington Post*). However, just because the company had released this patch, does not mean that the companies who were

attacked had downloaded the patch and rectified the problem. A few of the organizations that fell victim to this SQL injection attack include the U.S. Department of Energy, Shell, The British Broadcasting Corp, British Airways, and even states such as Louisiana and Oregon (*Washington Post*).

The goal of this attack was to ransome the data that CL0P had secured through the exploitation of this vulnerability and in the event that the group did not receive payment from the victims in a set amount of time, the group would release or sell the data that they had stolen online. The unfortunate reality of the situation is that even if the company that is victimized ends up paying the ransom, there is no guarantee that the individuals who stole the data and information will even delete the data from their systems or even decrypt the data themselves. All the company has is the hope that the hacking group will hold true to their word. According to the FBI, "The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity" (*Ransomware*).

This attack is the unfortunate reality that follows the world we, as citizens of the world wide web, have to deal with and live in. There are always risks when it comes to doing anything online, and this attack could not only happen to these major companies, but it could also happen to anyone at any time. While it is a shame that the attack can happen, the companies afflicted cannot be held to blame as there is no such thing as a perfect defense against cyber attacks. The best way to deal with and prevent future attacks is to keep up to date with information and training that deals with Cyber Security, this way the more an individual knows about safe habits online, minimizes their risk of attack.

References -

Cisco. (2024, February 21). What is a cyberattack? - most common types. Cisco. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~how-cyber-attacks-work

MOVEit Secure Managed File Transfer Software: Progress. Progress.com. (n.d.-a). https://www.progress.com/moveit

NIST. (n.d.). CVE-2023-34362 Detail. NVD. https://nvd.nist.gov/vuln/detail/CVE-2023-34362

Ransomware. (n.d.). https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/ransomware

SQL Injection. SQL Injection | OWASP Foundation. (n.d.). https://owasp.org/www-community/attacks/SQL_Injection

What to know about the moveit ransomware attack that hit U.S. agencies - The Washington Post. (n.d.-b). https://www.washingtonpost.com/technology/2023/06/16/moveit-ransomware-attack/

Zero Days explained: How unknown vulnerabilities become gateways for attackers. CSO Online. (2021, April 12). https://www.csoonline.com/article/565704/zero-days-explained-how-unknown-vulnerabilities-become-gateways-for-attackers.html

#STOPRANSOMWARE: Cl0p ransomware gang exploits CVE-2023-34362 moveit vulnerability: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, February 29). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a