CS462 Term Project: Report on MOVEit Cyber-attack

Michael Dawson

Old Dominion University

Susan Zehra

Introduction

As the world continues to spin, technology is advancing every day. Cybersecurity attacks have been around for quite a while now, but we have had time to learn about all the kinds of different attacks and vulnerabilities and have been able to protect against certain types of attacks and vulnerabilities. As hackers find new ways to do things, new vulnerabilities and zero-day exploits are found quite often, it is important to keep our systems as secure as possible from potential cybersecurity attacks. It is also important to have cybersecurity awareness and to promote it, one of the number one types of attacks is social engineering where people get manipulated. There are billions of different cybersecurity attacks that get carried out around the globe each year. In this in this paper I will be giving a detailed report on a single cybersecurity attack that occurred recently, that attack being the MOVEit Cyberattack that occurred in May of 2023.

Overview

MOVEit is a file transfer app, created by progress software. It is used by thousands of different organizations around the world, primarily by businesses and government agencies that need to share confidential or sensitive information. (Hayes, 2023). The app is designed to replace standard methods of file transferring, which can be vulnerable to simple cyberattacks. According to the Phillip Robinson the attackers that claimed to be responsible is a ransomware group called Cl0p, they are known for extorting people for money. (Robinson, 2024). The ransomware group was able to obtain sensitive data from government and public organizations around the world, then threatening to publicly release the solen data from their victims unless they pay a sum of money for them to delete it. (Robinson, 2024). The attackers were able to pull off this attack by

exploiting a zero-day vulnerability that they found in the app, allowing the attackers to launch SQL Injection attacks and access the database of MOVEit's customers. (Robinson, 2024).

The Attack

The MOVEit cybersecurity attack was first announced in May of 2023, when it was revealed that attackers had exploited a vulnerability in the MOVEit file transfer app. Progress Software, the vendor that owns MOVEit had released a security update to fix the vulnerability quickly, but by the time they did thousands of company's data had already been stolen. (Robinson, 2024.) The vulnerability was revealed to allow the attackers launch SQL Injections to access all MOVEit's database letting them download and navigate any files. Pieter Arntz of Malwarebytes claims "The method used to compromise systems is to drop a webshell in the wwwroot folder of the MOVEit install directory" (Najarro, 2024). This gave the attackers access to be able to create an administrative backdoor which gave them an active session to be able to bypass credentials and start to harvest data.

SQL Injection is one of the common attacks known used by cyber criminals around the world. When it comes to database security, SQL Injection is the biggest threat. (Thompson, 2024). According do Katrina Thompson, "This attack is performed by entering a query into a SQL form, and if the database interprets the result as "true" it enables access to the database" (Thompson, 2024). In the case of the MOVEit cybersecurity attack, the vulnerability allowed the attackers to access and collect sensitive information and files from organizations using the MOVEit file transfer app.

Once the attackers had successfully exploited the vulnerability, they were able to exfiltrate a large amount of data. In this attack, the attackers harvested data from different

organizations and cherry picked the biggest ones they could get the most money from. According to Phillip Robinson “Some of the victims of the attack include the BBC, British Airways, Boots and Aer Lingus, whose staff data, including national insurance numbers and bank details, may have been stolen” (Robinson, 2024).

Step by Step

The first step of the attack was the exploitation of a zero-day vulnerability. The hackers used SQL Injections in the MOVEit file transfer app to gain access to the database. The vulnerability allowed the attackers to bypass security controls and execute malicious SQL commands to extract data stored in the database.

The second step of the attack was the harvesting of data. After gaining access to the database by dropping a webshell in the root folder, the attackers harvested all the sensitive data to then move on to the third step and extort the companies for money.

The third and last step of the attack was to deploy the ransom. In the case of this attack the ransomware group Cl0p stole the sensitive data from different organizations and contacted them directly telling them to pay them money and they will delete all their data. The group targeted the biggest companies to try to get the most money. According to Phillip Robinson, “No encryption ransomware has been observed, and the attackers have said they will erase the data they stole from government websites. This is likely an attempt to avoid drawing unwanted attention” (Robinson, 2024).

After carrying out their goal successfully, the ransomware group known as Cl0p was able to steal sensitive data from thousands of organizations around the world and extort their victims by threatening to release their sensitive data unless they pay a sum. (Robinson, 2024). Which

lead to one of the biggest cyberattacks of the year, showing the importance of cybersecurity and the potential threats that are imminent.

What can be done?

When dealing by cyber-attacks there are a few things that can be done to guard again them. For example, the HTTP/HTTPs protocols are used when attackers exfiltrate data. Kenny Najarro states, “One of the quickest and most surefire ways to prevent further exfiltration is to deny access by shutting off both inbound and outbound HTTP and HTTPs data traffic” (Najarro, 2024). In the case of this attack, that is the first thing they should have been done is after they found out data was, they systems had been compromised.

Another thing that can be done to safeguard against cyber-attacks is to do regular updates and patches, as new vulnerabilities are found new fixes are also put in place, which is why it is important to keep your systems up to date with the most recent updates and patches whereas your systems could be vulnerable to a new vulnerability if not done so.

Impact on Society

Every cybersecurity attack has some kind of impact on society whether it be a big or small attack. This specific attack has multiple impacts on today’s society. The first impact is an economic impact. The economic damage caused by the attack on the MOVEit file transfer app was probably substantial. Some of bigger organizations that were affected probably faced costs for things like incident response, legal fees, and a list of other things.

Another impact this attack had on today’s society is a loss of trust. Lots of organizations that were affected by the attack will probably not trust MOVEit anymore and may ultimately stop using their services. Not only did the attack damage MOVEit’s reputation but also the

reputation of the organizations that were affected as some of their customers may have lost trust in them for trusting MOVEit.

One more impact the attack had on today's society is some legal impacts. Organizations that were affected by the attack could face legal action from people who fell victim as a result. For example, healthcare organizations that were affected by the attack and are protected under HIPAA regulations whose patient's sensitive data was leaked.

Conclusion

The cybersecurity attack carried out against Progress Software's MOVEit file transfer app servers as a strong reminder of the risks associated with database security and the need for strong cybersecurity practices, especially when handling confidential and sensitive data. While the MOVEit app was designed to provide secure file transfers, it was quite the opposite. The exploit of the Zero-day SQL Injection vulnerability shows the danger of this kind of exploit. The attack carried out by Cl0p had many significant impacts on today's society from economical concerns to legal concerns and more. This cyber-attack also highlights the critical importance of being able to keep data and systems secure. Organizations must provide security awareness and educate their employees, so they don't fall victim to attacks such as social engineering or phishing emails. Only through a thorough layered approach of cybersecurity can risks be partially mitigated, nothing is 100% secure, kind of like I said earlier, as technology advances, people are finding new ways to exploit things and finding new vulnerabilities. At the end of the day, it is up to the cybersecurity experts to make risk-based decisions on whether or a vulnerability should be mitigated or not.

References

Hayes, M. (2023) *What you need to know about the MOVEIT data breach*. Experian. https://www.experian.com/blogs/ask-experian/moveit-data-breach/

Katrina Thompson (2024) *Major database security threats and how to prevent them*. Tripwire. https://www.tripwire.com/state-of-security/major-database-security-threats-prevent#:~:text=SQL%20injection%20is%20the%20most,enables%20access%20to%20the%20database.

Najarro, K. (2024) *Moveit Hack: The ransomware attacks explained*. Kolide. https://www.kolide.com/blog/moveit-hack-the-ransomware-attacks-explained

Robinson, P. (2024). *The MOVEIT attack explained*. Lepide Blog: A Guide to IT Security, Compliance and IT Operations. https://www.lepide.com/blog/the-moveit-attack-explained/