Analyzing Adversory Attack on MOVEit File Transfer Appliaction

1st Aditi Venkatesh
Cybersecurity and Threat Intelligence
University of Guelph
Guelph, Canada
avenkate@uoguelph.ca

2nd Shreya Bhoje
Cybersecurity and Threat Intelligence
University of Guelph
Guelph, Canada
sbhoje@uoguelph.ca

3rd Fatemeh Khoda Parast
Faculty of Computer Science
University of Guelph
Guelph, Canada
khodapaf@uoguelph.ca

***Abstract*—In this research project we focus on how the TA505 APT group, also known as Cl0p ransomware group, exploited Vulnerability CVE-2023-34362 in the file transfer server application MOVEit. We aim to delve into TA505's past campaigns, particularly those targeting similar applications, in order to gain insights into their tactics. We chose this subject to gain a deeper understanding of how adversaries leverage specific vulnerabilities in widely utilized applications like file transfer platforms. Our analysis will focus on how TA505 weaponized the MOVEit vulnerability for large-scale exploitation. Given the widespread use of file transfer applications (FTA) for both internal and external file exchanges within organizations, this research holds significant relevance. Renowned organizations such as John Hopkins University and Tesco Bank were two of the many victimized by the attack. It is noteworthy that TA505 has previously capitalized on vulnerabilities in GoAnywhere MFT and Accellion FTA, among other file transfer application. The outcomes of this research will empower organizations to proactively identify and mitigate potential threats, fortifying their defenses against such attacks.**

***Index Terms*—TA505, Cl0p, CVE-2023-3436, SQL Injection, Zero-day Vulnerability, Lemurloot Webshell, Data Breach, Ransomware**

I. Introduction

MOVEit Transfer is a secure file transfer software application for businesses and enterprises that need to transfer sensitive files such as financial or medical records produced by Ipswitch, Inc. (now part of Progress Software) [1]. The application was previously known as MOVEit DMZ or MOVEit File Transfer and has over the years, evolved to cater to the changing needs of organizations.Due to the application's capability of transferring files in different languages such as French, German, Spanish, Japanese and Chinese irrespective of end user's location, many significant firms in the banking, healthcare, and government sectors started adopting the MOVEit File move Application to store their data [2]. Following this attack, Progress discovered a vulnerability in MOVEit Transfer that might have allowed for unauthorized access to the environment and the elevation of privileges [32][50]. On May 28, 2023, the MOVEit technical support team received call reporting about activity. Immediately after discovering and reporting the vulnerability, the engineering team flushed HTTP and HTTP traffic to MOVEit Cloud and notified MOVEit Transfer customers to do the same in their environments, while the team was developing appropriate fixes for MOVEit Cloud, as well as currently supported on-premises versions of MOVEit Transfer [3]. The attacker exploited the previously undiscovered zero-day vulneraility in MOVEit Transfer application [5]. The security vulnerability stemmed from SQL injection, a well-known technique for infiltrating applications by exploiting weaknesses in software code. These vulnerabilities open avenues for manipulating data and gaining unauthorized access to databases [20]. In the MOVEit breach, the attackers transitioned from initial manual testing the SQL injection flaw to executing automated exploits across a wide range of organizations [6].

The long list of those affected by the attacks continues to grow rapidly as MOVEit has been coordinates into the backend of numerous consumer-facing frameworks. The harm caused by this incident was passed on to the people rather than the companies accountable for securing their information.CalPERS (California Open Representatives Retirement Framework) infringement are one of the occurrences where, 4,444 CalPERS and its 769,000 influenced people were included within the MOVEit incident since their merchant, PBI Investigate Administrations, were attacked [49]. The compromised data consisted like date of birth, title and Social Security because file transfer tools which manage and share large volumes of sensitive data making them excellent targets for cybercriminals [4].

In this paper, we describe some aspects of the attack such as the how the attack progressed by mapping attack stages to the stages in the Lockheed Martin Cyber Kill Chain and techniques used by the APT group throughout the attack by mapping them to the techniques in MITRE ATTACK Framework, and the reasons for the steady increase in the number of compromised systems. The Background section gives additional information of terms and ideas related to MOVEit and the related information breach. The TA505 APT group's attack strategy against the MOVEit Transfer application is described in the Attack Methodology section. The Impact section points towards how did the attack affected organizations in different sectors. The Solutions section portrays mitigation and prevention techniques to be followed after the MOVEit attack. At last, the conclusion summarizes the incident and how the

organizations should approach these type of attacks.

II. Background

The MOVEit exploit is an example of financially motivated cyberattack. Such cyberattacks often involve use of ransomware to steal the sensitive data and make profit from the extortion [7]. The entire MOVEit attack timeline is summarised in Figure 1. There are many threat actor groups who have adopted this business model. The TA505 APT group, one of the ransomware-as-a service begrime groups, confirmed to be the one behind the MOVEit mass exploitation and that they will publish the stolen data if the victims refrain from paying the ransom [6]. The group stole the data leveraging the zero-day vulnerability in MOVEit Transfer leading to mass exploitation. Similar campaigns have been carried out by the ransomware gang, taking advantage of zero-day vulnerabilities found in file transfer applications such as Accellion in 2020 and 2021 and GoAnywhere MFT servers in early 2023. [8].

A. About the attacker: TA505, the Cl0p ransomware gang

Financially driven, TA505 is a cybercrime group that certainly speaks Russian. In addition to providing ransomware as a service, the gang has been aggressively disseminating several remote access trojans. The ransomware gang has been operating since 2014 and is well-known for its constantly changing use of malware and tactics, widespread malware distribution, and ransomware campaigns worldwide [9].

TA505 APT group heavily relies on malicious software to carry out fraudulent activities and now has evolved to be a sophisticated threat actor innovating its ways to gain access to the victim's system and environment for monetization [10]. There are countless malwares in Cl0p's toolkit that enables the group to maintain persistence in the victim's environment. The most famous from those malwares can be listed as follows:

1. FlawedAmmyy/FlawedGrace: It is a remote access trojan aiming collection of data and communication with the Command and Control (C2) enabling it to listen to the commands and perform exfiltration or to download more malware components [13][15].

2. SDBot:It's a remote access trojan that's utilized as a backdoor to communicate with the Command and control. It can find its way to expolit vulnerabilites and drop a copy of itself in removable disks and network share to further infect the network laterally. The RAT has ability to hide its existence using and be persistant [13][14].

3. Truebot: It is a third party malware used by TA505 as a initial stage downloader module to collect information about the victim. Once the persistance is established, Truebot is used to download malware compoments and load shell code or DLLs. The malware has ability to run them and delete itself making it hard to identify its existance [8][13].

4. DEWMODE: This is a custom webshell to interact with the underlying SQL database and access and exfiltrate data. The PHP webshell was used to in campaign against Accellion FTA devices to steal sensitive data [12][16].

May 28	Earliest evidence of exploitation occurred resulting in deployment of web shells and data theft
May 31	A zero-day vulnerability was reported in MOVEit Transfer and MOVEit Cloud by Progress
June 4	Microsoft attributed the attack with Lace Tempest, an associate of the Cl0p ransomware gang
June 5	TA505, the Cl0p ransomware gang claimed to be behind the attack
June 9	Progress software updated the advisory to include a patch after the investigation done by cybersecurity firm Huntress
June 15	Progress discovers a new vulnerability, CVE-2023-35708
July 11	The Cl0p gang issued threat to pay the ransom threatening the data to be made public
August 25	The MOVEit cyberattack affected 951 organizations and between 48.8 and 53.7 million people
November 10	UpToDate the number of victims of the MOVEit cyberattack is 2381 organizations and 67.5 and 72.4 million individual

Fig. 1. MOVEit Transfer Exploit timeline (2023) Source: Primary

5. LEMURLOOT: This is another custom webshell written in C hash and used in campaign against the MOVEit Transfer platform. The web shell may execute commands to download files from the MOVEit Transfer system, extract its Azure system settings, access comprehensive record information, create, insert, or delete a specific user, and authenticate incoming http requests using a hard-coded password [8][13].

B. Peeking into the past: Campaigns againsts Accellion FTA and GoAnywhere MFT

TA505 has had pulled off data breach campaigns against the file transfer application such as Accellion FTA and GoAnywhere MFT suggesting that the MOVEit data breach was not first of its kind.

1. Accellion Data Breach: Accellion FTA is a well-known American company offering file transfer and sharing services. The FTA has a wide range of customers from private financial and healthcare organizations to government agencies [11]. The zero-day vulnerability in the application was brought to light in December 2020. There have been four zero-day vulnerabilities discovered which were leveraged by the TA505 group, namely, CVE-2021-27101 - SQL injection via a crafted Host header, CVE-2021-27102 - OS command execution via a local web service call, CVE-2021-27103 - SSRF via a crafted POST request, CVE-2021-27104 - OS command execution via a crafted POST request [16]. The SQL injection vulnerability (CVE-2021-27101) was exploited to execute remote instructions on vulnerable devices by unauthorized user and install DEWMODE webshell enabling the attacker to steal the data from the compromised systems [12].

2. GoAnywhere Data Breach: GoAnywhere MFT is another file transfer and sharing platform used by large number of

organizations. Followed by the suspicious activity observed in January 2023, Fortra disclosed the data breach in February 2023. An unpatched vulnerability The TA505 group took advantage of the Remote Code Execution (REC) vulnerability, CVE-2023-0669. The vulnerability is a deserialization flaw that can be taken advantage of by making a post request to the endpoint at "/goanywhere/lic/accept." Additionally, the hacking tool Metasploit already has a plugin that makes exploitation considerably simpler[17].

Both the above exploits show the TA505's interest in targeting a service rather than any specific organization or sector suggesting that the financial gain is the motivation behind conducting mass exploitation. MOVEit Transfer data breach is similar financially-driven attack executed by exploiting the zero-day vulnerability.

C. Ransomware

Ransomware, a type of malicious software, is intended to prevent access to a system or its data until the attacker receives a certain ransom payment. [23]. Ransomware is typically categorized into two types based on its approach: cryptographic ransomware, which encrypts the files of the victim, and locker ransomware, which blocks victims from accessing their systems [24]. The progression of ransomware is not driven by technological advancements but rather by the emergence of a novel business model known as Ransomware as a Service (RaaS). Ransomware as a Service (RaaS) is a collaboration between a developer responsible for creating and managing tools for extortion operations and an affiliate tasked with deploying the actual ransomware payload. Both parties stand to benefit monetarily in the event that the affiliate's ransomware and extortion scheme is successful. [25]

D. Zero-Day Vulnerability Attack

A zero-day vulnerability is a newly found flaw for which there is no security patch and which is unknown to the impacted vendor. Given the possibility of zero-day exploits, it is imperative that a vendor releases a patch as soon as they become aware of a zero-day vulnerability. A zero-day vulnerability's exploitability risk, however, rises if it is made public because attackers are likely to use it to target weak systems. Stated differently, there is an increased risk of zero-day exploits when patches for zero-day vulnerabilities are delayed [18][19]. Zero attacks come into picture when the zero-day vulnerabilities are exploited. Even with measures like system patching, upgrades, antivirus software, and intrusion detection systems that can address various types of attacks, the challenge arises with zero-day attacks, as their nature remains unknown, making them difficult to counter [22].

E. SQL Injection

SQL injection attacks include manipulating the execution of predefined SQL commands by inserting SQL commands into input data. [20]. SQL injection has the potential to allow a malicious actor to circumvent authentication mechanisms and gain full control over the database on the remote server. The attacks exists in two main forms:

(1) Direct method: One method involves directly inserting the code into user-input variables that have been made to run by concatenating it with the SQL command. The use of this approach is demonstrated in the example above. The reason for its name, "direct injection attack method," is that it is directly linked to SQL statements.[21]

(2)Indirect method: The second type of attack is indirect; it involves inserting malicious code into strings that are saved as original documents or in tables. A dynamic SQL command linked to the stored string is used to run some malicious SQL code. To initiate the injection process, the text string is terminated beforehand, and a new command is then appended [21].

F. Webshell

Webshells are segments of code crafted in various scripting languages, and they are uploaded onto web servers following the exploitation of injection vulnerabilities. These tools furnish hackers with a web interface, enabling them to remotely execute commands, manipulate sensitive data, and infiltrate web servers [26]. Webshells, for the purpose of identification, can be classified into two main categories: Non-encrypted and Encrypted webshells. In Non-encrypted Webshells, the source code is stored in straightforward, easily understandable text. The functions utilized within it are evident from the source code files [27]. On the other hand, Encrypted Webshells belong to a category where the source code often consists of obfuscated and non-meaningful characters. Despite this, the webshell successfully performs its functions. Commonly employed encryption functions are crucial in this category [27]. Attackers might implant web shells on web servers as a means to establish enduring access to systems [28].

III. Attack Methodology

The MOVEit Transfer exploit was a sophisticated and well-staged zero-day vulnerability attack. The TA505 group performed mass exploitation with discovery of only one zero-day vulnerability, CVE-2023-35708, in the file transfer application. Researchers from Kroll Threat Intelligence, after conducting investigation discovered proof indicating that individuals associated with Cl0P were testing methods to take advantage of the MOVEit Transfer vulnerability as early as July 2021 [29]. The apt group was successful in exploiting the vulnerability in MOVEit application back in 2021, but opted to carry out the assaults in parallel rather than sequentially, causing the MOVEit exploit attack to come after the attack on the GoAnywhere application [30].

A. CVE-2023-34362

This is a SQL Injection vulnerability found in the Progress MOVEit Transfer application version before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1) [31]. The zero-day vulnerability was reported by Progress on May 31, 2023 [32]. Based on the

database engine used—MySQL, MS SQL Server, Azure SQL, etc.—an attacker might be able to infer details about the composition and organization of the database. This might make it possible for them to run SQL commands that add, remove, or alter database elements [33].

B. CVE-2023-35036 and CVE-2023-35708

These are two more SQL injection vulnerabilities discovered by Progress after the attack on MOVEit was reported [32]. An unauthenticated attacker may be able to gain unauthorized access to the MOVEit Transfer database because of these vulnerabilities. An attacker could alter and reveal the contents of the MOVEit database by sending a carefully constructed payload to a particular MOVEit Transfer application endpoint [34][35].

C. The Attack

To understand the MOVEit expolit we refer to Lockheed Martin developed Cyber Kill Chain and MITRE ATTACK Framework. The Cyber Kill Chain outlines the steps of a cyber attack, identifies weaknesses, and assists security teams in preventing and mitigating attacks at each stage of the process [36]. Using MITRE ATTACK Framework enables the secuirty analysts identify the objectives of the adversary and the techniques and procedures used by them to fulfill the objective.

The cyber kill chain describes seven stages that a attack goes through. While not all attacks will have all seven stages in its lifecycle, we have tried to map the attack with the cyber kill chain. For all the stages in cyber kill chain we have mapped the attackers steps to the MITRE ATTACK framework techniques.

(1) Reconnaissance:

In order to exploit the zero-day vulnerability in the MOVEit application, the TA505 APT group gathered information on the vulnerable systems. The attackers identify potential targets by scanning for Windows servers running a weakened version of the file transfer program MOVEit. To find exposed systems, they may have utilized internet indexing services like Shodan, a search engine actively scans the entire internet to locate and catalog connected devices. or port scanning techniques [37][39]. Fig. 2 shows the number of potentially vulnerable systems with the MOVEit Transfer zero-day vulnerability found using Shodan [39].

MITRE ATTACK Framework mapping:

Tactic: Reconnaissance — *Technique:* Gathering victim network information [T1590]

(2) Weaponization:

The CL0P ransomware group developed a weapon, in this case, the weapon was specifically designed to target vulnerabilities in MOVEit Transfer [12]. Lemurloot is the newly developed webshell that was uses filenames that mimic legitimate components like human.aspx from MOVEit Transfer software. The investigations detected numerous POST requests to the valid guestaccess.aspx file prior to engagement with the LEMURLOOT web shell, suggesting a focus on SQL injection attacks against that particular file [38].

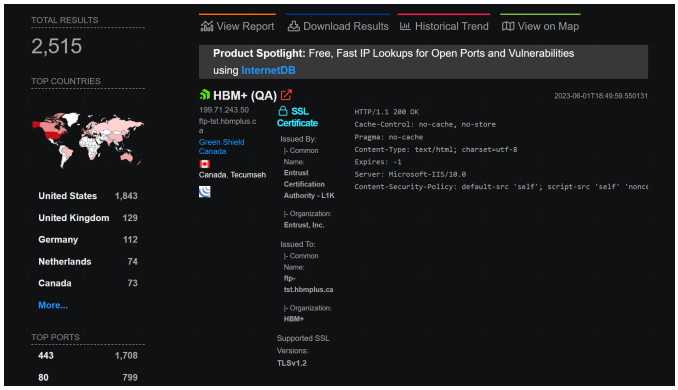

Fig. 2. Potential Vulnerable hosts found on Shodan Source: Adapted from [39]

MITRE ATTACK Framework mapping:

Tactic: Initial Access —*Technique:* Exploit Public-Facing Application [T1190]

Tactic: Defense Evasion —*Technique:* Masquerading [T1036]

(3) Delivery:

The delivery phase involved the actual deployment of the weapon. In this case, the attackers exploited the Installing the LEMURLOOT web shell on MOVEit Transfer web applications is vulnerable to the CVE-2023-34362 vulnerability [12]. The attackers uploaded any file to the server's directory using the moveitsvc service account by taking advantage of the SQL injection vulnerability [37].

MITRE ATTACK Framework mapping:

Tactic: Command and Control — *Technique:* Ingress Tool Transfer [T1105]

(4) Exploitation:

The attackers successfully exploited the SQL injection vulnerability to execute commands and install the LEMURLOOT web shell on the targeted system, gaining unauthorized access and control [12]. At this point, the system's svchost.exe process starts the IIS worker process w3wp.exe, which writes a number of files, including a C hash payload saved as human2.aspx, to a new working directory in Temp [37].

MITRE ATTACK Framework mapping:

Tactic: Execution —*Technique:* Execution through API [T1202]

Tactic: Collection — *Technique:* Data from Local System [T1005]

Tactic: Discovery — *Technique:* System Information Discovery [T1082]

(5) Installation:

The LEMURLOOT webshell was later installed on the compromised systems. The installation of the webshell served the purpose of maintaining persistance by evading being detected, data collection and perform data exfiltration [12]. The svchost.exe process of the system initiates the w3wp.exe (IIS worker process), which, in turn, creates multiple files in a fresh working directory within the Temp folder. These files include a C hash payload stored as human2.aspx [37].

Both this working directory and the files that come after it have the same pseudo-random naming scheme, consisting of eight characters. In an investigation the IIS log files from a affected system were analyzed to find that the moveitisapi.dll is employed to execute SQL injection upon receiving specific headers, while guestaccess.aspx is utilized to establish a session, extract CSRF tokens, and gather other field values to facilitate subsequent actions [39].

MITRE ATTACK Framework Mapping:

Tactic: Persistence — *Technique:* Scheduled Task [T1053]

Tactic: Collection — *Technique:* Data from Local System [T1005]

Tactic: Discovery — *Technique:* System Information Discovery [T1082]

Tactic: Defense Evasion — *Technique:* Obfuscated Files or Information [T1027]

(6) Command and Control (C2):

The payload (webshell), gathers details about the configuration of the database, enabling the attacker to establish connections to designated SQL databases. The web shell established communication channels with the attackers, allowing them to control the compromised system and issue commands [37]. Upon installation, the webshell generates a fixed random password for user authentication established by the X-siLock-Comment HTTP header. After successfully authenticating the password, the ASPX file establishes a link to the database and adjusts its functionalities based on the content of the X-siLock-Step1 header:

a)If X-siLock-Step1 is set to -2, it utilizes a SQL command to delete a user account named "Health Check Service" from the database [40].

b)When X-siLock-Step1 is -1, the file discloses Azure information via the response header and delivers a GZIP stream containing comprehensive details such as files, file owners, file sizes, and institution information within MOVEit Transfer [40].

c)If there is no specific X-siLock-Step1 value, the ASPX file retrieves a specified file based on X-siLock-Step2 (representing a folder ID) and X-SiLock-Step3 (representing a file ID). In the absence of these headers, it adds a new administrative user named "Health Check Service" to the database and initiates an extended active session for this account [40].

The web shell initiated communication channels with the attackers, providing them control over the compromised system and the ability to issue commands. The communication occurred via HTTP requests, utilizing a particular header field to ensure authentication [12].

MITRE ATTACK Framework Mapping:

Tactic: Command and Control — *Techniques:* Multi-stage channels [T1104]

(7) Action on Objective

Once control was established, the adversaries executed a range of malicious activities, including obtaining Microsoft Azure system configurations, enumerating the SQL database, storing and retrieving files, generating administrator accounts, and deleting specific user accounts [12]. The victims of the

Fig. 3. Cl0p ransomware gang note Source: Adapted from [48]

MOVEit Transfer application exploit were given alert by the Cl0p ransomware gang to pay ransom by June 14, 2023 or else they would expose the names of the victims publically [40]. Unlike the other data exfiltration campaigns by the TA505, in this case ransomware was not deployed instead only data was stolen. Fig. 3 shows the threat actor demanded ransom and threatened to make the data public if any victim refrains from paying up [48].

MITRE ATTACK Framework Mapping:

Tactic: Exfiltration — *Technique:* Exfiltration Over C2 Channel, Exfiltration Over Command and Control Channel [T1041]

Tactic: Collection — *Technique:* Data from Local System [T1005]

IV. Impacts

According to report on the MOVEit data breach, as of November 9, 2023, 2,659 organizations and over 67 million people were impacted. The majority of the affected organizations were located in the Canada, Germany,United States and the United Kingdom[41]. The industry most affected is education, as these attackers have taken over the data of multiple universities. Among the well-known universities

impacted by this breach are Webster University, the University of Alaska, John Hopkins University, and the public school system in New York City. The health industry, banks, financial institutions, and businesses are among the other sectors that have been severely affected by this breach.

Leading prenatal, newborn, and child registry service BORN Ontario revealed that they were impacted by the MOVEit breach in a statement they released on September 25, 2023. They claim that the MOVEit vulnerability made it possible for unauthorized third parties to obtain and duplicate files containing private health information that were transferred via secure file transfer software and were part of BORN Ontario records.As a result, Born Ontario shut down the compromised server right away, isolated the system, and began an investigation in collaboration with cybersecurity specialists to determine the extent of the theft and the precise data that was taken[41].

In addition to the above mentioned sectors which was compromised some of the businesses impacted by this incident reveals a great deal about the extensive effects of highly sophisticated cyberattack campaigns[47].Few among them are zellius , BBC and Norton LifeLock .Zellis, a well-known payroll provider used by numerous large businesses, was compromised due to the MOVEit vulnerability, some of Zellis' clients were affected by this attack. This demonstrates how breaches in the software supply chain have a domino effect. When it became clear that the UK's state broadcaster was among the victims of the MOVEit hack, the media around the world quickly took notice. It seems that the BBC was among the establishments that suffered as a result of Zellis. It was somewhat ironic that Norton, which is well-known for its antivirus software and identity theft prevention solution, experienced data loss as a result of this attack. Then reports surfaced that data belonging to employees had been taken from internal systems[6].

V. Solutions

In order to strengthen their organization's security posture in reaction to threat actors actions, the authoring agencies advise organizations to put the mitigations and prevention listed below into practice. The National Institute of Standards and Technology (NIST) and Cybersecurity Infrastructure Security Agency (CISA) created the Cross-Sector Cybersecurity Performance Goals (CPGs), which are in line with the mitigations and prevention. CISA and NIST advise all organizations to adopt the minimum practices and protections outlined in the CPGs. To defend against the most prevalent and dangerous threats and TTPs, CISA and NIST based the CPGs on the cybersecurity frameworks and guidelines already in place [42]. There were, three significant vulnerabilities in MOVEit instances which was found. The MOVEit developer, Progress, has quickly addressed identified risks by releasing fixes for every vulnerability. Still, the mere existence of these vulnerabilities emphasizes the necessity of a multi-layered, dynamic security strategy [43].

A. Mitigations

(1) One of the easiest and most reliable ways to stop additional exfiltration is closing off Hyper Text Transfer protocol (HTTP)and HTTPs data traffic, both inbound and outbound .When the vulnerability was first discovered, Progress advised that the only effective defense against attacks was to modify firewall rules [44].

a) Modify firewall rules to prevent MOVEit Transfer from receiving HTTP and HTTPS traffic on ports 80 and until traffic over HTTP and HTTPS is restored [44].

b) It will not be possible for users to log into the MOVEit Transfer web interface [44].

c) Tasks in MOVEit Automation that utilize the native MOVEit Transfer host will stop functioning [44].

d) The Outlook plugin MOVEit Transfer will no longer function [44].

e) Secure File Transfer Protocol(SFTP) and File Transfer Protocol (FTP)/s protocols, however, will keep operating as usual [44].

f) Administrators can still access MOVEit Transfer by connecting to the Windows device via remote desktop and going to https://localhost/ [44].

(2) Once the vulnerability is discovered a patch follows shortly after that . After news of the initial attacks surfaced, a patch for the MOVEit attacks was not released for approximately 48 hours. However, there's a big there is a distinction between having a patch available and really deploying it, and the security and IT teams of the organization are responsible for ensuring that the patches are installed. There has been frequent observation that organizations have difficulty installing patches, even when they are available. Even after Progress issued the fix, some MOVEit users continued to get hacked because they hadn't yet installed it on their networks [45]. Furthermore, since there is usually more than one vulnerability IT administrators still needed to deploy the updates after installing MOVEit's initial patch. Thus, they have to be ready to roll out additional emergency patches when this kind of breach occurs.There never just have to be one if you establish the prerequisites for having any.

(3) Aside from all the other due diligence the organisation must, find out about a new vendor's vulnerabilities. It's better to have an open discussion than to request documentation; if you choose that path, you can request their Security Operations Center(SOC) 2 or a comparable audit. However, it will be beneficial to find out what the company needs to anticipate[45].When a program or application is as crucial as a secure managed file transfer solution, find out from the suppliers about their policies and security precautions.

B. Preventions

(1) Use application controls, such as allowlisting remote access programs, to manage and control software execution. Application controls should stop other software and portable versions of unauthorized remote access from being installed and run. Any unlisted application execution will be prevented by an application allowlisting solution that is configured

correctly. Allowlisting is crucial because malicious portable executables can go undetected by antivirus programs if they combine encryption, obfuscation, and compression [46].

(2) Use of Remote Desktop Protocol (RDP) and other remote desktop services should be strictly limited. Use best practices strictly if RDP is required

a) Use RDP to audit the network for systems.

b) Shut down any unused RDP ports.

c) Implement account lockouts following a predetermined amount of tries.

d) Use multifactor authentication (MFA) that is resistant to phishing attacks.

e) Record attempts at RDP login [47].

(3) Turn off permissions and command-line and scripting operations. Use Group Policy to limit PowerShell access, and only give permission to particular users when necessary. PowerShell should normally only be accessible to users or administrators who oversee the network or Windows operating systems (OSs)[47] .Update Windows PowerShell or PowerShell Core to the most recent version and delete all previous versions of PowerShell. logs from Windows PowerShell versions prior to 5.0. Diminish the risk of credentials being compromised Include domain administrator accounts in the protected user group in order to prevent local hash caching of passwords. Do not allow scripts to store login credentials in cleartext[6].

VI. Conclusion

Threats constantly evolve and change but older threats do not necessarily go away. Assuring awareness of adversary behaviors and tendencies to adapt defenses in response to malicious actions managing the attack surface to restrict or modify the options available to attackers in order to undermine the protected environment. Even though none of the these are simple, but they are essential to ensuring that organizations are able to both learn after the fact whether such events actually had an impact on the monitored environment and try to prevent significant compromise in situations like the MOVEit attack . Not every point of presence that threat actors initially acquire during a campaign will be exploited. Thus, in slow-moving campaigns like this one, the ability to detect such activity or associated artifacts is essential to severing the long tail of threat actor operations.

References

[1] Progress "MOVEit Transfer" https://www.ipswitch.com/moveit-transfer.

[2] Progress MOVEit "MOVEit Transfer DMZ" https://www.moveitmanagedfiletransfer.com/products/moveit-transfer

[3] Lily Hay Newman, Matt Burgess "The Biggest Hack of 2023 Keeps Getting Bigger" https://www.wired.com/story/moveit-breach-victims/

[4] Kenny Najarro "MOVEit Hack: the Ransomware Attacks Explained", 2023

[5] Joseph Menn "What you should know about the MOVEit ransomware attack" https://www.washingtonpost.com/technology/2023/06/16/moveit-ransomware-attack/

[6] Outpost24 "The MOVEit hack and what it taught us about application security" https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/

[7] Ali Ahmed Mohammed Ali Alwashali, Nor Azlina Abd Rahman, Noris Ismail "*A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack*" in *14th International Conference on Developments in eSystems Engineering (DeSE)*, 2021

[8] Canadian Centre for Cyber Security"Profile: TA505 / CL0P ransomware"

[9] MITRE ATTACK "TA505", https://attack.mitre.org/groups/G0092

[10] Antonis Terefos, Anne Postma "TA505: A Brief History Of Their Time" https://research.nccgroup.com/2020/11/18/ta505-a-brief-history-of-their-time/

[11] Karl Kiesel, Tom Deep, Austin Flaherty, Suman Bhunia "*Analyzing Multi-Vector Ransomware Attack on Accellion File Transfer Appliance Server*" in 2022 *7th International Conference on Smart and Sustainable Technologies (SpliTech)*, 2022

[12] Cybersecuirty and Infrastructure Security Agency "Exploitation of Accellion File Transfer Appliance", https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-055a

[13] Cybersecuirty and Infrastructure Security Agency "StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability", https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

[14] MITRE ATTACK "SDBbot", https://attack.mitre.org/software/S0461/

[15] MITRE ATTACK "FlawedGrace" https://attack.mitre.org/software/S0383/

[16] Andrew Moore, Genevieve Stark, Isif Ibrahima, Van Ta, Kimberly Goody "Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion" https://www.mandiant.com/resources/blog/accellion-fta-exploited-for-data-theft-and-extortion

[17] Connor Jones "The GoAnywhere data breach explained" https://www.itpro.com/security/data-breaches/370409/the-goanywhere-data-breach-explained

[18] Leyla Bilge, Tudor Dumitras "*Before we knew it: an empirical study of zero-day attacks in the real world*" in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012

[19] Yaman Roumani "*Patching zero-day vulnerabilities: an empirical analysis* in *Journal of Cybersecurity*, 2021

[20] OWASP "SQL Injection" https://owasp.org/www-community/attacks/

[21] Limei Ma, Yijun Gao, Dongmei Zhao, Chen Zhao, *"Research on SQL Injection Attack and Prevention Technology Based on Web"* in International Conference on Computer Network, Electronic and Automation, 2019

[22] Huthifh Al-Rushdan, Mohammad Shurman, Sharhabeel H. Alnabelsi, Qutaibah Althebyan *"Zero-Day Attack Detection and Prevention in Software-Defined Networks"* in *2019 International Arab Conference on Information Technology*, 2019

[23] Harun Oz, Ahmet Aris, Albert Levi, A. Selcuk Uluagac "A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions" in *ACM Computing SurveysVolume 54Issue 11s*, 2022

[24] Samar Kamil, Siti Norul, Huda Sheikh Abdullah, Ahmad Firdaus, Opeyemi Lateef Usman "The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges" in *2019 International Arab Conference on Information Technology*, 2019

[25] Microsoft "Ransomware as a service: The new face of industrialized cybercrime" https://www.microsoft.com/en-us/security/business/security-insider/threat-briefs/ransomware-as-a-service/

[26] Abdelhakim Hannousse, Salima Yahiouche "*Handling webshell attacks: A systematic mapping and survey*" in *Computers and Security, Volume 108, Issue C*, 2021

[27] Truong Dinh Tu, Cheng Guang, Guo Xiaojun, Pan Wubin "*Webshell Detection Techniques in Web Applications*" in *Fifth International Conference on Computing, Communications and Networking Technologies*, 2014

[28] MITRE ATTACK "Server Software Component: Web Shell" https://attack.mitre.org/techniques/T1505/003/

[29] Jai Vijayan "Cl0P Gang Sat on Exploit for MOVEit Flaw for Nearly 2 Years" https://www.darkreading.com/attacks-breaches/cl0p-gang-exploit-moveit-flaw-2-years

[30] Scott Downie, Devon Ackerman, Laurie Iacono, Dan Cox "Clop Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021" https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362

[31] NIST "CVE-2023-34362 Detail" https://nvd.nist.gov/vuln/detail/CVE-2023-34362

[32] Progress "MOVEit Transfer and MOVEit Cloud Vulnerability" https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability

[33] CVE MITRE "CVE-2023-34362" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34362

[34] NIST ”CVE-2023-35708 Detail” https://nvd.nist.gov/vuln/detail/CVE-2023-35708
[35] NIST ”CVE-2023-35036 Detail” https://nvd.nist.gov/vuln/detail/CVE-2023-35036
[36] Pratik Dholakiya ”What Is the Cyber Kill Chain and How It Can Protect Against Attacks” https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks
[37] Alex Delamotte, James Haughom ”MOVEit Transfer Exploited to Drop File-Stealing SQL Shell” https://www.sentinelone.com/blog/moveit-transfer-exploited-to-drop-file-stealing-sql-shell
[38] Nader Zaveri ”Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft” https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft
[39] John Hammond ”MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response” https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response
[40] Drew Burton, Cynthia Wyre ”CVE-2023-34362: MOVEit Vulnerability Timeline of Events” https://www.rapid7.com/blog/post/2023/06/14/etr-cve-2023-34362-moveit-vulnerability-timeline-of-events/
[41] Jonathan Reed ”The MOVEit breach impact and fallout: How can you respond?” https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/
[42] Chioma Ibeakanma ”Were You a Victim of the MOVEit Breach? Here’s What You Need to Know” https://www.msn.com/en-us/news/technology/were-you-a-victim-of-the-moveit-breach-heres-what-you-need-to-know
[43] National Cyber Security Centre ”MOVEit vulnerability and data extortion incident” https://www.ncsc.gov.uk/information/moveit-vulnerability-moveit-breach-impact-and-fallout-how-can-you-respond/
[44] Jonathan Reed ”The MOVEit breach impact and fallout: How can you respond?” https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/
[45] Eviden Threat Intelligence team ”Detailed analysis of the Zero- Day vulnerability in MOVEit transfer” https://atos.net/en/lp/securitydive/detailed-analysis-of-the-zero-day-vulnerability-in-moveit-transfer
[46] Beenu Arora ”Unmasking MOVEit: Vulnerabilities, Cyberattacks And The Urgency For Stronger Security” https://www.forbes.com/sites/forbestechcouncil/2023/09/12/unmasking-moveit-vulnerabilities-cyberattacks-and-the-urgency-for-stronger-security/?sh=66fcace06fb8
[47] Cybersecuirty and Infrastructure Security Agency ”Cross-Sector Cybersecurity Performance Goals” https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
[48] Tenable ”FAQ for MOVEit Transfer Vulnerabilities and CL0P Ransomware Gang” https://www.tenable.com/blog/faq-for-moveit-transfer-vulnerabilities-cve-2023-34362-and-cl0p-ransomware-gang
[49] Financial Times ”Almost 770,000 Calpers members hit by cyber attack” https://www.tenable.com/blog/faq-for-moveit-transfer-vulnerabilities-cve-2023-34362-and-cl0p-ransomware-gang
[50] Hadrian ”MOVEit Breach: Timeline of the Largest Hack of 2023” https://hadrian.io/blog/moveit-cyberattacks-timeline-of-the-largest-hack-of-2023