

Analysis of the MOVEit Supply Chain Cyberattack

Pranavsai Gandikota

Abstract—On Memorial Day, a large Russian-linked supply chain attack by the cybercrime group, Cl0p, took place. They attacked on a day when not many employees would be working, using a vulnerability in Progress Software’s MOVEit Transfer application’s SQL injection (CVE-2023-34362). This resulted in over 2,500 organizations being compromised across the world. IBM, which used MOVEit, also had the Protected Health Information (PHI) of millions of Americans stolen as a result. This impact carried to the Colorado Department of Health Care Policy and Financing whose vendor was IBM. The paper analyzes the attack, history, method, and impact of this attack on the government and the data privacy of millions.

I. INTRODUCTION

There are lots of secure and automated transfers of data taking place daily and managed file transfer (MFT) is what runs a majority of this. It handles sensitive financial and healthcare information. In May of 2023, the MOVEit Transfer platform was compromised in a supply chain attack [1]. This means rather than attacking the main goal, the smaller vendor is attacked to get access to all connected organizations. Unlike normal ransom which encrypts data and prevents actions, this attack was more focused on silently pulling data from the databases. IBM, being a vendor, also affected the Colorado Department of Health Care Policy and HCPF financing [2].

II. HISTORY

A. Who was Cl0p?

The attack was attributed to the Cl0p ransomware group [1] (also known by Lace Tempest or FIN11). Although Cl0p was not state-sponsored, its execution was similar to a nation-state actor. Because they avoided targets in the Commonwealth of Independent States (CIS) and comments in code were in words linked to the Russian language, they were said to have originated in Russia.

B. How did the attack develop?

Accellion FTA (File Transfer Appliance) of December 2020 was the prototype for the MOVEit attack where they began to plan attacking the place of file transfer rather attacking companies individually. Fortra’s GoAnywhere MFT was the next major attack which helped them improve their strategy, affecting almost 130 organizations using the zero-day exploit. Those attacks helped in funding for the MOVEit attack. Researchers showed that MOVEit began its testing in around July 2021. This gave them some years in between to prepare. They started testing more around May of 2023 as they waited for the right time.

C. The Purpose and Their Actions

Monetary gain was the main reason for the incident. However, Cl0p, unlike other ransom did not use encryption with negotiations for the keys to the data. Rather, they listed the victims on a ”Leaked and Found” dark web site where they threatened to publish the sensitive personally identifiable information (PII) until paid a ransom [1].

III. THE ATTACK AND IMPACT

A. The Start

The attack began on May 27, 2023 during the U.S. Memorial Day [3]. This was intentionally planned as the IT team would not have many people working on that day. In 48 hours, the attackers automated the MOVEit server scanning and deployed their webshell before a patch could be made [4].

B. The Effect on IBM and Colorado HCPF

- **Discovery:** Progress Software announced about the attack on May 31, 2023. HCPF later launched an investigation showing unauthorized actors on MOVEit who used certain HCPF files around May 28 [3]. Almost 4 million people were affected, with their SSN, Medicaid IDs, income information, and medical data all stolen [5]. Not only that, but the Missouri Department of Social Services (DSS) was affected too since it was connected with IBM.

C. The Financial Impact

Adding up all the ransom payments, cost for investigations, remediation, and legal expenses, the expenses added up to almost more than \$ 12 billion in damages. National security was affected too since the U.S. Department of Energy (DOE) and other federal agencies were attacked [6].

D. The CIA Impact

As a result of this attack, the confidentiality of many people was compromised, with the PII and PHI being stolen from millions. The integrity of the system was also affected since LEMURLOOT was able to modify the server to allow commands without any authorization. Availability was affected as well since many organizations had to turn their instance of MOVEit off in order to patch it. This stopped many businesses and file transfers from running.

IV. GENERAL CHARACTERISTICS

A. The Attack's Penetration Strategy

The main vulnerability was in the "moveitisapi.dll" module of MOVEit Transfer [7], which allowed for SQL injection with no authentication. There was no proper check in the information coming from the header of the web request. By putting the attacking code into this header, the attackers were able to talk to the database. This let them have privileges like an admin and also let them use the system, faking as one of the users. Once in, they used a script called LEMURLOOT (its file name being human2.aspx) [4] that worked in place of the original to avoid detection, working to steal files.

B. The LEMURLOOT Web Shell

LEMURLOOT was built for this attack and was able to retrieve Azure Blob Storage settings to be able to steal data from the cloud directly [4]. It was unique as it required a password they made to access it. This let them download all the files straight from the cloud. To avoid being detected, they also used gzip to send the data back to themselves as a compressed file so it looked normal in the traffic.

V. USAGE DOMAINS

The intended domain was the trusted enterprise sectors. MOVEit was popular in industries handling high-value data, being compliant with data laws (HIPAA, the US federal law regarding PHI and GDPR, the European regulation on personal data).

A. Industries Targeted

The main targets for this attack were:

- **Healthcare:** Organizations such as IBM/HCPF were the main targets since medical records had a lot of value [2].
- **Government:** The Louisiana and Oregon DMVs had millions of drivers license numbers leaked.
- **Financial Services:** Pension funds such as CalPERS had the financial history of retirees exposed.

VI. THE DISTINCTIVE FEATURES

- **Zero-Day:** Cl0p planned a zero-day attack (which is exploiting a vulnerability that the company they are attacking is not aware of, giving them no time to fix it) waiting for a day when not many people were working. This was normally not done by many groups, especially at such a scale this large.
- **The Victims:** A majority of victims were clients of the vendor that used MOVEit rather direct MOVEit customers.
- **Method of Extortion:** Cl0p sent a public notice on the dark web instructing victims to contact them, unlike other ransom where the victims are generally privately pressured [1].

VII. ACTIVE DESCENDANTS

Despite the vulnerability being patched, the threat actor still remains.

A. Lace Tempest

Microsoft tracked the group as "Lace Tempest", who still continues to use their Zero Day technique to attack. One such example was in November 2023, in the SysAid IT support software exploitation. They used a web shell to steal data and demanded money, similar to the MOVEit incident.

B. The Legacy

Descendants of this attack are still continuing this method since it was an easier way to steal money. Unlike other ransomware that affected the computers and stopped services, this was more silent and used to run in the background. They only copy files and don't affect the victim in whatever tasks they do, making it harder to notice and not too alarming for the victim as well. It is also simpler and cost effective for hackers to avoid all the extra work in making locks and encrypting.

C. Why the Descendants Still Exist

Despite all the measures taken against these groups, they generally are able to get away for several reasons. First, since they are working out of Russia, they can't be found since Russia would be protecting them as long as the Russians don't get attacked. Let alone the fact that putting an end to the server of one hacker group would not stop them from making a new group. Also, many companies have a lot of vulnerabilities, and a hacker only needs one to get in. Sometimes, not being able to find such vulnerabilities is the victim's disadvantage as in the case of the MOVEit attack.

VIII. PREVENTION AND PUNITIVE ACTIONS

A. Punitive Actions

The U.S. government made an offer of a \$10 million in bounty in the "Rewards for Justice" program to get information that linked Cl0p to foreign governments. There were also lawsuits filed against Progress Software and IBM for negligence in data protection.

B. Prevention and Solutions

The attack was overcome through support from CISA and the FBI, where patches were released and customers were immediately told to apply them. The traffic to all HTTP and HTTPS connections to MOVEit Transfer Systems was also disabled.

To prevent such an attack in the future is important, and two methods that can be used are:

- **Updating Patches on Time:** By applying security patches as soon as they are made would help prevent gaps for a zero day attack.
- **Segmenting the Network:** By segmenting a network, even if one part is attacked, it would help prevent the spread to other data making it harder for the attacker to access all records from one spot. This is a part of the "Zero Trust" architecture where we are always alert and maintain security in all areas.

IX. CONCLUSIONS

The MOVEit cyberattack showed us an important problem to take care of in supply chain security, where even a secure organization is vulnerable if the vendor is compromised. The result was the theft of health data from more than 4 million Americans, the disruptions in many companies and loss of more than billions of dollars, all done through a zero day exploit. But methods, such as the Zero trust model can be used in preventing such an attack in the future against the many descendants continuing to grow to date.

REFERENCES

- [1] "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability." Cybersecurity and Infrastructure Security Agency (CISA). <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a> (accessed Feb. 1, 2026).
- [2] C. Page, "Millions of Americans' Health Data Stolen After MOVEit Hackers Targeted IBM," TechCrunch, Aug. 14, 2023.
- [3] "MOVEit transfer data breaches Deep Dive," ORX News Deep Dive, <https://orx.org/resource/moveit-transfer-data-breaches> (accessed Feb. 1, 2026).
- [4] "Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft," Google Cloud Threat Intelligence, June 2, 2023.
- [5] "IBM MOVEit Transfer Use Leads to Massive Data Breach, Millions of Americans' Health Data Stolen," Dataquest, Aug. 2023.
- [6] J. Greig, "Two Energy Department Entities Breached as Part of Massive MOVEit Compromise," CyberScoop, June 15, 2023.
- [7] "Threat Brief: MOVEit Transfer SQL Injection Vulnerabilities," Palo Alto Networks, June 5, 2023.