WESTFIELD SPECIALTY℠

MOVEit Widespread **Cyber Ransom Incident**

CO-AUTHORS

Sara Trokan
SVP Westfield Specialty
Pro – Claims Leader

Mike Colford
SVP Westfield Specialty
Pro – Cyber / Technology
Product Leader

What happened?

MOVEit is a managed file transfer ("MFT") software owned by the US-based Progress Software Corporation. MOVEit allows for the transfer of files between business partners and customers. In late May 2023, threat actors began exploiting a zero-day critical security vulnerability in the MOVEit file transfer software. Once they gained access to MOVEit servers, they injected a webshell to allow them to exfiltrate data from MOVEit databases.

Cl0p, a known ransomware group, publicly stated that it was responsible for the attacks, and it claims to have information on hundreds of companies. While Cl0p is the only bad actor to have publicly stated it has exploited the vulnerability, other threat actors could or may have already exploited the same vulnerability.

These bad actors direct victims to reach out via email to receive the ransom demand amount in order to avoid publication of the exfiltrated data on its website. To date, the list of victims range in size and can be found across multiple industries and as publicly reported, includes many state and federal government agencies.

How did we get to this point?

The cyber industry began seeing data extortion in late 2019 when the Maze ransomware group introduced what we now call "double extortion." With double extortion, prior to encrypting data on a computer system, the threat actor steals data and then extorts the entity not only for the price of the decryption key, but also for the return or deletion of the stolen data. If a victim does not pay, the threat actor threatens to release the data publicly. Many threat actor groups followed suit and double extortion is now common in ransomware attacks.

Today, as seen in the MOVEit event, some threat actors are focused on data extortion only and not encrypting files. Data exfiltration alone is not as destructive or disruptive to the victim organization. This approach, while not as destructive from the victim's point of view, is easier for the threat actor to manage. The threat actor does not have to bother with decryption keys across multiple entities, thus making the attack easier to scale. This method may also allow the threat actors to avoid detection longer and help them continue to operate while avoiding government sanctions often tied to specific variants of encryption malware. MFT software, like MOVEit, has increasingly become the focus of bad actors. Previous zero-day vulnerabilities were exploited to steal data and extort victims in the past, most notably in connection with two other MFT providers' software, Accellion in 2020 and 2021, and GoAnywhere in early 2023.

Perpetrating a ransomware and extortion operation against an organization has become more difficult with the advancement of detection technology and other security tools. Leveraging a vulnerability in an MFT program, like MOVEit, which is often exposed directly to the internet, allows the bad actors to access multiple victim organizations' data at a single transfer point without the need to breach the security of the organization, navigate the organization's network, and exfiltrate their data without being detected.

What to expect from cyber insurance carriers?

Due to the scale of this event, cyber insurance carriers will likely have additional questions related to these known vulnerabilities. Carriers will continue to monitor the potential impact arising from the MOVEit vulnerability. Carriers may not only address this specific vulnerability with their insureds, but will also likely reinforce the importance of understanding how insureds are able to identify and remediate future zero-day vulnerabilities within their own network security program as well as within the security programs of those third parties with whom they share data.

The following are examples of likely additional questions asked as part of the underwriting process:

- Does the insured use the impacted Progress Software's MOVEit file transfer program within their environment or anywhere within the course of their business operations?
- If yes, has the insured appropriately implemented all patches related to the zero-day vulnerabilities in the MOVEit transfer program (currently including CVE-2023-34362, CVE- 2023-35036, CVE-2023-35708) and reviewed and implemented the mitigation steps advised by Progress Software and CISA?
- Has the insured reviewed their use of the MOVEit program to assess any potential unauthorized access to the insured's network or data?
- Has the insured taken steps to assess the use of the MOVEit program by their third-party vendors where the insured's data could have been accessed by unauthorized third parties?
- Does the insured have a way to help ensure the patching of their third-party vendors as it relates to the MOVEit vulnerabilities or any other future zero-day vulnerabilities?
- Does the insured have a formal patch management program in place inclusive of specific steps to expedite patches upon release that are created to mitigate the exposure to known zero-day vulnerabilities?

Westfield Specialty℠ has highly experienced cyber underwriters and claims personnel offering industry-leading risk transfer and cyber risk management insurance solutions across all industry segments. For more information, please contact your insurance agent or broker.

Contact**Us**

E&O/Cyber Regional Leaders

John Castoro
VP Northeast
Johncastoro@westfieldgrp.com

Alex Whipple
AVP Southeast
Alexwhipple@westfieldgrp.com

Christine Dickenson
VP Central
Christinedickenson@westfieldgrp.com

Brian McCall
SVP West & Head of Field Operations
BrianMcCall@westfieldgrp.com

REFERENCES

Abrams, L. (2023, June 1). New MOVEit Transfer zero-day mass-exploited in data theft attacks. bleepingcomputer.com. www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/.

Abrams, L. (2023, June 5). Clop ransomware claims responsibility for MOVEit extortion attacks. bleepingcomputer.com. www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/.

Abrams, L. (2023, June 15). Clop ransomware gang starts extorting MOVEit data-theft victims. bleepingcomputer.com. www. Clop ransomware gang starts extorting MOVEit data-theft victims/.

Burt, J. (2022, October 9). When are we gonna stop calling it ransomware? It's just data kidnapping now. theregister.com. www.theregister.com/2022/10/09/extortion_ransomware_threats_category/.

Progress.com. (2023, June 15). MOVEit Transfer and MOVEit Cloud Vulnerability. Progress.com. www.progress.com/security/moveit-transfer-and-move-it-cloud-vulnerability.

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA). (2023, June 7). #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability. Cisa.gov. www.#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability.

WESTFIELD SPECIALTY℠

westfieldinsurance.com/specialty