MOVEit Transfer Breach

C-Suite level threat review by applicable business area addressing active threats.

Supply chain security is garnering the attention of cybersecurity personnel and governing bodies as a key risk area. The MOVEit Transfer breach further draws attention to this risk area and the importance of supply chain security in data management. MOVEit Transfer is Progress Software's managed file transfer solution, used by organizations for internal and external file-sharing purposes. Due to its function, organizations that do not directly own the tool are still affected by the recent breach, contributing to its scale. Some of these organizations may not yet be aware that they are impacted. To mitigate the impacts of this type of attack, organizations can start by identifying and assessing risks associated with supply chain security and date sharing practices. This can provide a foundation for the next steps.

Clop Ransomware Group:

The Clop Ransomware Group took responsibility for the MOVEit Breach. This ransomware variant emerged in 2019 and is associated with the Russian-based, financially motived FIN11. This threat actor is also known as Lace Tempest and TA505. It should be noted that some analysts assert FIN11 is a subgroup of TA505. While typically the threat actor will use double extortion (i.e., encrypting and exfiltrating data), it only exfiltrated data in the MOVEit breach. A broad set of industries have been affected, including education, government agencies, banking, and healthcare. Notably, this is the threat actor's third time successfully exfiltrating data from file transfer solutions.

Clop Ransomware

Threat Level: High

Attack:

The threat actor exploited a zero-day SQL injection vulnerability (CVE-2023-34362) in the MOVEit transfer software which enabled them to elevate privileges and deploy a web shell called LEMURLOOT. The web shell is geared towards interacting with the MOVEit transfer software. For example, it masquerades detection by using a file name similar to a legitimate file in the MOVEit transfer software. The web shell also targets Azure databases. LEMURLOOT can retrieve system setting and record information from Azure Storage blob, create / delete users and exfiltrate data.

Remediation:

- Organizations using MOVEit transfer should ensure the software is patched to prevent exploitation of the following vulnerabilities: CVE-2023-34362, CVE-2023-35036, CVE-2023-35708.
- Assess and implement secure supply chain and data sharing practices.
- Conduct regular vulnerability assessments.

MOVEit Transfer Attack Mapped to MITRE ATT&CK

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Description
Initial Access	Exploit Public Facing Application (T1190)	Exploited a SQL injection vulnerability in the managed file transfer solution
Persistence	Server Software Component: Web Shell (T1505.003)	Deployed a web shell named LEMURLOOT
Persistence	Create Account (T1136)	LEMURLOOT can create users in Azure
Privilege Escalation	Exploitation for Privilege Access (T1068)	Authenticated as a high-privilege user
Defense Evasion	Masquerading: Match Legitimate Name or Location (T1036.005)	Components mirror legitimate MOVEit Transfer components. For example, LEMURLOOT is deployed with the name human2.aspx which mirrors a legitimate file of the MOVEit Transfer software, human.aspx.
Discovery	Cloud Storage Object Discovery (T1619)	LEMURLOOT can retrieve system setting and record information from Azure Storage blob.
Command and Control	Application Layer Protocol: Web Protocols (T1071.001)	The threat actor communicates with the web shell via HTTP requests
Exfiltration	Exfiltration over C2 Channel (T1041)	Exfiltrated data to C2 server
Impact	Account Access Removal (T1531)	LEMURLOOT can delete users in Azure.

MOVEit Transfer Breach:

- **FBI and CISA joint cybersecurity advisory on the breach:** https://www.cisa.gov/sites/default/files/2023-06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
- **Additional information:** https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
  - Penetration testing
  - Tabletop exercises
  - Threat Intelligence Program Maturity
  - Develop playbooks of adversary TTPs