Advisory
CL0P MOVEit Campaign

Verizon Threat Research Advisory Center (VTRAC)

June 22, 2023

Threat Light Protocol (TLP) (Clear)

Executive Summary

The Verizon Threat Research Advisory Center is shedding light on a significant series of security incidents involving the exploitation of MOVEit Transfer, a managed file transfer solution developed by Progress Software. The responsible threat actor group is CL0P ransomware group, also identified as TA505. The cybercrime outfit is known for previous similar exploits in 2020, 2021, and early 2023. This series of breaches, all tied to the same exploit, has been impactful across a broad spectrum of industries and geographical locations, with a significant concentration in the United States and in sectors such as finance, healthcare, and government.

A campaign orchestrated by CL0P commenced in late May 2023, leveraging a then unknown SQL injection vulnerability (CVE-2023-34362) in MOVEit Transfer. This led to the installation of a web shell named LEMURLOOT, enabling unauthorized access to the MOVEit Transfer databases.

The Verizon Threat Research Advisory Center (VTRAC) is part of the Verizon Cyber Security Consulting organization and provides threat-related detection, intelligence, and response services to Verizon customers.

The threat actors employed a diverse suite of tools in their attack, demonstrating high levels of sophistication and adaptability. Initial access is achieved through SQL injection to infiltrate the MOVEit Transfer web application. Threat actors then deployed the SDBot backdoor, enabling them to execute further malicious commands on the compromised systems. TinyMet and Truebot were used for establishing communication with the threat actor's command and control (C2) server and downloading additional modules. Truebot also facilitated persistence, evasion, and data collection.

The CL0P actors then employed various techniques for privilege escalation, lateral movement, and data exfiltration. These included compromising the Active Directory (AD) servers, using Cobalt Strike, Remote Desktop Protocol (RDP), and FlawedAmmyy remote access trojan (RAT).

The breach's full implications are still being investigated, but the initial analysis suggests there may be significant exposure to sensitive data and potential disruptions to organizational operations. Immediate attention to this advisory's analysis and recommendations is important for any organization using MOVEit Transfer software.

Analysis

Progress Software's MOVEit Transfer is a commonly used solution that manages an organization's file transfer operations. Its web application is compatible with MySQL, Microsoft SQL Server, and Azure SQL database engines, making it an essential component within many IT infrastructures. However, the discovery of a SQL injection zero-day vulnerability (CVE-2023-34362) has exposed these systems to potential significant risk.

The CL0P ransomware group was able to exploit this vulnerability in May 2023, installing a malicious web shell named LEMURLOOT [T1190] on affected MOVEit Transfer web applications. The choice of the name 'human2.aspx' for the web shell appears to be a deliberate attempt to camouflage it as the legitimate 'human.aspx' file present within the MOVEit Transfer software. Upon its successful installation, the web shell generates a unique, random 36-character password for authentication purposes.

Communication between the web shell and its operators occurs through HTTP requests, specifically ones containing a header field named 'X-siLock-Comment'. The value assigned to this field must match the password created during the web shell's installation for the authentication to succeed. Once the authentication is established, the operators can relay various commands to the web shell.

These commands can enable operators to:

- Retrieve Microsoft Azure system settings and enumerate the underlying SQL database. This would allow threat actors to gain a deeper understanding of the system's configuration, potentially exposing additional vulnerabilities.
- Store a string sent by the operator and then retrieve a file with a name matching the string from the MOVEit Transfer system. This feature would enable the theft and exfiltration of sensitive data.
- Create a new administrator privileged account with a randomly generated username and 'LoginName' and 'RealName' values set to "Health Check Service." This would allow attackers to maintain access to the system, even if the initial point of entry is discovered and removed.
- Delete an account with 'LoginName' and 'RealName' values set to 'Health Check Service.' This would help conceal the attacker's presence by cleaning up after their activities.
- This approach has allowed CL0P to gain unauthorized access to data, create or delete administrator-level accounts, and potentially maintain persistence within a compromised MOVEit Transfer environment.

Attack Flow

The CL0P ransomware group utilizes a sophisticated series of steps to infiltrate vulnerable systems:

1. **Initial Access (T1190, T1566):** The actors initiate the attack sequence by exploiting public-facing applications such as the MOVEit Transfer web application. They employ SQL injection techniques to achieve unauthorized access. Simultaneously, they distribute spear-phishing emails designed to trick recipients into providing access credentials.
2. **Execution (T1059.001, T1059.003, T1129):** Upon gaining initial access, the group uses SDBot as a backdoor to execute commands and functions within the compromised systems. They use the TinyMet Meterpreter stager for establishing reverse shells to their command and control (C2) servers. Additionally, the Truebot botnet is used for downloading and executing additional malicious modules.
3. **Persistence (T1505.003, T1546.011):** To ensure continued access to the compromised system, they deploy a web shell named DEWMODE, specially designed to interact with a MySQL database. SDBot malware is also used to implement application shimming, allowing the actors to persist in the environment and evade detection.
4. **Privilege Escalation (T1068):** With access to the MOVEit Transfer databases, the actors elevate privileges within the compromised network.
5. **Defense Evasion (T1055, T1070, T1574.002):** The group further obfuscates its presence using Truebot for shell code injection and DLL side-loading. Any traces of Truebot malware are removed post-use to avoid detection.
6. **Discovery (T1018):** Using Cobalt Strike, the actors perform network reconnaissance after gaining access to Active Directory servers, furthering their reach within the network.
7. **Lateral Movement (T1021.002, T1563.002):** The group expands their reach within the network by exploiting SMB vulnerabilities and hijacking RDP sessions, extending their access to other systems.
8. **Collection (T1113):** Sensitive data is gathered using Truebot for screen capture operations. Truebot loads web shell code such as LEMURLOOT to download files from the MOVEit Transfer system, extract Azure system settings, create, insert, or delete a particular user. The web shell returns data in a gzip compressed format.
9. **Command and Control (T1071, T1105):** The actors maintain control over compromised systems using the FlawedAmmyy remote access trojan (RAT), enabling the download of additional malware components. They also deploy SDBot to propagate via removable drives and network shares.
10. **Exfiltration (T1041):** Finally, collected data is exfiltrated through command and control channels for potential use in future attacks or for ransom demands.

Impact on Organizations

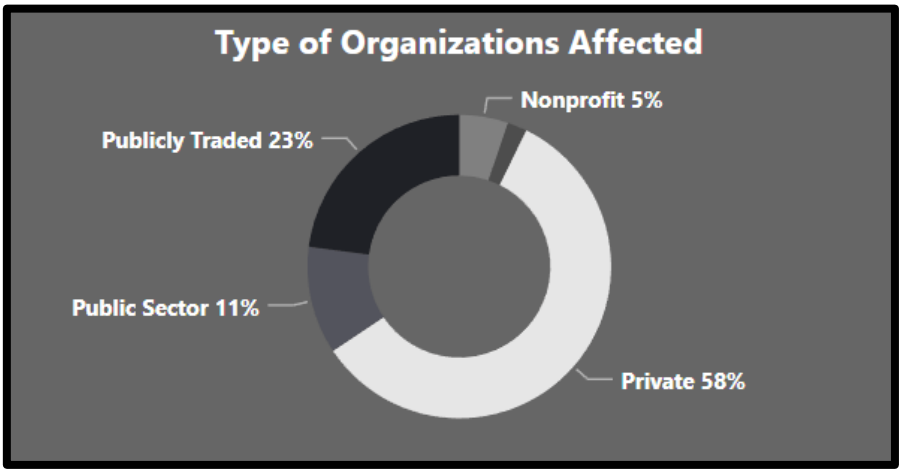

Figure 1: Types of Impacted Organizations

From the pool of 96 victims analyzed by Verizon researchers, it appears a diverse mix of private companies, publicly traded corporations, public sector organizations, and non-profit bodies have been targeted. The affected entities represent a wide cross-section of operational scales, with the median market cap for publicly traded companies standing at $6 billion, suggesting the attackers' focus on high-value targets.

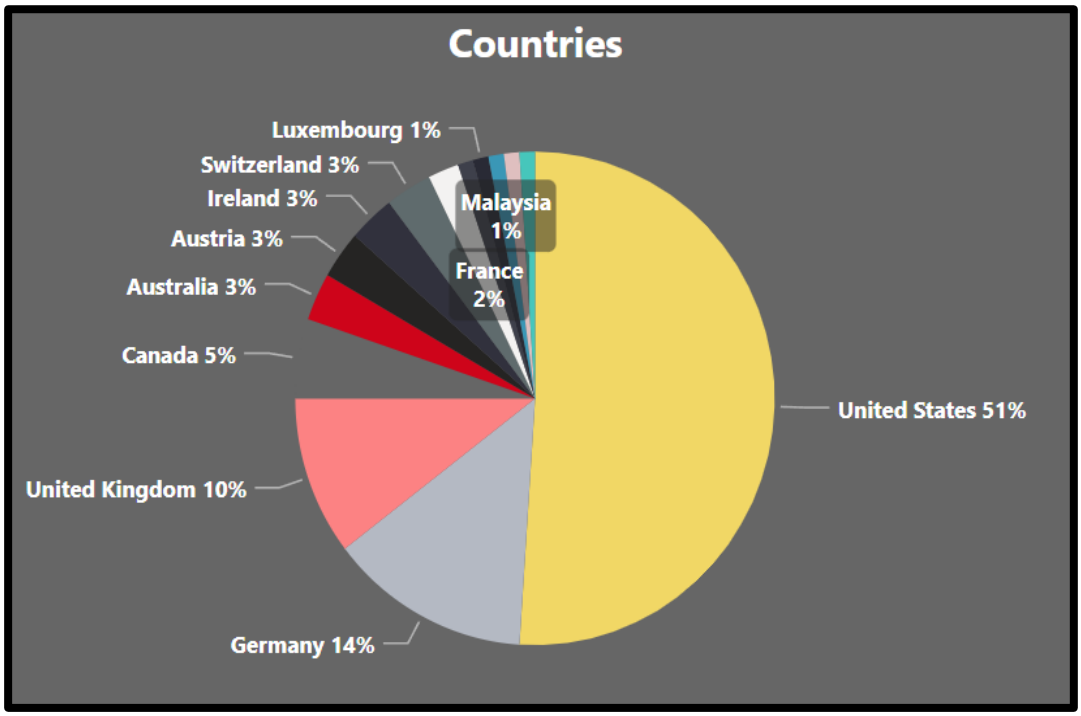

Figure 2: Countries of Origin for Impacted Organizations

Our data suggests that the impact of the breach is global, with a pronounced concentration in North America and Western Europe. The U.S. hosts most of the affected organizations, representing 51% of total cases. Germany, the U.K., and Canada follow with 14%, 11%, and 5% respectively.

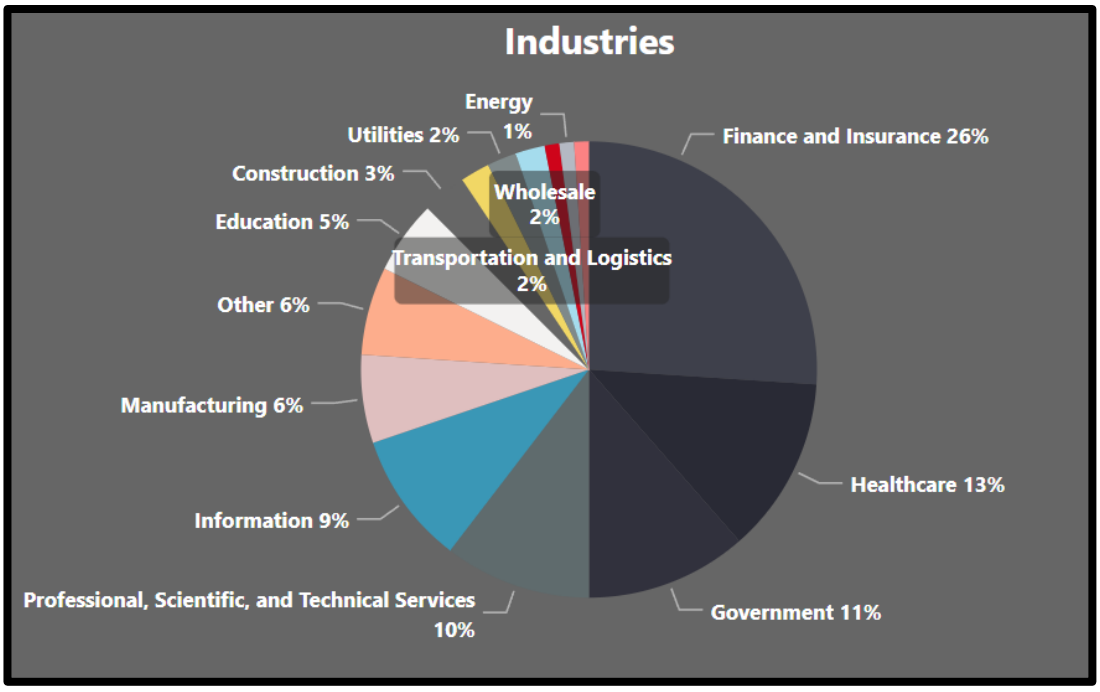

Figure 3: Industries of Impacted organizations

The financial and insurance sector constitutes the most significant proportion of affected organizations (26%), underlining its appeal as a high-value target for threat actors. This first place sector is followed by healthcare (13%), government (11%), professional, scientific, and technical services (10%), information (9%), manufacturing (6%), and education (5%).

MOVEit Campaign Indicators of Compromise

Source	URL
CISA	hxxps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-158a
Progress	hxxps://community.progress[.]com/s/relatedlist/ka74Q000000L8G1QAK/AttachedContentDocuments

The provided list of indicators of compromise (IoCs) associated with the MOVEit campaign is not exhaustive. Our understanding of the complete range of potential IoCs is still evolving. As researchers and security professionals continue to study and respond to these attacks, new IoCs will likely emerge. Thus, the current list should be viewed as a starting point, highlighting some of the most common or recognizable signs of these attacks, and not as a comprehensive guide. It's vital to stay informed about the latest developments in this area, as the threat landscape is rapidly evolving, with threat actors continually developing new techniques and approaches. Customers of the Verizon Threat Intelligence service are already equipped with these indicators of compromise (IoCs) as part of the Verizon Enhanced Intelligence Feed (VEIF). Moreover, they benefit from real-time access to updates and new findings. As we continue to identify and validate new IoCs related to CL0P ransomware and the MOVEit campaign, these will be promptly integrated into the VEIF, helping to ensure our customers are always at the forefront of knowledge in this rapidly evolving threat landscape.

Recommendations

The MOVEit attack underlines the critical importance of comprehensive and proactive security measures to detect, prevent, and respond to such sophisticated threats. Recommended best practices to consider would include:

1. **Auditing Remote Access Tools**: Regularly audit remote access tools on your network and review logs for execution anomalies.
2. **Implement Application Controls**: Control the execution of software by allowing the listing authorized remote access programs.
3. **Limit Use of RDP and Remote Desktop Services**: Rigorously apply best practices such as auditing, closing unused RDP ports, enforcing account lockouts, and employing multi-factor authentication (MFA).
4. **Disable Command-Line and Scripting**: Disallow command-line and scripting activities and permissions.
5. **Restrict PowerShell Usage**: Limit PowerShell access to specific users, update to the latest version, and uninstall earlier versions.
6. **Review Domain Controllers and User Accounts**: Regularly audit domain controllers, servers, workstations, and active directories for new or unrecognized accounts.
7. **Implement a Recovery Plan**: Maintain and retain multiple copies of sensitive data in a secure location and ensure offline backups of data.
8. **Enforce Password Policies**: Comply with NIST standards for password policies, including the use of longer passwords, storing passwords in hashed format, and implementing account lockouts after failed login attempts.

9. **Require Multi-factor Authentication (MFA)**: Implement MFA, particularly for webmail, virtual private networks, and accounts that access critical systems.
10. **Regularly Update Systems**: Keep operating systems, software, and firmware updated to minimize exposure to threats.
11. **Segment Networks**: Control traffic flows and restrict adversary lateral movement by segmenting networks.
12. **Install and Update Antivirus Software**: Ensure real-time detection for antivirus software on all hosts.
13. **Disable Unused Ports**: Block unused ports to reduce possible entry points for malicious actors.
14. **Add Email Banners**: Add an email banner to emails received from outside the organization.
15. **Disable Hyperlinks in Emails**: Disable hyperlinks in emails to help prevent inadvertent clicks leading to malicious sites.
16. **Encrypt and Protect Backup Data**: Ensure backup data is encrypted, immutable, and covers the entire data infrastructure.

Moreover, organizations should consider validating their security controls by aligning their technologies against MITRE ATT&CK techniques, testing these technologies, analyzing performance, and tuning the security program based on the generated data. By implementing these measures, organizations likely can significantly reduce the risk of similar breaches and enhance their cybersecurity posture.

Customers of Verizon cybersecurity services are reminded that they may engage Verizon's security consulting services to conduct a detailed assessment of their networks. This preventative due-diligence review can help to identify and mitigate possible malicious activities affecting critical services that can result in data loss and system integrity. For more information or further assistance, please contact your Verizon account representative or Professional Services liaison.