FIRMUS

FIRMUS ADVISORY

MOVEIT RANSOMWARE

Level 15, Hampshire Place 157 Hampshire,
Jalan Mayang Sari,
50450, Kuala Lumpur

+603-6411-2626 | info@firmussec.com

CREST PEN TEST MALAYSIA DIGITAL MALAYSIA CYBER SECURITY AWARDS

bsi ISO/IEC 27001 Information Security Management CERTIFIED

IS 743259

Summary

MOVEit Transfer, an established file transfer software, has been the target of high-profile hacks all across the world, including in Malaysia. Cl0p, a well-known threat group is behind all these ransomware attack. They exploited MOVEit which would lead to escalated privileges and potential unauthorized access to the environments. The method of attack is an SQL Injection attack to an unpatched MOVEit server that allow threat actor to gain access and execute arbitrary code remotely. The MOVEit Transfer web applications exposed to the internet were infected with the LEMURLOOT web shell, which was subsequently leveraged to steal data from underlying MOVEit Transfer databases.

Technical Details

MOVEit Transfer is a file transfer software used by organizations for file transfer operations that has a web application which supports MySQL, Microsoft SQL Server and Azure SQL database engines. The CL0P ransomware group used a SQL injection zero-day vulnerability CVE-2023-34362 in May 2023 to install the LEMURLOOT web shell on MOVEit Transfer web apps. Based on CVE-2023-34362, LEMURLOOT was utilised for persistence, information gathering and data theft. To communicate with MOVEit managed file transfer software, the webshell imports several libraries, including “”MOVEit.DMZ.ClassLib”, “MOVEit.DMZ.Application.Files”, and “MOVEit.DMZ.Application.Users”. The web shell was first discovered with the name human2.aspx in an attempt to impersonate the legitimate human.aspx file included in MOVEit Transfer software.

After installation, the web shell generates a random 36-character password to be used for authentication. The web shell communicates with its operator by awaiting HTTP requests containing a header field named X-siLock-Comment, which must have a value assigned equal to the password established upon the installation of the web shell. Operators pass commands to the web shell after authenticating with it, which can:

- Retrieve Microsoft Azure system settings, Azure Blob Storage, Azure Blob Storage account, Azure Blob key, and Azure Blob Container
- Enumerate the underlying SQL Database
- Store a string given by the operator and then obtain a file with the same name from the MOVEit Transfer system.
- Create a new administrator privileged account with a randomly generated username and LoginName and RealName values set to “Health Check Service”.
- Delete an account with LoginName and RealName values set to “Health Check Service”

Detection Methods

YARA Rules

```
rule CISA_10450442_01 : LEMURLOOT webshell communicates_with_c2
remote_access
{
  meta:
     Author = "CISA Code & Media Analysis"
     Incident = "10450442"
     Date = "2023-06-07"
     Last_Modified = "20230609_1200"
     Actor = "n/a"
     Family = "LEMURLOOT"
     Capabilities = "communicates-with-c2"
     Malware_Type = "webshell"
     Tool_Type = "remote-access"
     Description = "Detects ASPX webshell samples"
     SHA256_1                                                          =
"3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a745457
25b"
  strings:
     $s1 = { 4d 4f 56 45 69 74 2e 44 4d 5a }
     $s2 = { 25 40 20 50 61 67 65 20 4c 61 6e 67 75 61 67 65 3d }
     $s3 = { 4d 79 53 51 4c }
     $s4 = { 41 7a 75 72 65 }
     $s5 = { 58 2d 73 69 4c 6f 63 6b 2d }
  condition:
     all of them
}
```

```
rule M_Webshell_LEMURLOOT_DLL_1 {
   meta:
      disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
      description = "Detects the compiled DLLs generated from human2.aspx LEMURLOOT payloads."
      sample = "c58c2c2ea608c83fad9326055a8271d47d8246dc9cb401e420c0971c67e19cbf"
      date = "2023/06/01"
      version = "1"
   strings:
      $net = "ASP.NET"
      $human = "Create_ASP_human2_aspx"
      $s1 = "X-siLock-Comment" wide
      $s2 = "X-siLock-Step3" wide
      $s3 = "X-siLock-Step2" wide
      $s4 = "Health Check Service" wide
      $s5 = "attachment; filename={0}" wide
   condition:
      uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
      filesize < 15KB and
      $net and
      (
         ($human and 2 of ($s*)) or
         (3 of ($s*))
      )
}
```

```
rule M_Webshell_LEMURLOOT_1 {
   meta:
      disclaimer = "This rule is meant for hunting and is not tested to run in
a production environment"
      description = "Detects the LEMURLOOT ASP.NET scripts"
      md5 = "b69e23cd45c8ac71652737ef44e15a34"
      sample                                                              =
"cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60
ea45x"
      date = "2023/06/01"
      version = "1"
   strings:
      $head = "<%@ Page"
      $s1 = "X-siLock-Comment"
      $s2 = "X-siLock-Step"
      $s3 = "Health Check Service"
      $s4 = /pass, \"[a-z0-9]{8}-[a-z0-9]{4}/
      $s5 = "attachment;filename={0}"
   condition:
      filesize > 5KB and filesize < 10KB and
      (
         ($head in (0..50) and 2 of ($s*)) or
         (3 of ($s*))
      )
}
```

```
rule MOVEit_Transfer_exploit_webshell_aspx {

   meta:

      date = "2023-06-01"
      description = "Detects indicators of compromise in MOVEit Transfer
exploitation."
      author = "Ahmet Payaslioglu - Binalyze DFIR Lab"
      hash1 = "44d8e68c7c4e04ed3adacb5a88450552"
      hash2 = "a85299f78ab5dd05e7f0f11ecea165ea"
      reference1 =
"https://www.reddit.com/r/msp/comments/13xjs1y/tracking_emerging_m
oveit_transfer_critical/"
      reference2 =
"https://www.bleepingcomputer.com/news/security/new-moveit-
transfer-zero-day-mass-exploited-in-data-theft-attacks/"
      reference3 =
"https://gist.github.com/JohnHammond/44ce8556f798b7f6a7574148b67
9c643"
      verdict = "dangerous"
        mitre = "T1505.003"
      platform = "windows"
      search_context = "filesystem"

   strings:
      $a1 = "MOVEit.DMZ"
      $a2 = "Request.Headers[\"X-siLock-Comment\"]"
      $a3 = "Delete FROM users WHERE RealName='Health Check Service'"
      $a4 = "set[\"Username\"]"
      $a5 = "INSERT INTO users (Username, LoginName, InstID, Permission,
RealName"
      $a6 = "Encryption.OpenFileForDecryption(dataFilePath,
siGlobs.FileSystemFactory.Create()"
      $a7 = "Response.StatusCode = 404;"
   condition:

      filesize < 10KB
      and all of them
}
```

```
rule MOVEit_Transfer_exploit_webshell_dll {

   meta:

      date = "2023-06-01"
      description = "Detects indicators of compromise in MOVEit Transfer
exploitation."
      author = "Djordje Lukic - Binalyze DFIR Lab"
      hash1 = "7d7349e51a9bdcdd8b5daeeefe6772b5"
      hash2 = "2387be2afe2250c20d4e7a8c185be8d9"
      reference1                                                    =
"https://www.reddit.com/r/msp/comments/13xjs1y/tracking_emerging_m
oveit_transfer_critical/"
      reference2                                                    =
"https://www.bleepingcomputer.com/news/security/new-moveit-
transfer-zero-day-mass-exploited-in-data-theft-attacks/"
      reference3                                                    =
"https://gist.github.com/JohnHammond/44ce8556f798b7f6a7574148b67
9c643"
      verdict = "dangerous"
        mitre = "T1505.003"
      platform = "windows"
      search_context = "filesystem"

   strings:
      $a1 = "human2.aspx" wide
      $a2 = "Delete FROM users WHERE RealName='Health Check Service'"
wide
      $a3 = "X-siLock-Comment" wide
   condition:

      uint16(0) == 0x5A4D and filesize < 20KB
      and all of them
}
```

Indicator of Compromise

File	Hash
LEMURLOOT Web Shell	➢ 0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9 ➢ 0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495 ➢ 110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286 ➢ 1826268249e1ea58275328102a5a8d158d36b4fd312009e4a2526f0bfbc30de2 ➢ 2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5 ➢ 2ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59 ➢ 348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d ➢ 387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a ➢ 38e69f4a6d2e81f28ed2dc6df0daf31e73ea365bd2cfc90ebc31441404cca264

	➢ 3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b ➢ 3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409 ➢ 3c0dbda8a5500367c22ca224919bfc87d725d890756222c8066933286f26494c ➢ 4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf ➢ 48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a ➢ 58ccfb603cdc4d305fddd52b84ad3f58ff554f1af4d7ef164007cb8438976166 ➢ 5b566de1aa4b2f79f579cdac6283b33e98fdc8c1cfa6211a787f8156848d67ff ➢ 6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d ➢ 702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0 ➢ 769f77aace5eed4717c7d3142989b53bd5bac9297a6e11b2c588c3989b397e6b

	➢ 7c39499dd3b0b283b242f7b7996205a9b3cf8bd5c943ef6766992204d46ec5f1 ➢ 93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db ➢ 98a30c7251cf622bd4abce92ab527c3f233b817a57519c2dd2bf8e3d3ccb7db8 ➢ 9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead ➢ 9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a ➢ a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7 ➢ a8f6c1ccba662a908ef7b0cb3cc59c2d1c9e2cbbe1866937da81c4c616e68986 ➢ b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272 ➢ b5ef11d04604c9145e4fe1bedaeb52f2c2345703d52115a5bf11ea56d7fb6b03

	➢ b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad ➢ bdd4fa8e97e5e6eaaac8d6178f1cf4c324b9c59fc276fd6b368e811b327ccf8b ➢ c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4 ➢ c77438e8657518221613fbce451c664a75f05beea2184a3ae67f30ea71d34f37 ➢ cec425b3383890b63f5022054c396f6d510fae436041add935cd6ce42033f621 ➢ cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45 ➢ d477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899 ➢ d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195 ➢ daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4 ➢ e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e

	➢ ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a ➢ ed0c3e75b7ac2587a5892ca951707b4e0dd9c8b18aaf8590c24720d73aa6b90c ➢ f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d ➢ fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f

Malicious Domain
➢ http://hiperfdhaus[.]com ➢ http://jirostrogud[.]com ➢ http://qweastradoc[.]com ➢ http://qweastradoc[.]com/gate.php ➢ http://connectzoomdownload[.]com/download/ZoomInstaller.exe ➢ http://zoom[.]voyage/download/Zoom.exe ➢ http[:]//guerdofest[.]com/gate.php

HTTP Request
➢ POST /moveitisapi/moveitisapi.dll ➢ POST /guestaccess.aspx ➢ POST /api/v1/folders/[random]/files ➢ GET /human2.aspx

File Name
➢ human2.aspx ➢ human2.aspx.lnk ➢ huamn2.aspx.[random].compiled

IP Addresses
➢ 5.252.23.116 ➢ 5.252.25.88 ➢ 84.234.96.104 ➢ 89.39.105.108 ➢ 138.197.152.201 ➢ 148.113.152.144 ➢ 198.12.76.214 ➢ 209.97.137.33 ➢ 209.222.103.170 ➢ 104.194.222.107 ➢ 146.0.77.141 ➢ 146.0.77.155 ➢ 146.0.77.183 ➢ 162.244.34.26 ➢ 162.244.35.6 ➢ 179.60.150.143 ➢ 185.104.194.156 ➢ 185.104.194.24 ➢ 185.104.194.40 ➢ 185.117.88.17 ➢ 185.162.128.75 ➢ 185.174.100.215 ➢ 185.174.100.250 ➢ 185.181.229.240 ➢ 185.181.229.73 ➢ 185.183.32.122 ➢ 185.185.50.172 ➢ 188.241.58.244 ➢ 193.169.245.79 ➢ 194.33.40.103

- 194.33.40.104
- 194.33.40.164
- 198.27.75.110
- 206.221.182.106
- 209.127.116.122
- 209.127.4.22
- 45.227.253.133
- 45.227.253.147
- 45.227.253.50
- 45.227.253.6
- 45.227.253.82
- 45.56.165.248
- 5.149.248.68
- 5.149.250.74
- 5.149.250.92
- 5.188.86.114
- 5.188.86.250
- 5.188.87.194
- 5.188.87.226
- 5.188.87.27
- 5.34.180.205
- 62.112.11.57
- 62.182.82.19
- 62.182.85.234
- 66.85.26.215
- 66.85.26.234
- 66.85.26.248
- 79.141.160.78
- 79.141.160.83
- 84.234.96.31
- 89.39.104.118

- 91.202.4.76
- 91.222.174.95
- 91.229.76.187
- 93.190.142.131

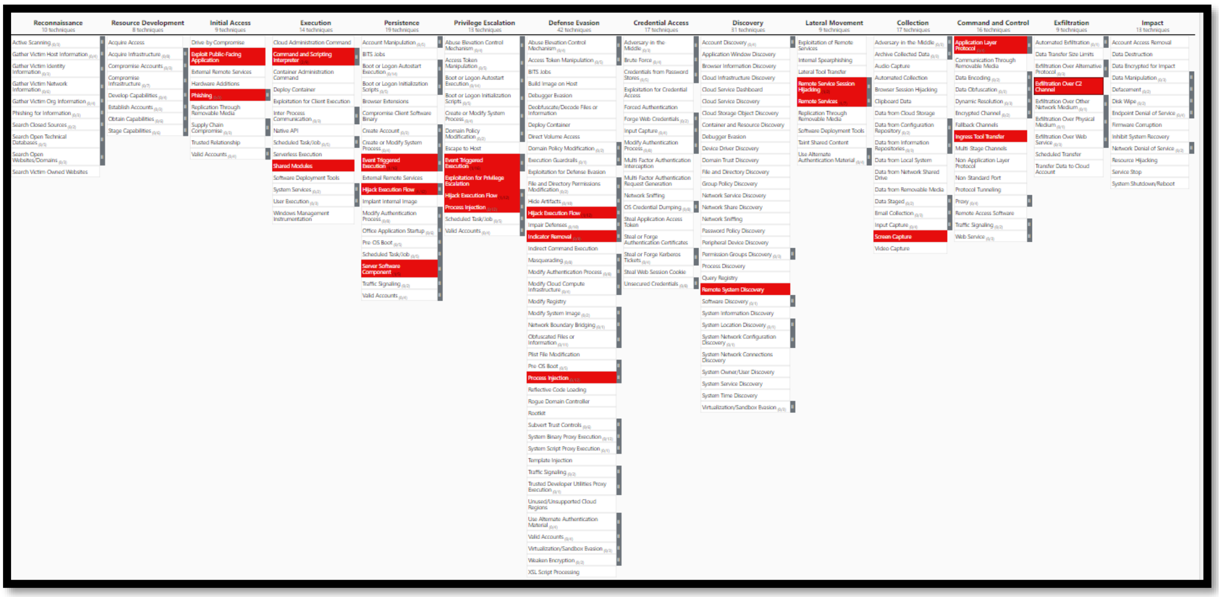
Affected Version

- MOVEit Transfer 2023.0.0 (15.0)
- MOVEit Transfer 2022.1.x (14.1)
- MOVEit Transfer 2022.0.x (14.0)
- MOVEit Transfer 2021.1.x (13.1)
- MOVEit Transfer 2021.0.x (13.0)
- MOVEit Transfer 2020.1.x (12.1)
- MOVEit Transfer 2020.0.x (12.0) or older

Fixed Version

- MOVEit Transfer 2023.0.2 (15.0.2)
- MOVEit Transfer 2022.1.6 (14.1.6)
- MOVEit Transfer 2022.0.5 (14.0.5)
- MOVEit Transfer 2021.1.5 (13.1.5)
- MOVEit Transfer 2021.0.7 (13.0.7)
- Special Patch (For MOVEit Transfer 12.1)
- Must upgrade to supported version (For MOVEit 12.0 and older)

CL0P Ransomware Group Tactics, Techniques and Procedures (TTPs)



Reconnaissance
10 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim Owned Websites

Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (0/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/7)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (0/6)
Stage Capabilities (0/6)

Initial Access
9 techniques
Drive by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/4)

Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (2/9)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter Process Communication (0/3)
Native API
Scheduled Task/Job (0/5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution (0/3)
Windows Management Instrumentation

Persistence
19 techniques
Account Manipulation (0/6)
BITS Jobs
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Create or Modify System Process (0/4)
Event Triggered Execution (1/16)
External Remote Services
Hijack Execution Flow (1/12)
Implant Internal Image
Modify Authentication Process (0/8)
Office Application Startup (0/6)
Pre OS Boot (0/5)
Scheduled Task/Job (0/5)
Server Software Component (1/5)
Traffic Signaling (0/2)
Valid Accounts (0/4)

Privilege Escalation
13 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/4)
Domain Policy Modification (0/2)
Escape to Host
Event Triggered Execution (1/16)
Exploitation for Privilege Escalation
Hijack Execution Flow (1/12)
Process Injection (0/12)
Scheduled Task/Job (0/5)
Valid Accounts (0/4)

Defense Evasion
42 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (0/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/10)
Hijack Execution Flow (1/12)
Impair Defenses (0/10)
Indicator Removal (0/9)
Indirect Command Execution
Masquerading (0/8)
Modify Authentication Process (0/8)
Modify Cloud Compute Infrastructure (0/4)
Modify Registry
Modify System Image (0/2)
Network Boundary Bridging (0/1)
Obfuscated Files or Information (0/11)
Plist File Modification
Pre OS Boot (0/5)
Process Injection (0/12)
Reflective Code Loading
Rogue Domain Controller
Rootkit
Subvert Trust Controls (0/6)
System Binary Proxy Execution (0/13)
System Script Proxy Execution (0/1)
Template Injection
Traffic Signaling (0/2)
Trusted Developer Utilities Proxy Execution (0/1)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (0/4)
Valid Accounts (0/4)
Virtualization/Sandbox Evasion (0/3)
Weaken Encryption (0/2)
XSL Script Processing

Credential Access
17 techniques
Adversary in the Middle (0/3)
Brute Force (0/4)
Credentials from Password Stores (0/5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Modify Authentication Process (0/8)
Multi Factor Authentication Interception
Multi Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/4)
Steal Web Session Cookie
Unsecured Credentials (0/6)

Discovery
31 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (0/3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (0/1)
System Information Discovery
System Location Discovery (0/1)
System Network Configuration Discovery (0/1)
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (0/3)

Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (1/2)
Remote Services (1/7)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)

Collection
17 techniques
Adversary in the Middle (0/3)
Archive Collected Data (0/3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (0/2)
Data from Information Repositories (0/3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Input Capture (0/4)
Screen Capture
Video Capture

Command and Control
16 techniques
Application Layer Protocol (0/4)
Communication Through Removable Media
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Ingress Tool Transfer
Multi Stage Channels
Non Application Layer Protocol
Non Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Software
Traffic Signaling (0/2)
Web Service (0/3)

Exfiltration
9 techniques
Automated Exfiltration (0/1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (0/3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)
Exfiltration Over Web Service (0/3)
Scheduled Transfer
Transfer Data to Cloud Account

Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (0/3)
Defacement (0/2)
Disk Wipe (0/2)
Endpoint Denial of Service (0/4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (0/2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

Figure 1: MITRE Attack Navigator (CL0P MOVEIT RANSOMWARE)

Initial Access

T1190: Exploit Public-Facing Application

The zero-day vulnerability CVE-2023-34362 affecting the MOVEit Transfer software is exploited by the CL0P ransomware group. It started from a SQL Injection to infiltrate the MOVEit Transfer web application.

T1566: Phishing

A large number of spear-phishing emails were sent to employees by CL0P actors to gain initial access.

Execution

T1059.001: Command and Scripting Interpreter: PowerShell

CL0P actors utilize SDBot as a backdoor to execute commands and functions in the compromised computer.

T1059.003: Command and Scripting Interpreter

TinyMet, a small open-source Meterpreter stager is used by CL0P actors to establish a reverse shell to their C2 server.

T1129: Shared Modules

CL0P actors use TrueBot to download additional modules.

Persistence

T1505.003: Server Software Component: Web Shell

LEMURLOOT, a web-shell curated specifically for MOVEit transfer software. CL0P actors utilize this web-shell to authenticates incoming http requests via hard-coded password and can run commands that will download files from the MOVEit Transfer system, extract its Azure system settings, retrieve detailed record information, create, insert, or delete a particular user.

T1546.011: Event Triggered Execution: Application Shimming

SDBot malware is used by CL0P for application shimming, to avoid detection and for persistence.

Privilege Escalation

T1068: Exploitation for Privilege Escalation

CL0P actors managed to gain access to MOVEit Transfer databases by escalating privilege within compromised network.

Defense Evasion

T1055: Process Injection

TrueBot is used by CL0P to load shell code.

T1070: Indicator Removal

CL0P actors delete traces of TrueBot malware after using it.

T1574.002: Hijack Execution Flow: DLL Side-Loading

TrueBot is used to load DLLs.

Discovery

T1018: Remote System Discovery

CL0P actors use Cobalt Strike to expand network access after gaining access to the Active Directory (AD) servers.

Lateral Movement

T1021.002: Remote Services: SMB/Windows Admin Shares

CL0P actors have been seen attempting to compromise an AD server using Server Message Block (SMB) vulnerabilities, followed by Cobalt Strike activities.

T1563.002: Remote Service Session Hijacking: RDP Hijacking

After gaining initial access, CL0P ransomware attackers have been detected utilizing Remote Desktop Protocol (RDP) to interact with affected systems.

Collection

T1113: Screen Capture

CL0P actors utilize TrueBot to capture screenshots in order to obtain sensitive information.

Command and Control

T1071: Application Layer Protocol

CL0P actors communicate with the Command and Control (C2) using the FlawedAmmyy remote access trojan (RAT).

T1105: Ingress Tool Transfer

CL0P actors are suspected of downloading additional malware components using the FlawedAmmyy remote access trojan (RAT). They employ SDBot to place copies of itself in removable drives and network shares.

Exfiltration

T1041: Exfiltration Over C2 Channel

CL0P actors exfiltrate data for C2 channels.

Mitigations

In order to respond to MOVEit ransomware, FIRMUS implies that all organizations execute the mitigation listed below to improve their security posture.

Conduct Compromise Assessment on all Organization's assets

Conducting a compromise assessment is a proactive and essential step for organizations to avoid ransomware and strengthen their overall cybersecurity posture. A compromise assessment involves examining an organization's network and systems to identify any signs of compromise or unauthorized activity. By conducting this, FIRMUS believes that current the organization will be more secure because vulnerabilities will be identified and resolved before getting exploited. Compromised Assessments will also check whether the organization is compromised or not by MOVEit ransomware or any other threats.

Reduce threat of Malicious actors using Remote Access Tool

FIRMUS recommend organizations to reduce the threat of Remote Access Tool by:

- Auditing Remote Access tools on the network to identify currently used and authorized software.
- Using security software to detect instances of remote access software that is only loaded in memory.
- Requiring authorized remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs), to be used exclusively from within your network.
- Examining logs for execution of remote access software to detect abnormal use of programs running as a portable executable.
- Blocking both inbound and outbound connections on common remote access software ports and protocols at the network perimeter.

Implement Application Control

It is important to manage and control the execution of software, including allowlisting remote access programs. Application controls should prevent portable versions of unauthorized remote access and other applications from being installed and executed. Any unlisted program execution will be blocked by a properly configured application allowlisting solution. Allowlisting is crucial because antivirus programs can overlook the execution of dangerous portable executables if the files use any combination of compression, encryption, or obfuscation.

Limit the use of RDP and other remote desktop services

If RDP is necessary, implement these best practices as stated below.

- Audit the network for systems using RDP
- Enforce account lockouts after a specified number of attempts.
- Close unused RDP ports.
- Apply Multi-Factor Authentication (MFA)
- Log all RDP login attempts.

Disable Command-line and scripting

FIRMUS recommend disabling both of these features to protect against Script-based attacks and to limit malicious command execution. By disabling these features, organizations can reduce their attack surface.

PowerShell should be restricted

Only allow specific users to use PowerShell by utilizing Group Policy.

Update PowerShell Core and Windows PowerShell

Update to the latest version and uninstall the earlier version. Logs from the latest PowerShell can help in incident response activities.

Check for unrecognized or new accounts added

Review domain controllers, workstations, active directories and servers for any new accounts and unrecognized accounts.

Audit accounts with administrative privileges

Organizations should audit all accounts with administrative privileges and configure access controls according to the principle of least privilege.

Minimizing the threat of Compromised Credentials

Place domain admin accounts in the protected users' group. Avoid storing plaintext credentials in scripts.

Implement time-based access for accounts

Applying this time-based access can limit the time window during which the user accounts are active. Specific time periods will reduce the risk of unauthorized access and misuse of accounts.

Maintain offline backups

Ensure that organizations have a regularly offline maintained backup to ensure that if they got infected by the ransomware, the offline backup would not be infected. It is best to backup daily or weekly.

Network Segmentation

Segment the network to prevent ransomware from getting spread. Segmentation can control the flow of traffic and restrict the ransomware from infecting further.

Implement a recovery plan

Implement a recovery plan to save several copies of sensitive or proprietary data and servers in a physically isolated, segregated, and secure location.

Apply Multi-factor Authentication (MFA)

The best practice is to apply MFA to all services that is possible, particularly on VPN, webmail and accounts that access critical systems.

Software, Firmware and Operating Systems are up to date

Ensure that all are up to date, especially the MOVEit version that is stated above. Prioritize patching known vulnerabilities exploited in internet facing systems.

Disable unused ports and hyperlinks

Disable both of these features to minimize the attack surface of the organization. Hyperlinks in received emails are very devastating especially when CL0P ransomware method of attack is spear-phishing.

Ensure all backups re encrypted and immutable

Ensure that all backups cannot be deleted or altered.

Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.

Implement a system that logs and reports all network traffic, including lateral movement activity, to aid in the detection of ransomware. Endpoint detection and response (EDR) tools are very good for detecting lateral connections since they know what network connections are typical and rare for each host. FIRMUS offers EDR services that can help organizations to detect vulnerabilities and existing threats inside the organization.

Summary

The MOVEit ransomware has taken the world by storm. It is everyone's responsibility to share awareness and protect each other from this notorious attack. FIRMUS hopes by sharing this information with the community, we could all protect our organizations and the South-East Asia region from this evolving cyber threat landscape. FIRMUS would also like to remind you that we offer EDR services and Compromised Assessments service which help strengthen an organization's security posture and at the same time, identify whether the organization has been compromised or not. Lastly, FIRMUS hopes that organizations check their current networks and assets by utilizing the Indicator of Compromise given. For non-cybersecurity organizations, feel free to contact FIRMUS for any inquiries. You Change The World, We Secure It.

Sources:

- https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft
- https://www.techrepublic.com/article/zero-day-moveit-vulnerability/
- https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/
- https://www.bleepingcomputer.com/news/security/exploit-released-for-moveit-rce-bug-used-in-data-theft-attacks/
- https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
- https://nvd.nist.gov/vuln/detail/CVE-2023-34362
- https://www.horizon3.ai/moveit-transfer-cve-2023-34362-deep-dive-and-indicators-of-compromise/