Threat Intelligence

Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft

June 2, 2023

Mandiant

Written by: Nader Zaveri, Jeremy Kennelly, Genevieve Stark, Matthew McWhirt, Dan Nutting, Kimberly Goody, Justin Moore, Joe Pisano, Zander Work, Peter Ukhanov, Juraj Sucik, Will Silverstone, Zach Schramm, Greg Blaum, Ollie Styles, Nicholas Bennett, Josh Murchie

---

UPDATE (June 9): On June 6, 2023, Mandiant merged UNC4857 into FIN11 based on targeting, infrastructure, certificate and data leak site (DLS) overlaps. This blog post has been updated to reflect the new attribution and supporting evidence.

Mandiant has observed wide exploitation of a zero-day vulnerability in the MOVEit Transfer secure managed file transfer software for subsequent data theft. This vulnerability was announced by Progress Software Corporation on May 31, 2023 and has been assigned CVE-2023-34362. Based on initial analysis from Mandiant incident response engagements, the earliest evidence of exploitation occurred on May 27, 2023 resulting in deployment of web shells and data theft. In some instances, data theft has occurred within minutes of the deployment of web shells. The seemingly opportunistic nature of this campaign and the subsequent data theft is consistent with activity we've seen from extortion actors; however, victims did not initially receive any ransom demands. Then on June 6, 2023, a post on the CL0P^_-LEAKS data leak site (DLS) claimed responsibility for this activity and threatened to post stolen data if victims did not pay an extortion fee. Mandiant initially attributed this activity to UNC4857, which has now been merged into FIN11 based on targeting, infrastructure, certificate, and DLS overlaps. This campaign has impacted organizations operating in a wide range of industries based in Canada, India, and the U.S., but the impact is almost certainly broader than Mandiant has directly observed.

- Following exploitation of the vulnerability, the threat actors are deploying a newly discovered LEMURLOOT web shell with filenames

POST requests made to the legitimate guestaccess.aspx file before interaction with the LEMURLOOT webshell, indicating SQL injection attacks were directed towards that file.

- We have observed LEMURLOOT samples with the filenames human2.aspx and _human2.aspx. Various samples with the name human2.aspx were uploaded to VirusTotal beginning on May 28, 2023. Samples of LEMURLOOT have been uploaded to public repositories from several additional countries—including Italy, Pakistan, and Germany—suggesting that UNC4857 has also impacted organizations in these nations.
- LEMURLOOT provides functionality tailored to execute on a system running MOVEit Transfer software, including the ability to generate commands to enumerate files and folders, retrieve configuration information, and create or delete a user with a hard-coded name. Initial analysis suggests that the LEMURLOOT web shell is being used to steal data previously uploaded by the users of individual MOVEit Transfer systems.
- Mandiant is aware of multiple cases where large volumes of files have been stolen from victims' MOVEit transfer systems. LEMURLOOT can also steal Azure Storage Blob information, including credentials, from the MOVEit Transfer application settings, suggesting that actors exploiting this vulnerability may be stealing files from Azure in cases where victims are storing appliance data in Azure Blob storage, although it is unclear if theft is limited to data stored in this way.
- In many cases, the scanning and exploitation leading to the delivery of LEMURLOOT was sourced from IP addresses in the range 5.252.188.0/22, however interaction with the web shell and data theft came from different systems. Many of the hosts used to support these second-stage operations hosted RDP services with certificates generated between May 19 and 22, which is suggestive of when this infrastructure may have been staged.

Analysis of this intrusion activity is ongoing and will be reflected on the CAMP.23.037 page within Mandiant Advantage; we will also update this blog post if and when additional information becomes available. Along with this blog post, Mandiant has produced a detailed MOVEit Containment and Hardening guide to assist organizations with this event. The document contains guidance on the following key items:

- Containment Measures
- Application and Infrastructure Hardening
- Logging and Hunting Recommendations

LEMURLOOT Analysis

LEMURLOOT is a web shell written in C# tailored to interact with the MOVEit Transfer platform. The malware authenticates incoming

system settings, retrieve detailed record information, create and insert a particular user, or delete this same user. Data returned to the system interacting with LEMURLOOT is gzip compressed.

Authentication and Database Connection

LEMURLOOT first checks if an incoming HTTP request contains the header field X-siLock-Comment and a corresponding 36-character GUID-formatted value, which varies across samples. It effectively uses this GUID as a password and returns an HTTP 404 status code to clients that do not pass the expected header field and value.

If the correct password is passed to LEMURLOOT, it sends a header response X-siLock-Comment and value comment, indicating the connection is successful and can accept tasking. The malware connects to a SQL server from the executing host using the settings retrieved using SystemSettings.DatabaseSettings(). It then processes data received from the connecting client, parsing expected commands from the following HTTP header fields: X-siLock-Step1, X-siLock-Step2, and X-siLock-Step3.

X-siLock-Step1 Command Sequence

1. If the value of the header field X-siLock-Step1 is -1, LEMURLOOT retrieves and returns the Azure system settings from MOVEit Transfer, including the configured Azure Blog storage account, and its associated key and container (AzureBlobStorageAccount, AzureBlobKey, and AzureBlobContainer). It then performs SQL queries to retrieve files, file size, folders, file owners, and institution name data. The resulting data is gzip compressed and returned to the client interacting with LEMURLOOT.
2. If the X-siLock-Step1 header field value is -2, it deletes a user account with the LoginName and RealName set to "Health Check Service" using the SQL command in Figure 1. Note that this user is inserted using the following functionality.

```
Delete FROM users WHERE RealName='Health Check Service'
```

Figure 1: MOVEit user deletion command

X-siLock-Step2 and X-siLock-Step3 Command Sequence

1. If the value of header field X-siLock-Step1 is neither -1 or -2, the malware parses the values from header fields X-siLock-Step2 and X-siLock-Step3 and stores them in variables named fileid and folderid, respectively.
2. If the values of fileid and folderid are not null, the malware retrieves the file from the local MOVEit Transfer system with these same values, gzip compresses it, and returns it to the connecting client.
3. If the fileid and folderid variables are null, LEMURLOOT attempts to identify an existing account with permission level “30” and InstID = the value set from "X-siLock-Step1" otherwise it creates a new account with a randomly generated username and with LoginName and RealName values set to "Health Check Service" This account is inserted it into an active MOVEit application session.

Attribution

Mandiant initially attributed this activity to UNC4857, which has now been merged into FIN11 based on targeting, infrastructure, certificate, and data leak site (DLS) overlaps. The activity is reminiscent of prior mass exploitation events targeting file transfer software and leading to FIN11-attributed data theft extortion via the CL0P^_- LEAKS data leak site (DLS).

- FIN11-attributed data theft extortion has occurred following exploitation of multiple other file transfer systems. From late 2020 to early 2021, threat actors exploited multiple zero-day vulnerabilities in Accellion's legacy File Transfer Appliance (FTA) to install the DEWMODE web shell. Similarly, in early 2023, threat actors exploited GoAnywhere Managed File Transfer (MFT) vulnerability CVE-2023-0669.
- Mandiant has identified numerous overlaps in the ISPs, netblocks, and IP addresses used in this campaign and historical FIN11 operations.
  - Notably, an IP address that was attempting exploitation of CVE-2023-34362 was used by FIN11 as early as mid-January 2023. At the time this system was first used by FIN11 it was hosting an RDP service on TCP port 3389. This service was still active and presenting the same x509 certificate when UNC4857's use of the system began.
- On June 5, 2023, Bleeping Computer claimed that someone affiliated with the CLOP ransomware group stated that they were behind incidents in which the MOVEit transfer system vulnerability was exploited for data theft. On June 6, 2023, a post on the CL0P^_- LEAKS DLS claimed responsibility for this activity (Figure 2).

Implications

Mandiant routinely observes threat actors with varying motivations targeting sensitive data. For example, state-sponsored threat actors have demonstrated ongoing interest in targeting entities with policy research, military and government files, intellectual property, and personally identifiable information. Cyber criminals can also directly monetize stolen data via extortion operations, post it for sale on underground forums, or leverage it in secondary operations such as business email compromise.

Mandiant has not yet directly observed any extortion emails sent to confirmed victims. However, in prior cases where FIN11 exploited vulnerabilities in secure file transfer systems, the threat actors did not send extortion emails demanding a payment in return for not publishing the data on the CL0P^_- LEAKS DLS until several weeks later. It is plausible that FIN11 delayed sending the ransom emails in an attempt to extend the amount of time that the zero-day vulnerabilities remained undetected and thus increase the number of victims and/or capacity to negotiate with a large number of victims simultaneously. Although the CLOP brand has posted to their DLS suggesting victims should initiate contact, if their TTPs remain consistent it is likely that the group will begin to initiate contact with some impacted organizations in the coming days and/or weeks.

Detections

The following YARA rules are not intended to be used on production systems or to inform blocking rules without first being validated through an organization's own internal testing processes to ensure appropriate performance and limit the risk of false positives. These rules are intended to serve as a starting point for hunting efforts to identify LEMURLOOT payloads; however, they may need adjustment over time if the malware family changes.

```
rule M_Webshell_LEMURLOOT_DLL_1 {
    meta:
        disclaimer = "This rule is meant for hunting and is
        description = "Detects the compiled DLLs generated
        sample = "c58c2c2ea608c83fad9326055a8271d47d8246dc9
        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
```

```
        $s5 = "attachment; filename={0}" wide
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x0
        filesize < 15KB and
        $net and
        (
            ($human and 2 of ($s*)) or
            (3 of ($s*))
        )
}
```

YARA rule for detecting compiled LEMURLOOT DLLs

```
rule M_Webshell_LEMURLOOT_1 {
    meta:
        disclaimer = "This rule is meant for hunting and is
        description = "Detects the LEMURLOOT ASP.NET script
        md5 = "b69e23cd45c8ac71652737ef44e15a34"
        sample = "cf23ea0d63b4c4c348865cefd70c35727ea8c82ba
        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*))
        )
}
```

YARA rule for detecting LEMURLOOT ASP.NET scripts

Indicators

MD5	SHA256
00c6bce35c40ce1601aa06c4e808c0f1	38e69f4a6d2e81f28ed2dc
04b474e8db353d368e2d791ba5dee6d6	3a977446ed70b02864ef8
11eadcf3f1bc9b0ed6994c3ede299ce8	b1c299a9fe6076f370178d

359a1141a79480555aa996fd6d9e4af1	702421bcee1785d93271d3
44d8e68c7c4e04ed3adacb5a88450552	387cee566aedbafa8c114e
45685c190c91ebe0966e8a0aeca31280	4359aead416b1b2df8ad9e
538d6e172d18d4cebeac211873779ba5	daaa102d82550f9764288
67fca3e84490dfdddf72e9ba558b589a	6015fed13c5510bbb89b0a
7d5e5537c5346d764f067f66cca426ba	9d1723777de67bc7e11678c
8cd6c75e6160b90de2a52c967b3d4846	c56bcb513248885673645f
8d88e451e39506ae258f3aa99da8db9a	0ea05169d111415903a109
911230b5dca1c43f6d22e65c66b0f6b1	d49cf23d83b2743c573ba3
96d467fd9663cf2e5572f8529e54f13e	5b566de1aa4b2f79f579cd
9f3c306dabc3f349b343251f4443412c	f0d85b65b9f6942c752712
a85299f78ab5dd05e7f0f11ecea165ea	fe5f8388ccea7c548d587d
b1bdad086567efd202babf56eac17e1d	9e89d9f045664996067a0
b52e56bfc03878cc5cb9eae9d3896808	ea433739fb708f5d25c937
b69e23cd45c8ac71652737ef44e15a34	cf23ea0d63b4c4c348865
bf7c1dd613101c0a95027249a5fcb759	2413b5d0750c23b07999e
c2db1091eb7bac28461877f736d86d83	348e435196dd795e1ec311
d71a6b5ae3d89dc33cbbb6877e493d52	b9a0baf82feb08e42fa6ca
ddd95f1c76a1d50b997b2e64274f386a	a1269294254e958e0e58fc
e9a5f0c7656329ced63d4c8742da51b4	48367d94ccb4411f15d7ef9
eea4d43f9e3700ebcd61405776eb249a	d477ec94e522b8d741f46b
fbba113d1d121220fa43f90b3a20870a	3ab73ea9aebf271e5f3ed7

LEMURLOOT Samples

Mandiant Security Validation Actions

Organizations can validate their security controls using the following actions with Mandiant Security Validation.

VID	Name
A106-469	Malicious File Transfer - LEMURLOOT, Download, Variant #1
A106-467	Malicious File Transfer - LEMURLOOT, Download, Variant #2
A106-472	Malicious File Transfer - LEMURLOOT, Download, Variant #3
A106-468	Web Application Vulnerability - FIN11, MOVEit Transfer SQL Injection CVE-2023-34362
A106-470	Web Shell Activity - FIN11, LEMURLOOT, Delete Database User
A106-471	Web Shell Activity - FIN11, LEMURLOOT, Retrieve File
S100-281	Malicious Activity Scenario - Campaign 23-037, FIN11 Utilizing a Critical Vulnerability in MOVEit Transfer

Acknowledgements

Beyond the listed authors are dozens of consultants and analysts who have already been working to help our clients with cases related to exploitation of CVE-2023-34362. We would also like to specifically thank Raymond Leong from the Mandiant FLARE team for his invaluable support.

Posted in Threat Intelligence

Related articles

Threat Intelligence

Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives

By Google Threat Intelligence Group • 10-minute read

Threat Intelligence

Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)

By Mandiant • 19-minute read

Threat Intelligence

How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends

By Mandiant • 10-minute read

Threat Intelligence

capa Explorer Web: A Web-Based Tool for Program Capability Analysis

By Mandiant • 6-minute read