Product ID: AA23_158A

June 7, 2023

#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

SUMMARY

Note: this joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known CL0P ransomware IOCs and TTPs identified through FBI investigations as recently as June 2023.

According to open source information, beginning on May 27, 2023, CL0P Ransomware Gang, also known as TA505, began exploiting a previously unknown SQL injection vulnerability (CVE-2023-34362) in Progress Software's managed file transfer (MFT) solution known as MOVEit Transfer. Internet-facing MOVEit Transfer web applications were infected with a web shell named LEMURLOOT, which was then used to steal data from underlying MOVEit Transfer databases. In similar spates of activity, TA505 conducted zero-day-exploit-driven campaigns against Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, and Fortra/Linoma GoAnywhere MFT servers in early 2023.

Actions to take today to mitigate cyber threats from CL0P ransomware:

- Take an inventory of assets and data, identifying authorized and unauthorized devices and software.
- Grant admin privileges and access only when necessary, establishing a software allow list that only executes legitimate applications.
- Monitor network ports, protocols, and services, activating security configurations on network infrastructure devices such as firewalls and routers.
- Regularly patch and update software and applications to their latest versions, and conduct regular vulnerability assessments.

U.S. organizations: To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Report@cisa.dhs.gov.

FBI and CISA encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of CL0P ransomware and other ransomware incidents.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 13. See MITRE ATT&CK for Enterprise for all referenced tactics and techniques.

Appearing in February 2019, and evolving from the CryptoMix ransomware variant, CL0P was leveraged as a Ransomware as a Service (RaaS) in large-scale spear-phishing campaigns that used a verified and digitally signed binary to bypass system defenses. CL0P was previously known for its use of the 'double extortion' tactic of stealing and encrypting victim data, refusing to restore victim access and publishing exfiltrated data on Tor via the CL0P^_-LEAKS website. In 2019, TA505 actors leveraged CL0P ransomware as the final payload of a phishing campaign involving a macro-enabled document that used a Get2 malware dropper for downloading SDBot and FlawedGrace. In recent campaigns beginning 2021, CL0P preferred to rely mostly on data exfiltration over encryption.

Beyond CL0P ransomware, TA505 is known for frequently changing malware and driving global trends in criminal malware distribution. Considered to be one of the largest phishing and malspam distributors worldwide, TA505 is estimated to have compromised more than 3,000 U.S.-based organizations and 8,000 global organizations.

TA505 has operated:

- A RaaS and has acted as an affiliate of other RaaS operations,
- As an initial access broker (IAB), selling access to compromised corporate networks,
- As a customer of other IABs,
- And as a large botnet operator specializing in financial fraud and phishing attacks.

In a campaign from 2020 to 2021, TA505 used several zero-day exploits to install a web shell named DEWMODE on internet-facing Accellion FTA servers. Similarly, the recent exploitation of MOVEit Transfer, a SQL injection vulnerability was used to install the web shell, which enabled TA505 to execute operating system commands on the infected server and steal data.

In late January 2023, the CL0P ransomware group launched a campaign using a zero-day vulnerability, now catalogued as CVE-2023-0669, to target the GoAnywhere MFT platform. The group claimed to have exfiltrated data from the GoAnywhere MFT platform that impacted approximately 130 victims over the course of 10 days. Lateral movement into the victim networks from the GoAnywhere MFT was not identified, suggesting the breach was limited to the GoAnywhere platform itself. Over the next several weeks, as the exfiltrated data was parsed by the group, ransom notes were sent to upper-level executives of the victim companies, likely identified through open source research. The ransom notes threatened to publish the stolen files on the CL0P data leak site if victims did not pay the ransom amount.

Figure 1: CL0P Ransom Note

```
Hello, this is the CL0P hacker group. As you may know, we recently carried
out a hack, which was reported in the news on site [redacted].

We want to inform you that we have stolen important information from your
GoAnywhere MFT resource and have attached a full list of files as evidence.

We deliberately did not disclose your organization and wanted to negotiate
with you and your leadership first. If you ignore us, we will sell your
information on the black market and publish it on our blog, which receives
30-50 thousand unique visitors per day. You can read about us on [redacted]
by searching for CL0P hacker group.

You can contact us using the following contact information:

unlock@rsv-box[.]com

and

unlock@support-mult[.]com
```

CL0P's toolkit contains several malware types to collect information, including the following:

- **FlawedAmmyy/FlawedGrace remote** access trojan (RAT) collects information and attempts to communicate with the Command and Control (C2) server to enable the download of additional malware components [T1071], [T1105].
- **SDBot** RAT propagates the infection, exploiting vulnerabilities and dropping copies of itself in removable drives and network shares [T1105]. It is also capable of propagating when shared though peer-to-peer (P2P) networks. SDBot is used as a backdoor [T1059.001] to enable other commands and functions to be executed in the compromised computer. This malware uses application shimming for persistence and to avoid detection [T1546.011].
- **Truebot** is a first-stage downloader module that can collect system information and take screenshots [T1113], developed and attributed to the Silence hacking group. After connecting to the C2 infrastructure, Truebot can be instructed to load shell code [T1055] or DLLs [T1574.002], download additional modules [T1129], run them, or delete itself [T1070]. In the case of TA505, Truebot has been used to download FlawedGrace or Cobalt Strike beacons.
- Cobalt Strike is used to expand network access after gaining access to the Active Directory (AD) server [T1018].
- **DEWMODE** is a web shell written in PHP designed to target Accellion FTA devices and interact with the underlying MySQL database, and is used to steal data from the compromised device [1505.003].

- **LEMURLOOT** is a web shell written in C# designed to target the MOVEit Transfer platform. The web shell authenticates incoming http requests via a 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. When responding to the request, the web shell returns data in a gzip compressed format.

CVE-2023-34362 MOVEIT TRANSFER VULNERABILITY

MOVEit is typically used to manage an organization's file transfer operations and has a web application that supports MySQL, Microsoft SQL Server, and Azure SQL database engines. In May 2023, the CL0P ransomware group exploited a SQL injection zero-day vulnerability CVE-2023-34362 to install a web shell named LEMURLOOT on MOVEit Transfer web applications [T1190] [1]. The web shell was initially observed with the name `human2.aspx` in an effort to masquerade as the legitimate `human.aspx` file present as part of MOVEit Transfer software. Upon installation, the web shell creates a random 36 character password to be used for authentication. The web shell interacts with its operators 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. After authenticating with the web shell, operators pass commands to the web shell that can:

- Retrieve Microsoft Azure system settings and enumerate the underlying SQL database.
- Store a string sent by the operator and then retrieve a file with a name matching the string 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.'

Progress Software announced the discovery of CVE-2023-34362 MOVEit Transfer vulnerability and issued guidance on known affected versions, software upgrades, and patching. Based on evidence of active exploitation, CISA added this vulnerability to the Known Exploited Vulnerabilities (KEVs) Catalog on June 2, 2023. This MOVEit Transfer critical vulnerability exploit impacts the following versions of the software [2]:

- MOVEit Transfer 2023.0.0
- MOVEit Transfer 2022.1.x
- MOVEit Transfer 2022.0.x
- MOVEit Transfer 2021.1.x
- MOVEit Transfer 2021.0.x
- MOVEit Transfer 2020.1.x
- MOVEit Transfer 2020.0.x

Due to the speed and ease TA505 has exploited this vulnerability, and based on their past campaigns, FBI and CISA expect to see widespread exploitation of unpatched software services in both private and public networks. For IOCs related to the MOVEit campaign, see table 2.

DETECTION METHODS

Below, are open source deployable YARA rules that may be used to detect malicious activity of the MOVEit Transfer Zero Day Vulnerability. For more information, visit GitHub or the resource section of this CSA. [1] [3]:

```
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 =
"cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45x"
        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_moveit_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/44ce8556f798b7f6a7574148b679c643"
        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_moveit_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/44ce8556f798b7f6a7574148b679c643"
        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
}
```

If a victim rebuilds the web server but leaves the database intact, the CL0P user accounts will still exist and can be used for persistent access to the system.

Victims can use the following SQL query to audit for active administrative accounts, and should validate that only intended accounts are present.

```
SELECT * FROM [<database name>].[dbo].[users] WHERE Permission=30 AND
Status='active' and Deleted='0'
```

MOVEit Campaign Indicators of Compromise

Files	Hash
LEMURLOOT Web Shell e.g. `human2.aspx`	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

GoAnywhere Campaign Indicators of Compromise

Files	Hash	Description
larabqFa.exe Qboxdv.dll	0e3a14638456f4451fe8d76fdc04e591fba942c2f16da31857ca66293a58a4c3	Truebot
%TMP%\7ZipSfx.000\Zoom.exe	1285aa7e6ee729be808c46c069e30a9ee9ce34287151076ba81a0bea0508ff7e	Spawns a PowerShell subprocess which executes a malicious DLL file

%TMP%\7ZipSfx.000\ANetDiag.dll	2c8d58f439c708c28ac4ad4a0e9f93046cf076fc6e5ab1088e8943c0909acbc4	Obfuscated malware which also uses long sleeps and debug detection to evade analysis
AVICaptures.dll	a8569c78af187d603eecdc5faec860458919349eef51091893b705f466340ecd	Truebot
kpdphhajHbFerUr.exe gamft.dll	c042ad2947caf4449295a51f9d640d722b5a6ec6957523ebf68cddb87ef3545c	Truebot
dnSjujahur.exe Pxaz.dll	c9b874d54c18e895face055eeb6faa2da7965a336d70303d0bd6047bec27a29d	Truebot
7ZSfxMod_x86.exe ZoomInstaller.exe Zoom.exe	d5bbcaa0c3eeea17f12a5cc3dbcaffff423d00562acb694561841bcfe984a3b7	Fake Zoom installer - Truebot
update.jsp	eb9f5cbe71f9658d38fb4a7aa101ad40534c4c93ee73ef5f6886d89159b0e2c2	Java Server Pages (JSP) web shell with some base64 obfuscation
%TMP%\<folder>\extracted_at_0xe5c8f00.exe	f2f08e4f108aaffaadc3d11bad24abdd625a77e0ee9674c4541b562c78415765	Employs sandbox detection and string obfuscation - appears to be a collection of C# hack tools
UhfdkUSwkFKedUUi.exe gamft.dll	ff8c8c8bfba5f2ba2f8003255949678df209dbff95e16f2f3c338cfa0fd1b885	Truebot

Email Address	Description
unlock@rsv-box[.]com	CL0P communication email
unlock@support-multi[.]com	CL0P communication email
rey14000707@gmail[.]com	Login/Download
gagnondani225@gmail[.]com	Email

Malicious Domain
http://hiperfdhaus[.]com
http://jirostrogud[.]com
http://qweastradoc[.]com
http://qweastradoc[.]com/gate.php
http://connectzoomdownload[.]com/download/ZoomInstaller.exe
https://connectzoomdownload[.]com/download/ZoomInstaller.exe

http://zoom[.]voyage/download/Zoom.exe
http://guerdofest[.]com/gate.php

Certificate Name	Status	Date Valid	Thumbprint	Serial Number
Savas Investments PTY LTD	Valid Issuer: Sectigo Public Code Signing CA R36	10/7/2022 - 10/7/2023	8DCCF6AD21A58226521 E36D7E5DBAD133331C181	00-82-D2-24-32-3E-FA-65-06-0B-64- 1F-51-FA-DF-EF-02

MOVEit Campaign Infrastructure IP Addresses May/June 2023	GoAnywhere Campaign Infrastructure IP Addresses January/February 2023
104.194.222[.]107	100.21.161[.]34
138.197.152[.]201	104.200.72[.]149
146.0.77[.]141	107.181.161[.]207
146.0.77[.]155	141.101.68[.]154
146.0.77[.]183	141.101.68[.]166
148.113.152[.]144	142.44.212[.]178
162.244.34[.]26	143.31.133[.]99
162.244.35[.]6	148.113.159[.]146
179.60.150[.]143	148.113.159[.]213
185.104.194[.]156	15.235.13[.]184
185.104.194[.]24	15.235.83[.]73
185.104.194[.]40	162.158.129[.]79
185.117.88[.]17	166.70.47[.]90
185.162.128[.]75	172.71.134[.]76
185.174.100[.]215	173.254.236[.]131
185.174.100[.]250	185.104.194[.]134
185.181.229[.]240	185.117.88[.]2
185.181.229[.]73	185.174.100[.]17
185.183.32[.]122	185.33.86[.]225
185.185.50[.]172	185.33.87[.]126
188.241.58[.]244	185.80.52[.]230
193.169.245[.]79	185.81.113[.]156

194.33.40[.]103	192.42.116[.]191
194.33.40[.]104	195.38.8[.]241
194.33.40[.1]64	198.137.247[.]10
198.12.76[.]214	198.199.74[.]207
198.27.75[.]110	198.199.74[.]207:1234/update.jsp
206.221.182[.]106	198.245.13[.]4
209.127.116[.]122	20.47.120[.]195
209.127.4[.]22	208.115.199[.]25
209.222.103[.]170	209.222.98[.]25
209.97.137[.]33	213.121.182[.]84
45.227.253[.]133	216.144.248[.]20
45.227.253[.]147	23.237.114[.]154
45.227.253[.]50	23.237.56[.]234
45.227.253[.]6	3.101.53[.]11
45.227.253[.]82	44.206.3[.]111
45.56.165[.]248	45.182.189[.]200
5.149.248[.]68	45.182.189[.]228
5.149.250[.]74	45.182.189[.]229
5.149.250[.]92	5.149.250[.]90
5.188.86[.]114	5.149.252[.]51
5.188.86[.]250	5.188.206[.]76
5.188.87[.]194	5.188.206.76[:]8000/se1.dll
5.188.87[.]226	5.34.178[.]27
5.188.87[.]27	5.34.178[.]28
5.252.23[.]116	5.34.178[.]30
5.252.25[.]88	5.34.178[.]31
5.34.180[.]205	5.34.180[.]48
62.112.11[.]57	50.7.118[.]90
62.182.82[.]19	54.184.187[.]134
62.182.85[.]234	54.39.133[.]41
66.85.26[.]215	63.143.42[.]242
66.85.26[.]234	68.156.159[.]10
66.85.26[.]248	74.218.67[.]242
79.141.160[.]78	76.117.196[.]3
79.141.160[.]83	79.141.160[.]78
84.234.96[.]104	79.141.161[.]82
84.234.96[.]31	79.141.173[.]94
89.39.104[.]118	81.56.49[.]148
89.39.105[.]108	82.117.252[.]141
91.202.4[.]76	82.117.252[.]142

91.222.174[.]95	82.117.252[.]97
91.229.76[.]187	88.214.27[.]100
93.190.142[.]131	88.214.27[.]101
	91.222.174[.]68
	91.223.227[.]140
	92.118.36[.]210
	92.118.36[.]213
	92.118.36[.]249
	96.10.22[.]178
	96.44.181[.]131
	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

MITRE ATT&CK TECHNIQUES

See tables below for referenced CL0P tactics and techniques used in this advisory.

Table 1. ATT&CK Techniques for Enterprise: Initial Access

Initial Access		
Technique Title	**ID**	**Use**
Exploit Public-Facing Application	T1190	CL0P ransomware group exploited the zero-day vulnerability CVE-2023-34362 affecting MOVEit Transfer software; begins with a SQL injection to infiltrate the MOVEit Transfer web application.
Phishing	T1566	CL0P actors send a large volume of spear-phishing emails to employees of an organization to gain initial access.

Table 2. ATT&CK Techniques for Enterprise: Execution

Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter: PowerShell	T1059.001	CL0P actors use SDBot as a backdoor to enable other commands and functions to be executed in the compromised computer.
Command and Scripting Interpreter	T1059.003	CL0P actors use TinyMet, a small open-source Meterpreter stager to establish a reverse shell to their C2 server.
Shared Modules	T1129	CL0P actors use Truebot to download additional modules.

Table 3. ATT&CK Techniques for Enterprise: Persistence

Persistence		
Technique Title	**ID**	**Use**
Server Software Component: Web Shell	T1505.003	DEWMODE is a web shell designed to interact with a MySQL database, and is used to exfiltrate data from the compromised network.
Event Triggered Execution: Application Shimming	T1546.011	CL0P actors use SDBot malware for application shimming for persistence and to avoid detection.

Table 4. ATT&CK Techniques for Enterprise: Privilege Escalation

Privilege Escalation		
Technique Title	**ID**	**Use**
Exploitation for Privilege Escalation	T1068	CL0P actors were gaining access to MOVEit Transfer databases prior to escalating privileges within compromised network.

Table 5. ATT&CK Techniques for Enterprise: Defense Evasion

Defense Evasion		
Technique Title	**ID**	**Use**
Process Injection	T1055	CL0P actors use Truebot to load shell code.
Indicator Removal	T1070	CL0P actors delete traces of Truebot malware after it is used.
Hijack Execution Flow: DLL Side-Loading	T1574.002	CL0P actors use Truebot to side load DLLs.

Table 6. ATT&CK Techniques for Enterprise: Discovery

Discovery		
Technique Title	**ID**	**Use**
Remote System Discovery	T1018	CL0P actors use Cobalt Strike to expand network access after gaining access to the Active Directory (AD) servers.

Table 7. ATT&CK Techniques for Enterprise: Lateral Movement

Lateral Movement		
Technique Title	**ID**	**Use**
Remote Services: SMB/Windows Admin Shares	T1021.002	CL0P actors have been observed attempting to compromise the AD server using Server Message Block (SMB) vulnerabilities with follow-on Cobalt Strike activity.
Remote Service Session Hijacking: RDP Hijacking	T1563.002	CL0P ransomware actors have been observed using Remote Desktop Protocol (RDP) to interact with compromised systems after initial access.

Table 8. ATT&CK Techniques for Enterprise: Collection

Collection		
Technique Title	**ID**	**Use**
Screen Capture	T1113	CL0P actors use Truebot to take screenshots in effort to collect sensitive data.

Table 9. ATT&CK Techniques for Enterprise: Command and Control

Command and Control		
Technique Title	**ID**	**Use**
Application Layer Protocol	T1071	CL0P actors use FlawedAmmyy remote access trojan (RAT) to communicate with the Command and Control (C2).
Ingress Tool Transfer	T1105	CL0P actors are assessed to use FlawedAmmyy remote access trojan (RAT) to the download of additional malware components. CL0P actors use SDBot to drop copies of itself in removable drives and network shares.

Table 10. ATT&CK Techniques for Enterprise: Exfiltration

Exfiltration		
Technique Title	**ID**	**Use**
Exfiltration Over C2 Channel	T1041	CL0P actors exfiltrate data for C2 channels.

MITIGATIONS

The authoring agencies recommend organizations implement the mitigations below to improve their organization's security posture in response to threat actors' activity. These

mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats and TTPs. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections to reduce the risk of compromise by CL0P ransomware.

- **Reduce threat of malicious actors** using remote access tools by:
    - **Auditing remote access tools** on your network to identify currently used and/or authorized software.
    - **Reviewing logs for execution of remote access software** to detect abnormal use of programs running as a portable executable [CPG 2.T].
    - **Using security software** to detect instances of remote access software only being loaded in memory.
    - **Requiring authorized remote access solutions** only be used from within your network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
    - **Blocking both inbound and outbound connections** on common remote access software ports and protocols at the network perimeter.
- **Implement application controls** to manage and control execution of software, including allowlisting remote access programs.
    - Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.
- **Strictly limit the use of RDP and other remote desktop services**. If RDP is necessary, rigorously apply best practices, for example [CPG 2.W]:
    - Audit the network for systems using RDP.
    - Close unused RDP ports.
    - Enforce account lockouts after a specified number of attempts.
    - Apply phishing-resistant multifactor authentication (MFA).

- Log RDP login attempts.

- **Disable command-line and scripting** activities and permissions [CPG 2.N].
- **Restrict the use of PowerShell**, using Group Policy, and only grant to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows operating systems (OSs) should be permitted to use PowerShell [CPG 2.E].
- **Update Windows PowerShell or PowerShell Core** to the latest version and uninstall all earlier PowerShell versions. Logs from Windows PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities [CPG 1.E, 2.S, 2.T].
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 4.C].
- **Audit user accounts with administrative privileges** and configure access controls according to the principle of least privilege [CPG 2.E].
- **Reduce the threat of credential compromise** via the following:
  - **Place domain admin accounts in the protected users' group** to prevent caching of password hashes locally.
  - Refrain from storing plaintext credentials in scripts.
- **Implement time-based access for accounts** set at the admin level and higher [CPG 2.A, 2.E].

In addition, the authoring authorities of this CSA recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the impact and risk of compromise by ransomware or data extortion actors:

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- **Maintain offline backups of data** and regularly maintain backup and restoration (daily or weekly at minimum). By instituting this practice, an organization limits the severity of disruption to its business practices [CPG 2.R].
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) **to comply** with National Institute for Standards and Technology (NIST) standards for developing and managing password policies.

- Use longer passwords consisting of at least eight characters and no more than 64 characters in length [CPG 2.B].
- Store passwords in hashed format using industry-recognized password managers.
- Add password user "salts" to shared login credentials.
- Avoid reusing passwords [CPG 2.C].
- Implement multiple failed login attempt account lockouts [CPG 2.G].
- Disable password "hints."
- Refrain from requiring password changes more frequently than once per year. **Note:** NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
- Require administrator credentials to install software.

- **Require multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems [CPG 2.H].
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement [CPG 2.F].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host [CPG 3.A].
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Disable unused ports** [CPG 2.V].
- **Consider adding an email banner to emails** received from outside your organization [CPG 2.M].
- **Disable hyperlinks** in received emails.

- **Ensure all backup data is encrypted, immutable** (i.e., ensure backup data cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R].

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, FBI and CISA recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring authorities of this CSA recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see table 2).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

RESOURCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.

REFERENCE

[1] Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft | Mandiant

[2] MOVEit Transfer Critical Vulnerability (May 2023) - Progress Community

[3] MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response (huntress.com)

REPORTING

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with CL0P group actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file. The FBI and CISA do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to a local FBI Field Office, report the incident to the FBI Internet Crime Complaint Center (IC3) at ic3.gov, or CISA at cisa.gov/report.

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. CISA and the FBI do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA or the FBI.