US Coast Guard Cyber Command
Maritime Cyber Alert 03-23

October 4, 2023

Information Sharing Protocol: TLP: CLEAR (https://www.us-cert.gov/tlp)

Threat from Cl0p Ransomware Group

Summary:

The Coast Guard is observing malicious activity, linked to the Cl0p Ransomware Group, affecting the Marine Transportation System (MTS) and entities that directly support the MTS. Cl0p began leaking lists of the victims they've exploited on the internet in June 2023, which have grown to include compromised data from approximately 400 victims. Many of these victims are either direct members of the MTS or provide critical services to the maritime industry.

Background:

Cl0p first appeared in 2019 and has operated both as a Ransomware-as-a-Service (RaaS) and initial access broker that sells access to compromised corporate networks. Cl0p is known for leveraging a double extortion scheme where they demand a ransom payment for stolen data and threaten to make the data public if the entity refuses to pay.

Targeted Applications & Systems:

Beginning in late May 2023, Cl0p began exploiting a previously unknown vulnerability (CVE-2023-34362) in Progress Software Corporation (PSC)'s managed file transfer solution known as Progress® MOVEit® Transfer. By exploiting internet-accessible MOVEit Transfer web applications, Cl0p was able to gain unauthorized access to underlying MOVEit Transfer databases and exfiltrate files transferred using MOVEit Transfer software.

The MOVEit Transfer vulnerability affects the following versions of the MOVEit Transfer software:

- 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

Cl0p Tactics:

Below are Cl0P tactics referenced by MITRE ATT&CK®[1] techniques, which are linked to previous Cl0P attacks (https://attack.mitre.org/techniques/enterprise):

- **T1190: Exploit Public-Facing Application**
  - Cl0p is exploiting a previously unknown vulnerability (CVE-2023-34362) affecting MOVEit Transfer software, which begins with an SQL injection in the public-facing MOVEit Transfer web application.
- **T1041: Exfiltration Over C2 Channel**
  - Once they compromise the software, Cl0p threat actors exfiltrate data from compromised systems over command-and-control channel.

Mitigation Measures:

The recommended mitigating strategies below may be used to decrease Cl0p's opportunity for exploitation.

- **Mitigate the Opportunity for Attacks**
  - **Patch MOVEit Transfer Software**
    - PSC has released a series of security patches to remediate the MOVEit Transfer vulnerabilities. Timely patching is critical to minimizing exposure to cybersecurity threats, especially in internet-facing systems.
  - **Minimize Public-Facing Attack Surface**
    - Do not host any internet-facing applications that are not essential to business operations.
  - **Monitor for known Indicators of Compromise (IOCs)**
    - MTS entities are encouraged to utilize the IOCs listed in Appendix A to monitor their infrastructure for potential compromises. In the event of a compromise, entities are encouraged to report their situation to the National Response Center.
  - **Maintain Offline Data Backups**
    - MTS entities are encouraged to maintain regular data backups in offline and separate systems to limit the severity of a business disruption in the event of a compromise.

If your organization has any questions related to this alert, please contact the U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at 202-372-2904.

[1] Reference to MITRE ATT&CK® techniques does not constitute an endorsement.

Appendix A: Indicators of Compromise

MOVEit Campaign Indicators of Compromise and Infrastructure

File Hash	0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9
File Hash	0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495
File Hash	110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286
File Hash	1826268249e1ea58275328102a5a8d158d36b4fd312009e4a2526f0bfbc30de2
File Hash	2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
File Hash	2ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59
File Hash	348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d
File Hash	387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a
File Hash	38e69f4a6d2e81f28ed2dc6df0daf31e73ea365bd2cfc90ebc31441404cca264
File Hash	3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b
File Hash	3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409
File Hash	3c0dbda8a5500367c22ca224919bfc87d725d890756222c8066933286f26494c
File Hash	4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf
File Hash	48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a
File Hash	58ccfb603cdc4d305fddd52b84ad3f58ff554f1af4d7ef164007cb8438976166
File Hash	5b566de1aa4b2f79f579cdac6283b33e98fdc8c1cfa6211a787f8156848d67ff
File Hash	6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d
File Hash	702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0
File Hash	769f77aace5eed4717c7d3142989b53bd5bac9297a6e11b2c588c3989b397e6b
File Hash	7c39499dd3b0b283b242f7b7996205a9b3cf8bd5c943ef6766992204d46ec5f1
File Hash	93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db
File Hash	98a30c7251cf622bd4abce92ab527c3f233b817a57519c2dd2bf8e3d3ccb7db8
File Hash	9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead
File Hash	9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a
File Hash	a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7
File Hash	a8f6c1ccba662a908ef7b0cb3cc59c2d1c9e2cbbe1866937da81c4c616e68986
File Hash	b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272
File Hash	b5ef11d04604c9145e4fe1bedaeb52f2c2345703d52115a5bf11ea56d7fb6b03
File Hash	b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad
File Hash	bdd4fa8e97e5e6eaaac8d6178f1cf4c324b9c59fc276fd6b368e811b327ccf8b
File Hash	c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4
File Hash	c77438e8657518221613fbce451c664a75f05beea2184a3ae67f30ea71d34f37
File Hash	cec425b3383890b63f5022054c396f6d510fae436041add935cd6ce42033f621
File Hash	cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45
File Hash	d477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899
File Hash	d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195
File Hash	daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4
File Hash	e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e
File Hash	ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a
File Hash	ed0c3e75b7ac2587a5892ca951707b4e0dd9c8b18aaf8590c24720d73aa6b90c
File Hash	f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d
File Hash	fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f
IPv4 Address	104.194.222[.]107
IPv4 Address	146.0.77[.]141
IPv4 Address	146.0.77[.]155
IPv4 Address	146.0.77[.]183
IPv4 Address	148.113.152[.]144
IPv4 Address	162.244.34[.]26
IPv4 Address	162.244.35[.]6
IPv4 Address	179.60.150[.]143

IPv4 Address	**185.104.194[.]156**
IPv4 Address	**185.104.194[.]24**
IPv4 Address	**185.104.194[.]40**
IPv4 Address	**185.117.88[.]17**
IPv4 Address	**185.162.128[.]75**
IPv4 Address	**185.174.100[.]215**
IPv4 Address	**185.174.100[.]250**
IPv4 Address	**185.181.229[.]240**
IPv4 Address	**185.181.229[.]73**
IPv4 Address	**185.183.32[.]122**
IPv4 Address	**185.185.50[.]172**
IPv4 Address	**188.241.58[.]244**
IPv4 Address	**193.169.245[.]79**
IPv4 Address	**194.33.40[.]103**
IPv4 Address	**194.33.40[.]104**
IPv4 Address	**194.33.40[.1]64**
IPv4 Address	**198.12.76[.]214**
IPv4 Address	**198.27.75[.]110**
IPv4 Address	**206.221.182[.]106**
IPv4 Address	**209.127.116[.]122**
IPv4 Address	**209.127.4[.]22**
IPv4 Address	**209.222.103[.]170**
IPv4 Address	**45.227.253[.]133**
IPv4 Address	**45.227.253[.]147**
IPv4 Address	**45.227.253[.]50**
IPv4 Address	**45.227.253[.]6**
IPv4 Address	**45.227.253[.]82**
IPv4 Address	**45.56.165[.]248**
IPv4 Address	**5.149.248[.]68**
IPv4 Address	**5.149.250[.]74**
IPv4 Address	**5.149.250[.]92**
IPv4 Address	**5.188.86[.]114**
IPv4 Address	**5.188.86[.]250**
IPv4 Address	**5.188.87[.]194**
IPv4 Address	**5.188.87[.]226**
IPv4 Address	**5.188.87[.]27**
IPv4 Address	**5.252.23[.]116**
IPv4 Address	**5.252.25[.]88**
IPv4 Address	**5.34.180[.]205**
IPv4 Address	**62.112.11[.]57**
IPv4 Address	**62.182.82[.]19**
IPv4 Address	**62.182.85[.]234**
IPv4 Address	**66.85.26[.]215**
IPv4 Address	**66.85.26[.]234**
IPv4 Address	**66.85.26[.]248**
IPv4 Address	**79.141.160[.]78**
IPv4 Address	**79.141.160[.]83**
IPv4 Address	**84.234.96[.]104**
IPv4 Address	**84.234.96[.]31**
IPv4 Address	**89.39.104[.]118**
IPv4 Address	**89.39.105[.]108**
IPv4 Address	**91.202.4[.]76**
IPv4 Address	**91.222.174[.]95**
IPv4 Address	**91.229.76[.]187**
IPv4 Address	**93.190.142[.]131**

References:

(1) Labs, McAfee. 2023. “CLOP Ransomware Exploits MOVEit Software.” McAfee Blog. June 21, 2023. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware-exploits-moveit-software/.

(2) “MOVEit Transfer and MOVEit Cloud Vulnerability.” 2023. Progress.com. July 5, 2023. https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability.

(3) “#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability | CISA.” 2023. www.cisa.gov. June 7, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

The information contained in this cyber alert is provided for **informational purposes only**. This information is based on common standards and best practices, and the implementation of which does not relieve any domestic, international safety, operational, or material requirements. The USCG does not provide any warranties of any kind regarding this information and shall not be held liable for any damages of any kind that arose out of the results of, or reliance upon this information.