Clop Ransomware: History, Timeline, And Adversary Simulation

fourcore.io/blogs/clop-ransomware-history-adversary-simulation

Article

Last Updated on Tue Jun 03, 2023

Written by **Jones Martin**

Security Engineer @ FourCore

What is Clop Ransomware

The infamous Clop ransomware, mainly known as Cl0p, targets various industries and organizations, extorting data for a considerable ransom. It advances actively with new emerging campaigns. The Clop ransomware is associated with the **Russian threat group TA505**, which primarily operates as a (RaaS) ransomware-as-a-service. It is also seen that the threat group has been using various zero-day exploits for its campaigns, which include the latest Moveit Transfer exploitation. The ransomware is primarily Cryptomix ransomware, making its first appearance in 2019.

History

Clop ransomware mainly targets victims through spear-phishing campaigns, primarily focusing on the banking, healthcare, and finance sectors. The banking sector experiences the highest number of campaigns. On the contrary, the threat group avoids targeting the healthcare sector out of humanitarian considerations. However, the healthcare sector is still affected by its campaigns. The ransomware is also specific in targeting countries such as the USA, Canada, and most parts of the Asia Pacific. The most affected countries are the USA, Canada, and India, all falling victim to these campaigns.

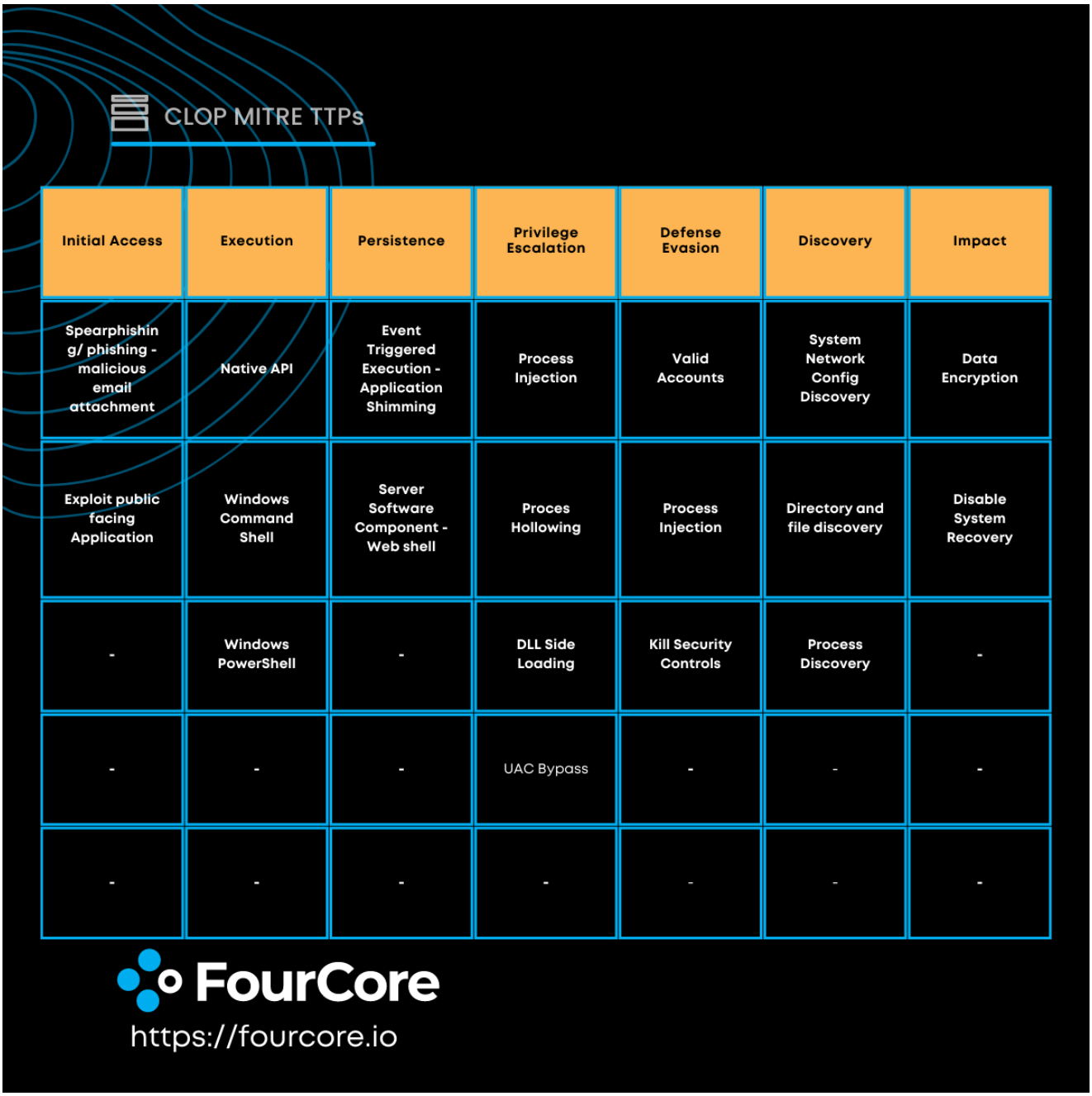
The ransomware is observed exploiting numerous zero-day vulnerabilities with different variations. Installing `DEWMODE`, a webshell, was initially detected on FTA servers by exploiting zero-days. Recently, it was also observed exploiting the MOVEIT Transfer vulnerability, which is an MFT with a SQL injection vulnerability. These exploits were primarily used to exfiltrate data from databases and install webshells, granting the threat actors complete control over the affected endpoints. In a new campaign launched by the threat group, they are seen exploiting GOAnywhere (MFT) using a zero-day vulnerability.

The ransomware actively targets various organizations, and it has been observed since late 2020 that the threat actors have compromised over 100 companies. In collaboration with **Fin11**, a financially motivated threat group, they exploited a zero-day vulnerability in the File Transfer Appliance (FTA) of Kiteworks (formerly known as Accellion). It is important to note that no data was encrypted; however, the threat actors threatened to expose millions of user data on the black market. The Clop ransomware was primarily used to exfiltrate the data. Additionally, the threat actors maintain a blog providing updates on their recent activities. They also operate a market selling data from various organizations for financial gain.

Clop Ransomware Timeline

1. February 2019: First noticed in the wild with large-scale spear phishing.
2. January 2020: Fin11 deployed Clop ransomware on the File Transfer Appliance (FTA) of Kiteworks, formerly Accellion.
3. April 2020: The Clop ransomware threat group gained access to a pharmaceutical company and leaked their user data.
4. November 2021: Maritime services in Singapore fell prey to the Clop ransomware, exfiltrating sensitive information regarding commercial details and employee data, including bank details.
5. November 2021: Security researchers discovered Clop ransomware exploiting the SolarWinds vulnerability, breaching several organizations.
6. April 2022: Security researchers discovered several MOVEit Transfer servers were compromised, which had sensitive information.
7. June 2023: Several companies from various sectors were compromised, including US federal agencies, BBC, hospitals, and EY.

Clop Ransomware Infection chain



The infection chain of the Clop ransomware involves the following stages:

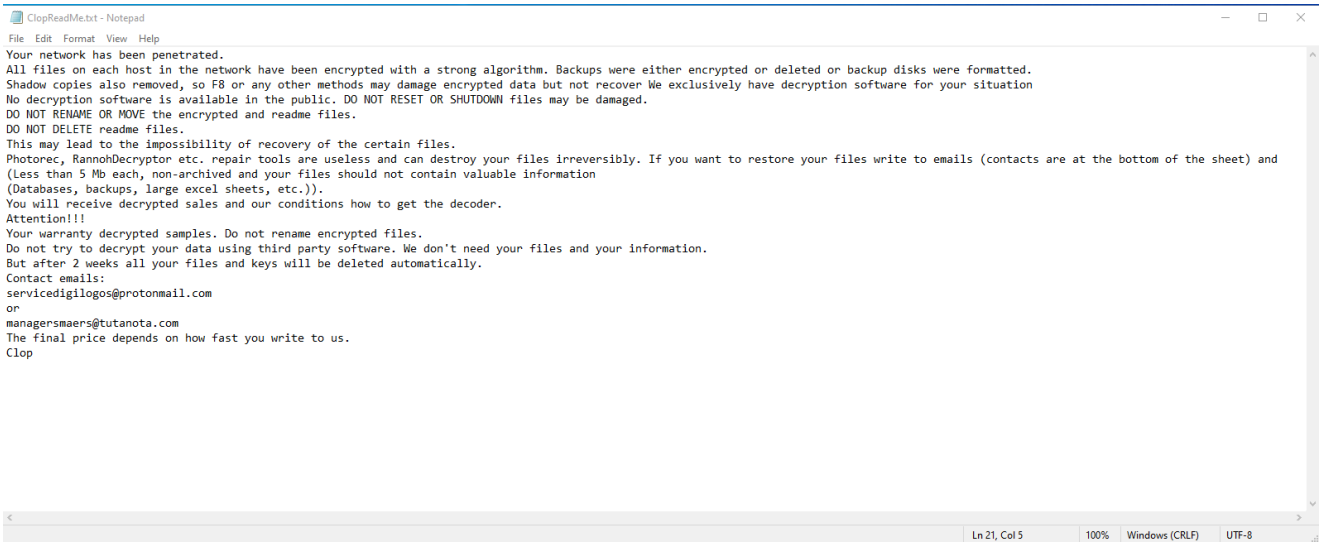
1. Initial Access: T1190 - Exploit Public-Facing Application T1566 - Phishing The initial access is achieved through spear-phishing victims, often accompanied by the SDBot and FlawedAmmy RAT. The ransomware also exploits various applications using zero-days and known CVEs for gaining initial access. Additionally, compromised RDP credentials are utilized as another entry point.
2. Execution: T1059.001 - Command and Scripting Interpreter: PowerShell T1059.003 - Command and Scripting Interpreter: Windows Command Shell T1129 - Shared Modules The ransomware predominantly utilizes native APIs and command interpreters like Windows PowerShell and Visual Basic macros for executing commands.

3. Persistence: T1505.003 - Server Software Component: Web Shell T1546.011 - Event Triggered Execution: Application Shimming The ransomware ensures persistence by being executed during system autostart. It also modifies system processes to evade detection and maintain persistence.
4. Privilege Escalation: T1068 - Exploitation for Privilege Escalation T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control To escalate privileges, the ransomware employs commonly exploited techniques, including UAC bypass and leveraging publicly available CVEs.
5. Defense Evasion: T1055 - Process Injection T1070 - Indicator Removal T1574.002 - Hijack Execution Flow: DLL Side-Loading The ransomware utilizes sophisticated defense evasion techniques. It masquerades as a legitimate process by using valid known signatures. It terminates security controls present on the endpoint and employs process injection to evade detection. Furthermore, it clears the event logs on the infected system.
6. Discovery: T1018 - Remote System Discovery The ransomware scans the endpoint for various files to encrypt and exfiltrate. It also searches for other endpoints connected to the network and identifies processes to check for security controls, terminating them if found.
7. Command and Control: T1071 - Application Layer Protocol T1105 - Ingress Tool Transfer Clop ransomware predominantly utilizes Cobalt Strike for its command and control operations. It frequently sends beacons to actively monitor the infected systems.
8. Impact: T1486 - Data Encrypted for Impact The ransomware encrypts data using a 1024-bit RSA and RC4 key. The encrypted data may be exfiltrated for sale on dark markets, unless the victims comply with the threat actor's demands. Additionally, all shadow volumes are deleted to prevent data recovery.

Clop ransomware targetting the MOVEIT Transfer vulnerability

Clop ransomware specifically targets the MOVEIT Transfer vulnerability, an application designed to facilitate efficient management of file transfer operations within organizations. The threat actors took advantage of a SQL injection vulnerability present in the web application of MOVEIT Transfer. They exploited this vulnerability by installing a webshell known as `LEMURLOOT`. Furthermore, the webshell incorporated various libraries from Moveit and primarily focused on enumerating and retrieving data from the underlying databases. This exploit not only enabled the threat actors to exfiltrate sensitive data but also gave them the ability to execute malicious code. The situation is particularly worrisome as it has been observed that more than 2000 servers are still utilizing the vulnerable version of the MOVEIT Transfer application, rendering them active targets for the threat actor.

The ransom note left by threat actors of Clop ransomware.



Indicator of Compromise (IoC)

Hashes:

Clop ransomware MOVEIT campaign LEMURLOOT Webshell

```
1 0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495
2 110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286
3 1826268249e1ea58275328102a5a8d158d36b4fd312009e4a2526f0bfbc30de2
4 2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
5 2ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59
6 348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d
7 387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a
8 38e69f4a6d2e81f28ed2dc6df0daf31e73ea365bd2cfc90ebc31441404cca264
9 3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b
10 3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409
11 3c0dbda8a5500367c22ca224919bfc87d725d890756222c8066933286f26494c
12 4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf
13 48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a
14 58ccfb603cdc4d305fddd52b84ad3f58ff554f1af4d7ef164007cb8438976166
15 5b566de1aa4b2f79f579cdac6283b33e98fdc8c1cfa6211a787f8156848d67ff
16 6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d
17 702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0
18 769f77aace5eed4717c7d3142989b53bd5bac9297a6e11b2c588c3989b397e6b
19 7c39499dd3b0b283b242f7b7996205a9b3cf8bd5c943ef6766992204d46ec5f1
20 93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db
21 98a30c7251cf622bd4abce92ab527c3f233b817a57519c2dd2bf8e3d3ccb7db8
22 9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead
23 9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a
24 a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7
25 a8f6c1ccba662a908ef7b0cb3cc59c2d1c9e2cbbe1866937da81c4c616e68986
26 b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272
27 b5ef11d04604c9145e4fe1bedaeb52f2c2345703d52115a5bf11ea56d7fb6b03
28 b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad
29 bdd4fa8e97e5e6eaaac8d6178f1cf4c324b9c59fc276fd6b368e811b327ccf8b
30 c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4
31 c77438e8657518221613fbce451c664a75f05beea2184a3ae67f30ea71d34f37
32 cec425b3383890b63f5022054c396f6d510fae436041add935cd6ce42033f621
33 cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45
34 d477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899
35 d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195
36 daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4
37 e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e
38 ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a
39 ed0c3e75b7ac2587a5892ca951707b4e0dd9c8b18aaf8590c24720d73aa6b90c
40 f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d
41 fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f
```

Emails :

Yara Rule:

Presented below is the YARA rule for the MOVEIT CVE, by AhmetPayaslioglu.

```
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
```

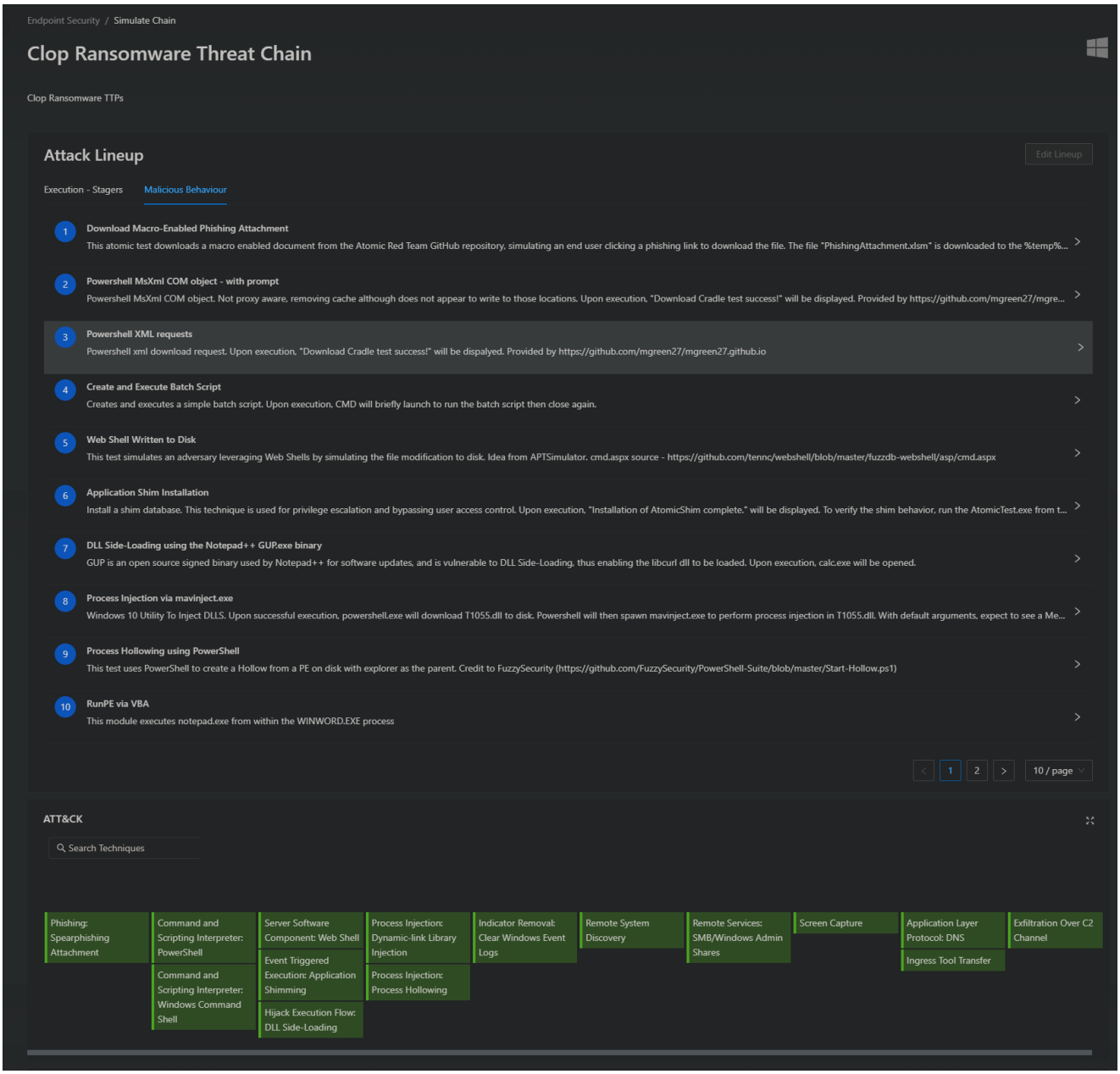
```
61        and all of them
62}
```

CVEs list exploited by the Clop ransomware:

- CVE-2023-34362
- CVE-2023-35036
- CVE-2023-0669
- CVE-2021-27101
- CVE-2021-27102
- CVE-2021-27103
- CVE-2021-27104
- CVE-2021-35211
- CVE-2021-27102

Clop Ransomware Adversary Simulation

FourCore has utilized analysis reports, TTPs, and threat intelligence to develop an adversary simulation assessment for Clop Ransomware. This assessment aims to validate the effectiveness of your organization's security controls using the FourCore ATTACK Platform.



References

- https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
- https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-testing-moveit-zero-day-since-2021/

FourCore ATTACK Breach and Attack Simulation