<https://nvd.nist.gov/vuln/detail/CVE-2023-34362>  
this is exploited in the wild in May and June 2023

In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database

https://www.cisa.gov/sites/default/files/2023-07/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability\_8.pdf

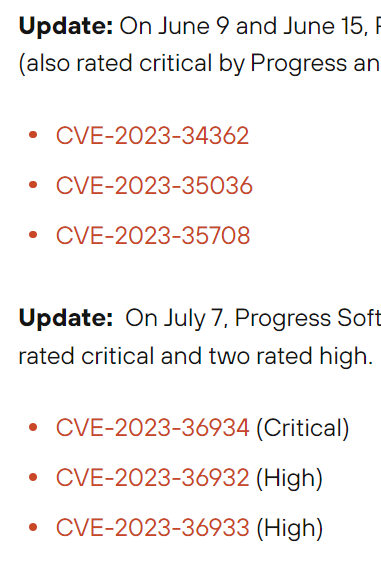
More CVE stuff

<https://nvd.nist.gov/vuln/detail/CVE-2023-35708>

<https://unit42.paloaltonetworks.com/threat-brief-moveit-cvMee-2023-34362/>

<https://www.darkreading.com/cyberattacks-data-breaches/cl0p-claims-moveit-attack-how-gang-did-it>

“MediSecure is aware that a data set containing the personal information and limited health information of our customers has been made available on a dark web forum,” [wrote](https://www.medisecure.com.au/) MediSecure.



So as a recap of I believe what we are going for, we believe the Threat Actor is Cl0p as they have previously exploited a zero day exploit through MoveIt. This is the CVE <https://nvd.nist.gov/vuln/detail/CVE-2023-34362> That then leads to this: CWE-89 <https://cwe.mitre.org/data/definitions/89.html>

<https://www.cisa.gov/sites/default/files/2023-07/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_8.pdf>

**Group Name: TA505**

Associated Groups: Hive0065, Spandex Tempest, CHIMBORAZO

Description: TA505 is a malicious cyber group that are known to have been active since 2014. This group is known for frequently changing its malware making it much harder to detect and prevent attacks resulting in TA505 becoming globally recognised in malware distribution and ransomware campaigns.

Techniques:

* **Acquire Infrastructure: Domains** (T1583.001): TA505 uses this technique to register domains to impersonate services such as Dropbox to trick victims into installing malware.
* **Account Discovery: Email Account** (T1087.003): TA505 uses this technique with a software called EmailStealer to steal and send emails to a remote server.
* **Data Encrypted for Impac**t (T1486): TA505 has used a wide range of ransomware such as cl0p and GlobeImposter to encrypt files and demand ransom from victims.
* **Native API** (T1106): TA505 has deployed payloads using windows API calls on compromised devices.
* **User Execution: Malicious File** (T1204.002): TA505 uses this technique to make malware look like Microsoft word document to lure victims into executing malicious files and attachments.

**Software Name: Cl0p**

Group Association: cl0p is a variant of the CryptoMix ransomware. The TA505 group uses this software.

Description: Cl0p is a Russian developed ransomware which was first introduced in 2019, it operates on the windows platform and is used widespread across multiple industries but has primarily been maliciously used in the retail, automotive, financial, healthcare, and high-tech industries. Cl0p uses several techniques to steal sensitive information and ransom its victims at a high price.

Techniques:

* [**Data Encrypted for Impact**](https://attack.mitre.org/techniques/T1486) (T1486): cl0p uses this to encrypt files using ciphers and add a “. clop” extension to the encrypted files.
* **System Language Discovery** (T1614): cl0p uses this to check the native keyboard language to avoid installing on any Russian associated machines.
* **Subvert Trust Controls: Code Signing** (T1553.002): cl0p uses code signing to evade detection and subvert trust controls.
* **Service Stop** (T1489): cl0p uses this to terminate processes and services that backup and secure the device.

**Cl0p’s Lifecycle**

Cl0p’s main objective is to get into a network of computers and

*Explain the steps that Cl0p goes through to make an attack possible. List all the techniques uses*

1. [T1486](https://attack.mitre.org/techniques/T1486) - Can encrypt files using AES, RSA, and RC4 and will add the ".clop" extension to encrypted files.
2. [T1614](https://attack.mitre.org/techniques/T1614) - Has checked the keyboard language using the GetKeyboardLayout() function to avoid installation on Russian-language or other Commonwealth of Independent States-language machines; it will also check the GetTextCharset function.
3. [T1204](https://attack.mitre.org/techniques/T1204) - has used lures to get users to click links in emails and attachments. For example, makes their malware look like legitimate Microsoft Word documents, .pdf and/or .lnk files.
4. T1583 - Has registered domains to impersonate services such as Dropbox to distribute malware.
5. [T1218](https://attack.mitre.org/techniques/T1218) - Can use msiexec.exe to disable security tools on the system.

There are many other techniques that is used by Cl0p in order to get access to and then perform their ransomware.

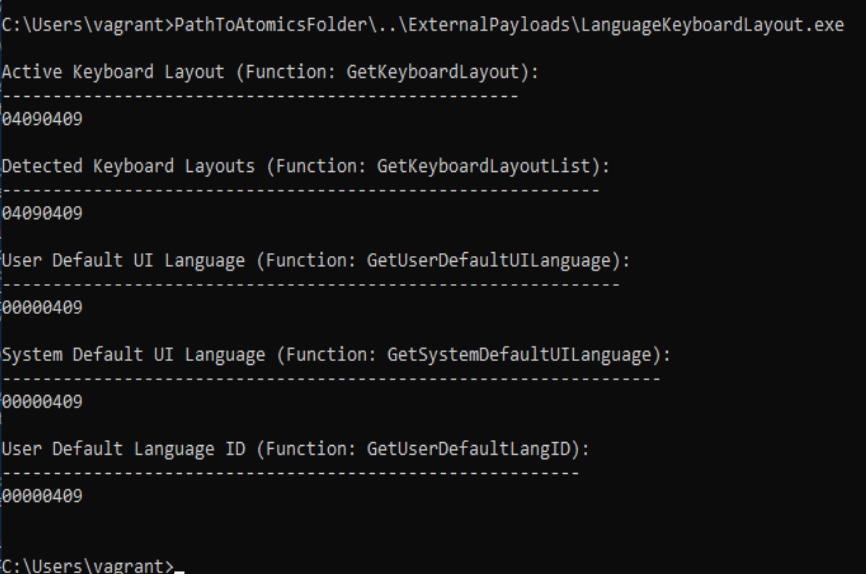
**Analysis of likelihood of CVE exploitation of TA505**

As we work at Medisecure, we use the company MoveIt in order to securely transfer files and help with automation. There is a couple of zero-day vulnerabilities inside MoveIt that the attack likely has come from. These CVE’s are: CVE-2023-34362, CVE-2023-35708, CVE-2023-36934.

**Emulating Attack**

**Technique 1**

Emulating how cl0p would first check if the system is Russian based on the native installed language as to not attack “one of their own”. This would be done using the function “GetKeyboardLayout” against the hardcoded values.

****

In this example, our system shows 0409 which when checked in the OS hex meaning it comes to **English - United States.** Therefore, if this attack where to be realistic cl0p would then proceed with the attack.

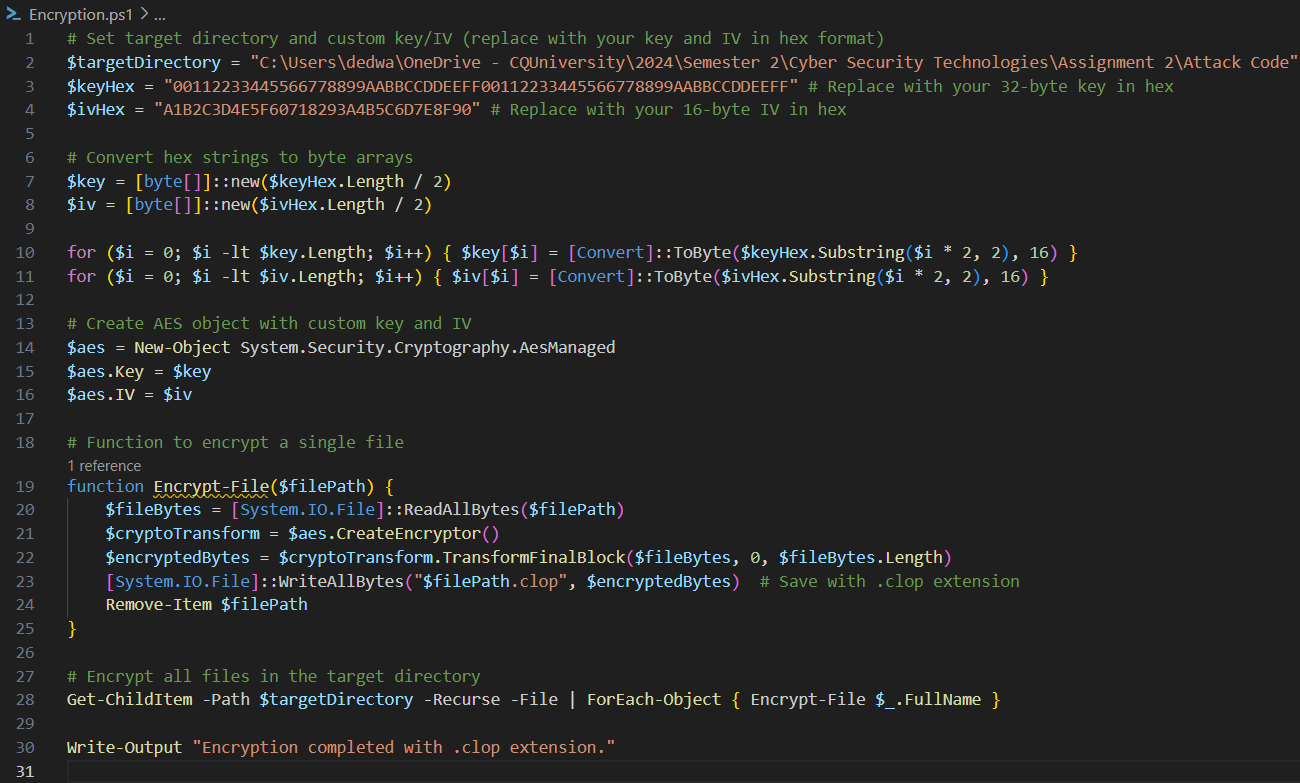
**Detection:** Sysmon was used in PowerShell to display a list to monitor and log system activity to the Windows event log. The command used was: **A blue screen with white text

Description automatically generated**

Get-WinEvent \*Sysmon\* | where message -like "\*LanguageKeyboardLayout.exe\*" | format-list

**Technique 2**

Encrypting files

Encrypts files and creates a new file with .clop extension

**Detection**

Get-WinEvent -LogName $logName | Where-Object { $\_.Id -eq 11 -and $\_.Message -like "\*.clop\*" }

**A screen shot of a computer

Description automatically generated**

**References**

Cybereason 2023, *Cybereason vs. clop ransomware*, viewed 17 September 2024, <https://www.cybereason.com/blog/research/cybereason-vs.-clop-ransomware>.

Dark Reading 2023, *Cl0p the* , viewed 17 September 2024, <https://www.darkreading.com/cyberattacks-data-breaches/cl0p-claims-moveit-attack-how-gang-did-it>.

National Institute of Standards and Technology (NIST) 2023, *Vulnerability summarySummary for cveCVE-2023-34362*, viewed 17 September 2024, <https://nvd.nist.gov/vuln/detail/CVE-2023-34362>.

Red Canary Co. 2024, *Atomic red team t1486: data encrypted for impact*, viewed 17 September 2024, [https://github.com/redcanaryco/atomic-red team/blob/master/atomics/T1486/T1486.md](https://github.com/redcanaryco/atomic-red%20team/blob/master/atomics/T1486/T1486.md).

Red Canary Co. 2024, *Atomic red team t1614.001: system location discovery*, viewed 17 September 2024, <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1614.001/T1614.001.md.>