**Week 7 - Threat Intelligence Report**

**Albrent Pangan, 12185449**

**------------------------------------------------------------------------------------------------------------------------**

**Group Name:** Lace Tempest ([Ransomware actors exploiting MoveIt Transfer vulnerability | TechTarget](https://www.techtarget.com/searchsecurity/news/366539278/Ransomware-actors-exploiting-MoveIt-Transfer-vulnerability))  
**Associated Groups:** Clop Ransomware ([Ransomware actors exploiting MoveIt Transfer vulnerability | TechTarget](https://www.techtarget.com/searchsecurity/news/366539278/Ransomware-actors-exploiting-MoveIt-Transfer-vulnerability))  
**Description:** Lace Tempest, also known as DEV-0950, is a threat actor group that has exploited zero-day vulnerabilities in software such as Progress Software’s MoveIt Transfer. This group is recognized for deploying the Clop ransomware to exfiltrate data from compromised networks and conduct extortion attacks. ([DEV-0950 (Threat Actor) (fraunhofer.de)](https://malpedia.caad.fkie.fraunhofer.de/actor/dev-0950#:~:text=Lace%20Tempest%2C%20also%20known%20as,exfiltrating%20data%20from%20compromised%20networks.))

**Techniques:**

* **Exploitation of Zero-Day Vulnerability:** CVE-2023-34362 (T1190) – Lace Tempest exploited a critical SQL injection flaw in MoveIt Transfer to gain unauthorized access and deploy a custom web shell. ([Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/techniques/T1190/)), ([Ransomware actors exploiting MoveIt Transfer vulnerability | TechTarget](https://www.techtarget.com/searchsecurity/news/366539278/Ransomware-actors-exploiting-MoveIt-Transfer-vulnerability))
* **Web Shell Deployment:** Custom web shell “Lemurloot” (T1071.001) – Used for data exfiltration, disguised with the filename "human.aspx." ([Application Layer Protocol: Web Protocols, Sub-technique T1071.001 - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/techniques/T1071/001/)), ([Ransomware actors exploiting MoveIt Transfer vulnerability | TechTarget](https://www.techtarget.com/searchsecurity/news/366539278/Ransomware-actors-exploiting-MoveIt-Transfer-vulnerability))

**Software Name:** Clop Ransomware ([Ransomware actors exploiting MoveIt Transfer vulnerability | TechTarget](https://www.techtarget.com/searchsecurity/news/366539278/Ransomware-actors-exploiting-MoveIt-Transfer-vulnerability)),   
**Group Association:** Clop Ransomware is the primary tool used by Lace Tempest for data theft and extortion. ([Ransomware gang behind MOVEit attacks is targeting new zero-day, Microsoft says (therecord.media)](https://therecord.media/clop-ransomware-gang-targets-new-zero-day))  
**Description:** Clop ransomware is employed by Lace Tempest to encrypt files and demand ransoms. The ransomware is used in conjunction with other tools to achieve persistence and data extraction. ([Ransomware gang behind MOVEit attacks is targeting new zero-day, Microsoft says (therecord.media)](https://therecord.media/clop-ransomware-gang-targets-new-zero-day)), ([Ransomware actors exploiting MoveIt Transfer vulnerability | TechTarget](https://www.techtarget.com/searchsecurity/news/366539278/Ransomware-actors-exploiting-MoveIt-Transfer-vulnerability))

**Platform:** Windows, Powershell

**Techniques:**

* **Boot or Logon Autostart Execution:** Registry Run Keys / Startup Folder (T1547.001) – Clop ransomware has been observed using Registry Run keys to establish persistence. ([Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/techniques/T1547/001/)), ([Ransomware actors exploiting MoveIt Transfer vulnerability | TechTarget](https://www.techtarget.com/searchsecurity/news/366539278/Ransomware-actors-exploiting-MoveIt-Transfer-vulnerability))
* **File and Directory Discovery:** Custom methods – Clop ransomware has used malicious techniques to discover and exfiltrate sensitive data from compromised systems. ([Ransomware actors exploiting MoveIt Transfer vulnerability | TechTarget](https://www.techtarget.com/searchsecurity/news/366539278/Ransomware-actors-exploiting-MoveIt-Transfer-vulnerability))