blackpoint

THREAT PROFILE:

Clop Ransomware

Table of Contents

Executive Summary

First Identified:
2019

Operation style:
Ransomware-as-a-Service (RaaS)

Extortion method:
Originally a double extortion group; however, since 2020, the group has focused on data extortion via large scale supply chain attacks and threatening to leak data via their data leak site if the ransom demand is not paid.

Most frequently targeted industry:
- Technology

Most frequently targeted victim HQ region:
- United States, North America

Known Associations:
- CryptoMix Ransomware
- FIN7
- FIN11
- Silence Group
- TA505
- UNC2546
- UNC2582

INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

Valid accounts, exploitation of remote services, vulnerability exploitation, social engineering (MITRE ATT&CK: T1078, T1133, T1190, T1566)

Server software component, create/modify system processes, event triggered execution, boot or logon autostart execution (MITRE ATT&CK: T1505, T1543, T1546, T1547)

Exploitation of remote services, remote service session hijacking, RDP, lateral tool transfer (MITRE ATT&CK: T1021, T1563, T1570)

Description

Clop (sometimes referred to as Cl0p) ransomware was first identified in 2019 and, in 2020, added the double extortion method, where victims' data is stolen and leaked via a data leak site if the ransom is not paid, to their arsenal. Clop is purportedly derived from the Cryptomix ransomware operation; it is widely believed that the group's name originates from a Russian "klop", which means "bed bug." The group was identified after launching a large-scale phishing campaign that used a verified and digitally signed binary, which made it look like a legitimate executable file.

Clop operators have gained notoriety over the previous four years for exploiting high-profile vulnerabilities to conduct large scale supply chain attacks targeting hundreds to thousands of victims. In these cases, the group has reportedly avoided encryption and focused their efforts on stealing sensitive information that can be used to extort the victims, their partners, and clients.

- In December 2020, Clop operators exploited Accellion FTA zero-day vulnerabilities (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104) to breach up to 100 companies using Accellion's legacy File Transfer Appliance. The group used the DEWMODE web shell to exfiltrate sensitive data and then threatened to leak the data if the ransom was not paid. This attack was attributed to the FIN11 affiliate of the Clop ransomware operation.
- In February 2023, Clop operators exploited CVE-2023-0669 in Fortra's GoAnywhere MFT secure transfer tool to gain RCE on unpatched instances. The Clop operators reportedly stole data from compromised victims, including 130 companies, over a period of 10 days. The group then listed organizations that refused to pay a ransom on their data leak site.

Clop is purportedly derived from the Cryptomix ransomware operation.

- In May 2023, Clop operators exploited CVE-2023-34362 in Progress MOVEit Transfer solution to exfiltrate data from thousands of companies – researchers have estimated 2,000 victims. The attacks began on May 27, 2023, and victims were named on the group's data leak site beginning on June 14, 2023. The group reportedly deleted any data stolen from governments, military organizations, and children's hospitals during the attacks; however, it is not known if that is true. In the previous Accellion and GoAnywhere attacks, the operators emailed their extortion demands to the victims. In the MOVEit attacks, the group required the victims to make contact with the group to begin negotiations of a ransom demand.
- In December 2024, Clop operators claimed responsibility for targeting and exploiting zero-day vulnerabilities in Cleo Harmony, VLTrader, and LexiCom file transfer platforms. In October an unrestricted file uplaods and downloads vulnerability, CVE-2024-50623 was patched in the software; in December 2024 the patch was found to be insufficient. Threat actors were able to exploit another zero-day, CVE-2024-55956, to conduct data theft attacks.

Similar to other operations, Clop attempts to delete backup files, Volume Shadow Copy Service, and event logs; terminate security software; and resize disk space prior to encryption (when they use the encryption feature). Ransomware binaries are specific to the victim, including an embedded 1024-bit RSA public key and a unique ransom note. The malware encrypts the data using the Windows CryptoAPI and then writes the encrypted data to a new file before deleting the original.

Description

In 2021, an international law enforcement operation, including 19 agencies and 17 countries, led to the apprehension of six purported Clop members. The operation was a 30-month investigation into attacks against South Korean companies and U.S. academic institutions. While law enforcement operations have proven successful in disruptions, the continued operations of the Clop ransomware group highlight the difficulties faced in completely shutting down a prolific ransomware operation.

In 2023, The U.S. State Department's Rewards for Justice program announced up to a $10 million bounty for information linking the Clop ransomware attacks to a foreign government. The bounty was announced after the Clop ransomware group claimed responsibility for data theft attacks on companies using the MOVEit Transfer platform.

Clop Ransomware has repeatedly targeted vulnerabilities in file transfer software to conduct data theft attacks.

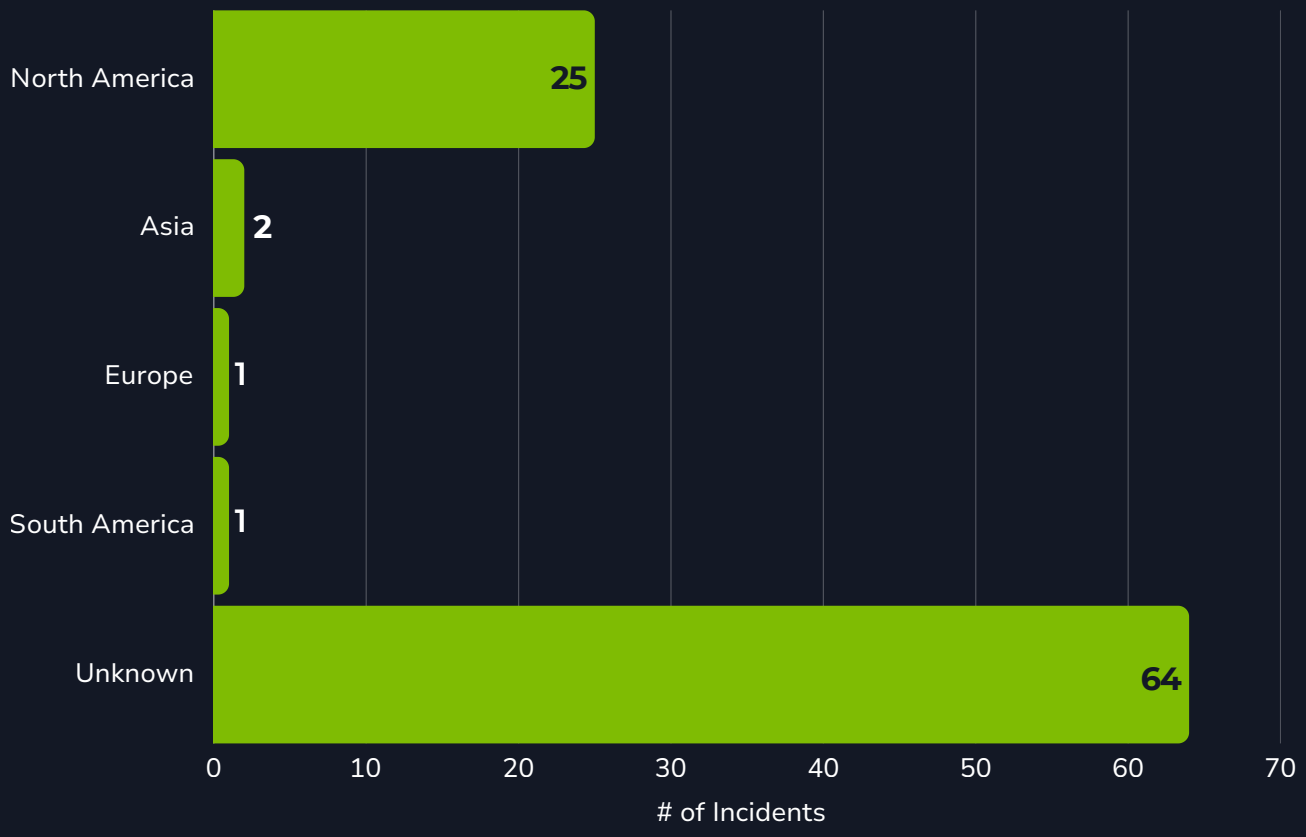
Previous Targets: Clop

Previous Industry Targets from 01 Jan 2024 to 31 Dec 2024

The 64 “unknown” victims are purportedly related to the Cleo Software exploitation. The victim names have not been disclosed at the time of writing, therefore could not be tracked by vertical.

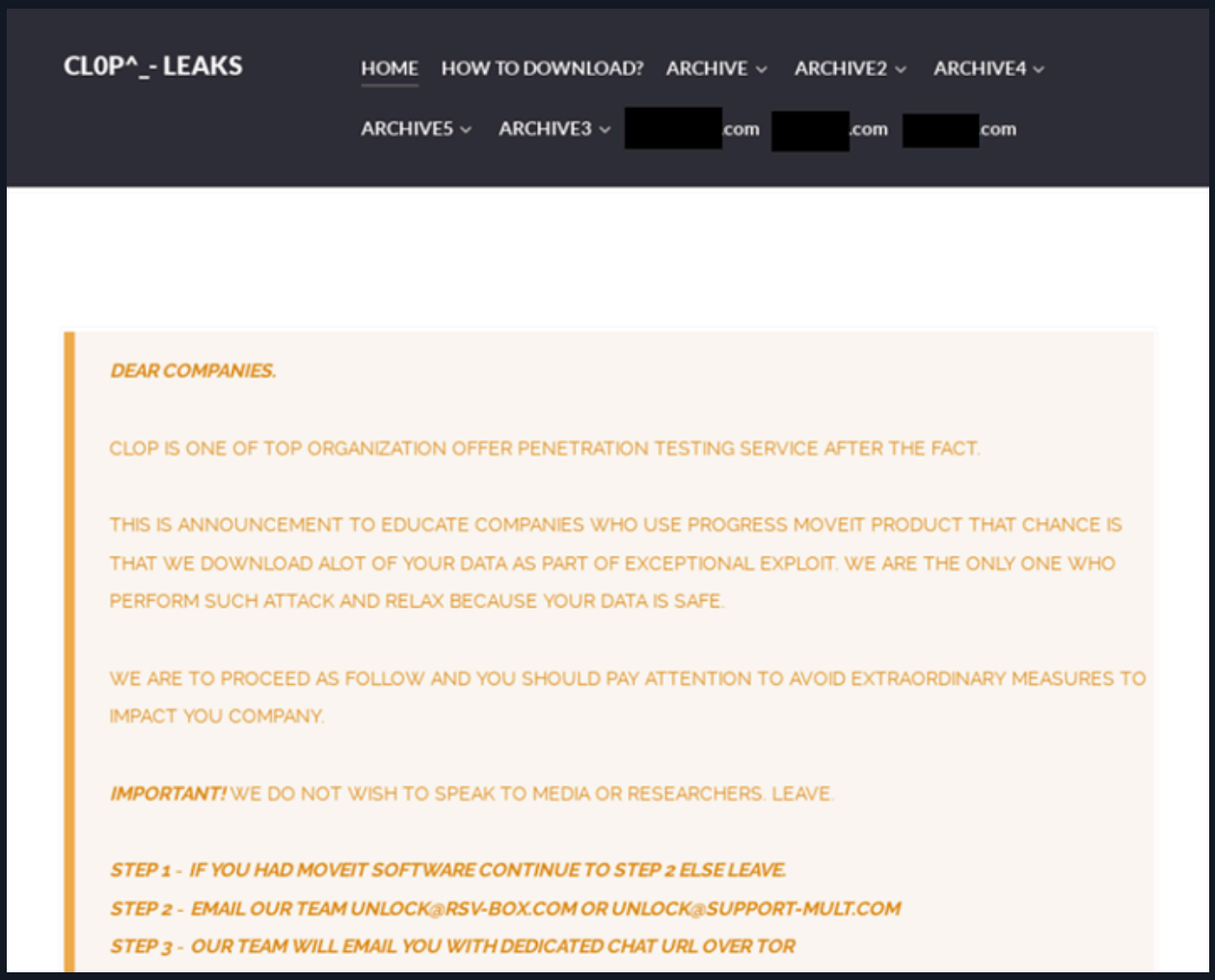
Previous Targets: Clop

Previous Victim HQ Regions from 01 Jan 2024 to 31 Dec 2024



The 64 “unknown” victims are purportedly related to the Cleo Software exploitation. The victim names have not been disclosed at the time of writing, therefore could not be tracked by vertical.

Data Leak Site: Clop



hxxp://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad[.]onion/
·hxxp://toznnag5o3ambca56s2yacteu7q7x2avrfherzmz4nmujrjuib4iusad[.]onion/
hxxp://ekbgzchl6x2ias37[.]onion/

Known Exploited Vulnerabilities

CVE-2019-19781 (CVSS: 9.8)

Directory Traversal Vulnerability
Product Affected: Citrix Application Delivery Controller and Citrix Gateway

CVE-2021-27101 (CVSS: 9.8)

SQL Injection Vulnerability
Product Affected: Accellion FTA

CVE-2021-27102 (CVSS: 7.8)

OS Command Injection Vulnerability
Product Affected: Accellion FTA

CVE-2021-27103 (CVSS: 9.8)

SSRF Vulnerability
Product Affected: Accellion FTA

CVE-2021-27104 (CVSS: 9.8)

OS Command Injection Vulnerability
Product Affected: Accellion FTA

CVE-2021-35211 (CVSS: 10)

Remote Memory Escape Vulnerability
Product Affected: SolarWinds Serv-U

CVE-2022-1388 (CVSS: 9.8)

Missing Authentication Vulnerability
Product Affected: F5 BIG-IP

Known Exploited Vulnerabilities

CVE-2023-0669 (CVSS: 7.2)

RCE Vulnerability
Product Affected: Fortra GoAnywhere MFT

CVE-2023-27350 (CVSS: 9.8)

Improper Access Control Vulnerability
Product Affected: PaperCut MF/NG

CVE-2023-27351 (CVSS: 7.5)

Improper Access Control Vulnerability
Product Affected: PaperCut NG 22.0.5

CVE-2023-34362 (CVSS: 9.8)

SQL Injection Vulnerability
Product Affected: Progress MOVEit Transfer

CVE-2023-35063 (CVSS: 6.5)

Information Disclosure Vulnerability
Product Affected: Microsoft WordPad

CVE-2023-35708 (CVSS: 9.8)

SQL Injection Vulnerability
Product Affected: Progress MOVEit Transfer

CVE-2023-47246 (CVSS: 9.8)

Path Traversal Vulnerability
Product Affected: SysAid Server

Known Exploited Vulnerabilities

CVE-2024-50623

Unrestricted File Upload and Download Vulnerability
Product Affected: Cleo Harmony, VLTrader, and LexiCom

CVE-2024-55956

Unauthenticated Malicious Hosts Vulnerability
Product Affected: Cleo Harmony, VLTrader, and LexiCom

Log4Shell (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832) (CVSS: 10, 9, 5.9, 6.6)

RCE, DoS, DoS, RCE Vulnerabilities
Product Affected: Apache Log4j Java Library

ZeroLogon (CVE-2020-1472) (CVSS: 10)

Privilege Escalation Vulnerability
Product Affected: Netlogon

Associations: Clop

CryptoMix Ransomware

Clop is believed to be derived from the Cryptomix ransomware family.

FIN7

AKA Carbon Spider, Gold Waterfall, Sangria Tempest. A financially motivated threat group that has been observed deploying the Clop ransomware variant in cyberattacks.

FIN11

AKA DEV-0950, Lace Tempest. A financially motivated threat group that has been observed deploying the Clop ransomware variant in cyberattacks.

Silence Group

An IAB group that has been tied to the Truebot malware and has been observed providing access to victim networks for TA505 and, thus, the Clop ransomware group.

TA505

AKA Graceful Spider, Gold Evergreen, Gold Tahoe, Hive0065, Spandex Tempest. A threat group that conducts both financially motivated and APT-style attacks to steal sensitive information. The group has been observed deploying the Clop ransomware in cyberattacks.

UNC2546

A threat cluster observed deploying the Clop ransomware variant

UNC2582

A threat cluster observed deploying the Clop ransomware variant.

Known Tools: Clop

bcdedit	A command line tool for managing Configuration Data; it can be used to create new stores, modify existing stores, and add boot menu options.
cmd	A program used to execute commands on a Windows computer.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
DEWMODE	A PHP web shell that allows threat actors to view and download files in the victim machine.
FlawedAmmyy	A RAT that has been active since, at least, 2016 and has been attributed to the TA505 threat group. The malware contains the ability to execute commands, collect sensitive information, detect anti-virus products, and deploy additional malware.
FlawedGrace	AKA GraceWire. A RAT written in C++ that has been active since, at least, 2017 and has the capability to collect system information and provide remote access to threat actors.
Get2	A downloader written in C++ that has been used to deploy additional payloads to a compromised device.
LEMURLOOT	A web shell written in C# that is designed to exfiltrate data and execute on systems running MOVEit Transfer.
LSASS	A Windows process that takes care of security policy for the OS.
Malichus	A JavaScript backdoor that allows attackers to stealer data, execute commands, and gain further access to a compromised network. Clop operators were reported to use the backdoor when targeting Cleo managed file transfer platforms.
MEGASync	A cloud-based synchronization tool that is designed to work with the MEGA file-sharing service.

Known Tools: Clop

Net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PowerTrash	An in-memory dropper written in PowerShell that executes an embedded payload
Raspberry Robin	A worm-like malware dropper that sells initial access to compromised networks to ransomware groups and malware operators.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
Reg	A Windows utility used to interact with the Windows Registry; it can be used at the command-line interface to query, add, modify, and remove information.
SDBot	A backdoor with installer and loader components that has been active since, at least, 2019. The malware has the ability to access files, enumerate a list of processes, collect system information, and establish persistence.
SMB	A client-server communication protocol used for sharing access to files, printers, serial ports, and other resources on a network.
Taskkill	A legitimate Windows file that is used by malware to terminate processes on the victims' computer.
TinyMet	A Meterpreter stager that supports various transports and allows destination port and destination host setting during runtime.
Truebot	A botnet that has been used by threat actors to collect and exfiltrate information from targeted machines.
VSSAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes.

Observed Clop Behaviors: Windows

Execution	WNetOpenEnumW() WNetEnumResourceW() WNetCloseEnum() GetProcAddress() VirtualAlloc()
Defense Evasion	vssadmin delete shadows /all /quiet cmd.exe /C vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB cmd.exe /C net stop BackupExecAgentBrowser /y cmd.exe /C taskkill /IM powerpnt.exe /F

MITRE ATT&CK® Mappings: Clop

Reconnaissance	
T1590: Gather Victim Network Information	
T1595: Active Scanning	.002: Vulnerability Scanning
T1598: Phishing for Imformation	.002: Spearphishing Attachment .003: Spearphishing Link
Resource Development	
T1587: Develop Capabilities	.001: Malware .004: Exploits
T1588: Obtain Capabilities	.001: Malware .002: Tool .005: Exploits
T1608: Stage Capabilities	.001: Upload Malware .002: Upload Tool
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link

MITRE ATT&CK® Mappings: Clop

Execution	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .007: JavaScript
T1106: Native API	
T1129: Shared Modules	
T1204: User Execution	.001: Malicious File .002: Malicious Link
Persistence	
T1505: Server Software Component	.003: Web Shell
T1543: Create or Modify System Process	.003: Windows Service
T1546: Event Triggered Execution	.004: Unix Shell Configuration Modification .011: Application Shimming
T1547: Boot or Logon Autostart Execution	
Privilege Escalation	
T1068: Exploitation for Privilege Escalation	
T1484: Domain Policy Modification	.001: Group Policy Modification

MITRE ATT&CK® Mappings: Clop

Defense Evasion	
T1027: Obfuscated Files or Information	.002: Software Packing
T1036: Masquerading	.001: Invalid Code Signature
T1055: Process Injection	.001: Dynamic-Link Library Injection
T1070: Indicator Removal	.001: Clear Windows Event Log .004: File Deletion
T1112: Modify Registry	
T1140: Deobfuscate/Decode Files or Information	
T1202: Indirect Command Execution	
T1218: System Binary Proxy Execution	.007: Msiexec
T1222: File and Directory Permissions Modification	.002: Linux and Mac File and Directory Permissions Modification
T1497: Virtualization/Sandbox Evasion	.003: Time Based Evasion
T1553: Subvert Trust Controls	.002: Code Signing
T1562: Impair Defense	.001: Disable or Modify Tools
T1574: Hijack Execution Flow	.002: DLL Side-Loading
Discovery	
T1012: Query Registry	

MITRE ATT&CK® Mappings: Clop

Discovery	
T1018: Remote System Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: FIle and Directory Discovery	
T1135: Network Share Discovery	
T1518: Software Discovery	.001: Security Software Discovery
T1614: System Location Discovery	.001: System Language Discovery
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares
T1563: Remote Service Session Hijacking	.002: RDP Hijacking
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1113: Screen Capture	
T1114: Email Collection	

MITRE ATT&CK® Mappings: Clop

Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1105: Ingress Tool Transfer	
T1573: Encrypted Channel	
Exfiltration	
T1041: Exfiltration Over C2 Channel	
T1567: Exfiltration Over Web Service	
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1499: Endpoint Denial of Service	.001: OS Exhaustion Flood
T1657: Financial Theft	

References

- Abrams, Lawrence (2024, December 15) “Clop ransomware claims responsisbility for Cleo data theft attacks.” https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-cleo-data-theft-attacks/
- Abrams, Lawrence (2023, June 17) “US govt offers $10 million bounty for info on Clop ransomware.” https://www.bleepingcomputer.com/news/security/us-govt-offers-10-million-bounty-for-info-on-clop-ransomware/
- CISA (2023, June 07) “#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
- Cyberint Research Team (2023, October 23) “CL0P Ransomware: The Latest Updates.” https://cyberint.com/blog/techtalks/cl0p-ransomware/
- Cyble (2023, April 03) “Cl0p Ransomware: Active Threat Plaguing Businesses Worldwide.” https://cyble.com/blog/cl0p-ransomware-active-threat-plaguing-businesses-worldwide/
- Din, Antonia (2023, August 03) Heimdal Security: “Clop Ransomware: Overview, Operating Mode, and Prevention [UPDATED 2023].” https://heimdalsecurity.com/blog/clop-ransomware-overview-operating-mode-prevention-and-removal/
- Downie, Scott; Ackerman, Devon; Iacono, Laurie; Cox, Dan (2023, June 08) Kroll: “Clop Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021.” https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362
- ETDA (2023, September 05) “Tool: Clop.” https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Clop&n=1
- Frank, Daniel (n.d.) Cybereason: “Cybereason vs. Clop Ransomware.” https://www.cybereason.com/blog/research/cybereason-vs.-clop-ransomware
- Imano, Shunichi; Slaughter, James (2023, July 21) Fortinet: “Ransomware Roundup – Clop.” https://www.fortinet.com/blog/threat-research/ransomware-roundup-cl0p
- MITRE (2021, October 15) “Clop.” https://attack.mitre.org/software/S0611/
- Mundo, Alexandre (2019, August 01) McAfee: “Clop Ransomware.” https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/
- Neagu, Cristian (2023, November 10) Heimdal Security: “SysAid Zero-Day Vulnerability Exploited by Threat Actors.” https://heimdalsecurity.com/blog/sysaid-zero-day-vulnerability/
- Santos, Doel (2021, April 13) Palo Alto Unit 42: “Threat Assessment: Clop Ransomware.” https://unit42.paloaltonetworks.com/clop-ransomware/
- Securin (2023, July 11) “All About Clop Ransomware.” https://www.securin.io/blog/all-about-clop-ransomware/
- SentinelOne (n.d.) “Clop.” https://www.sentinelone.com/anthology/clop
- SOCRadar (2023, July 21) “Dark Web Threat Profile: CLOP Ransomware.” https://socradar.io/dark-web-threat-profile-clop-ransomware/
- Trend Micro Research (2022, February 22) “Ransomware Spotlight: Clop.” https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop

References

- White, Jeff (2023, September 29) Palo Alto Unit 42: “CL0P Seeds ^_- Gotta Catch Em All!” https://unit42.paloaltonetworks.com/cl0p-group-distributes-ransomware-data-with-torrents/
- ZeroFox Intelligence (2023, July 18) “Flash Report: Analysis of Clop Ransomware Activity.” https://www.zerofox.com/blog/flash-report-analysis-of-clop-activity/

Adversary Pursuit Group

blackpoint