Pentera Ransomware Emulation Report

The Pentera™ automated security validation report summarizes the vulnerabilities, exploit achievements, and remediation action items recommended in your network based on the latest ethical hacking pentesting techniques.

Disclaimer:
For security reasons, this report is anonymized and excludes sensitive data

Executive Summary

Percentage of hosts that proved resilient to ransomware. Excludes hosts with no files to test

Type	**Cl0p Ransomware Emulation**
Time	July 7 2025 13:12 - July 7 2025 14: 30
Test Name	**Cl0p Targeted Test - Data Center B**
Description	Advanced Targeted Testing
IP Ranges	172.20.3.0 - 172.20.3.255, 172.21.5.0... 2 Ranges
Data Exfiltration to	Designated C2
Targeted Hosts of Testing Candidates*	80% (80 / 100)

Action Success Rate

55% (6 of 11)

Payload Launch	55%
File Enumeration	100%
Process Manipulation	0%
Encryption	100%
Data Exfiltration	100%
Host Modification	100%

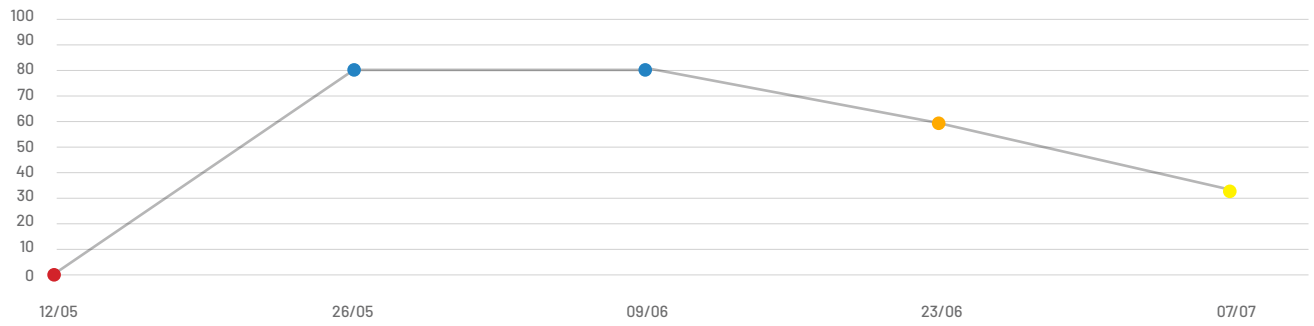
AV / EDR Bypass
65 Hosts
Encrypted files while bypassing endpoint security controls

Ransomware Completed
60 Hosts
Performed all campaign-related actions

Ransomware Interrupted
15 Hosts
Interrupted by security controls or network connectivity issues

Found No Files To Encrypt
5 Hosts
Targeted standard user-related files

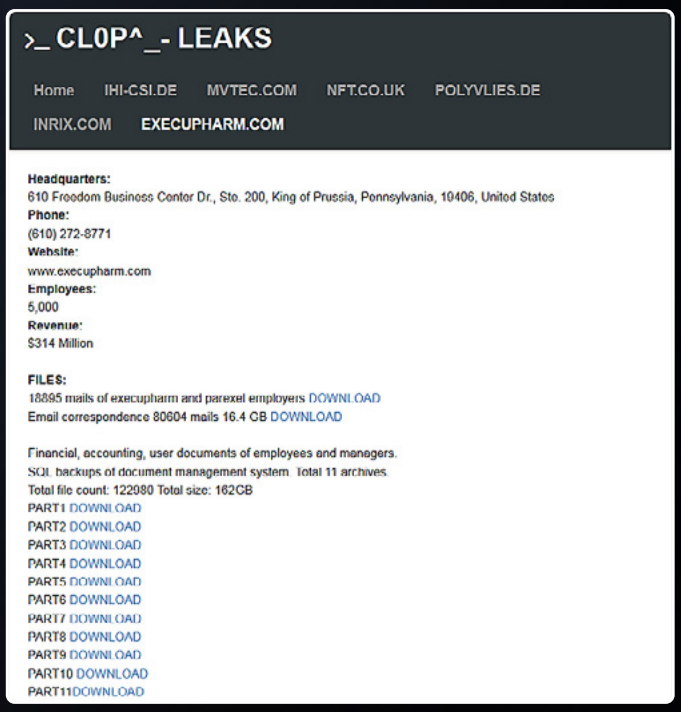
Resilience Score over the last 5 runs



Cl0p

Cl0p is a sophisticated and persistent ransomware strain that has been active since 2019 and is associated with the larger CryptoMix ransomware family. Known for its capability to target both Windows and Linux environments, Cl0p has evolved significantly. Now, it utilizes double extortion tactics, encrypting data while exfiltrating it to pressure victims into paying ransoms.

Cl0op operators often exploit zero-day vulnerabilities, particularly in file transfer software (like MOVEit), VPNs, and remote access tools, to gain initial access. Once inside, they deploy tools to disable security measures, move laterally, escalate privileges, and encrypt or exfiltrate data while covering their tracks. The group is known for its deliberate deletion of shadow copies, creation of scheduled tasks, and disabling of security controls to maximize impact.



Related Campaigns

CryptoMix, TA505

Threat Actor

Cl0p

Origins

Russian Federation

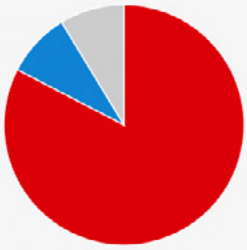
Target Network Key Findings

23 Targeted Hosts

Of the hosts approved for testing: 21 were evaluated, 2 could not be tested.

Distribution of Testing Results (23 Targeted Hosts)

- **19** Ransomware killchain completed (82.6%)
  2 Critical Assets
- **2** Ransomware killchain interrupted (8.7%)
  2 Critical Assets
- **2** Found no files to encrypt (8.7%)
  2 Critical Assets
  Check if relevant file types are included in the template and present on the host.



AV/EDR Bypass Events

Endpoint security controls detected on the targeted hosts and their ability to interrupt the ransomware.

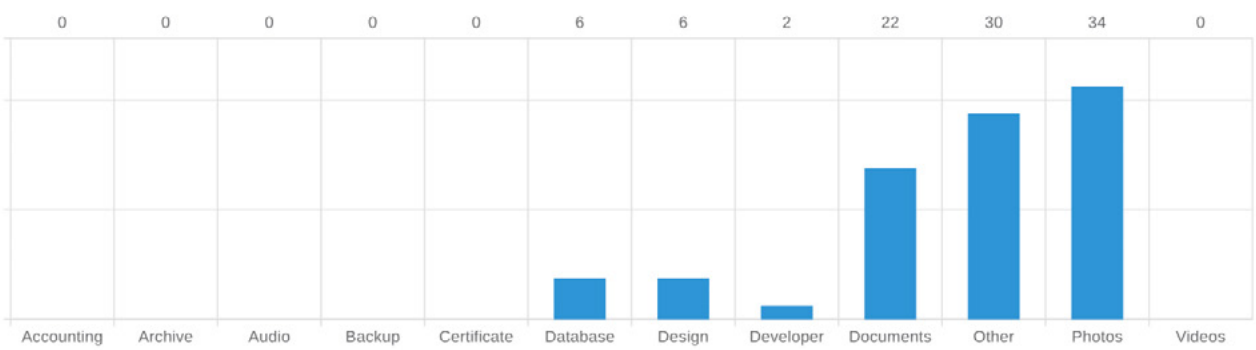
Vendor	Hosts	AV / EDR Bypass
No AV & EDR Detected	15 Hosts	12 Hosts

Encrypted File Types

No changes were made to Pentera's default file type selection; all user-related file extensions were targeted for encryption.

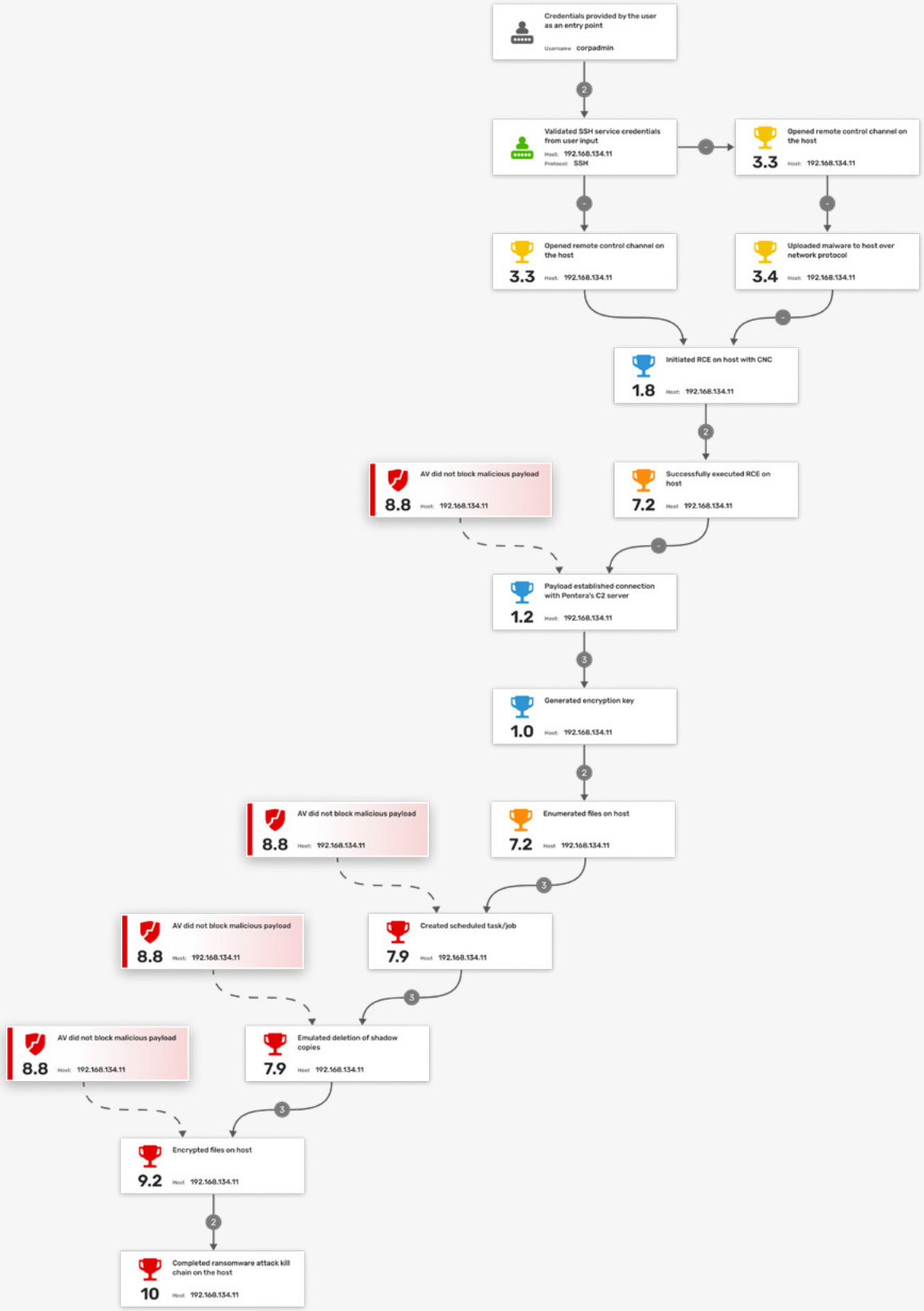
Targeted Hosts	Encrypted Files
100% (4 of 4)	**100% (100 of 100)**

Encryption distribution by file category

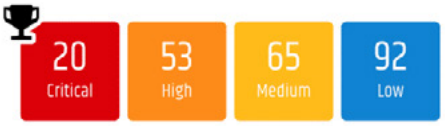


Attack Kill Chain

10 Completed ransomware attack kill chain on the host



230 Achievements



Pentera accomplished 230 achievements in total. Every achievement represents a discrete successful action performed by Pentera.

Listing 30 of 30 items.

Severity Details

10
Severity

(5) Completed ransomware attack kill chain on the host

Pentera was able to execute an end-to-end attack of the selected ransomware family without being blocked.

9.2
Severity

(5) Encrypted files on the host

Attackers may encrypt files, data, cloud storage objects, and online backups on local and remote drives to disrupt operations and interrupt system availability. In ransomware attacks, a unique decryption key is offered in exchange for a ransom payment.

8.2
Severity

(5) Emulated termination of backup services

Adversaries may try to stop live backup services in order to prevent the victim from being able to recover data without the encryption key

7.9
Severity

(5) Emulated automatic logon entry in Windows registry

Attackers may write information in the automatic logon settings in Windows (SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon) to ensure persistence and maintain control over the infected system. This way, even if the system reboots, it can log in again automatically. This allows the attacker's ransomware to continue its malicious activities without requiring manual intervention, maintain a foothold on the system, and continue to encrypt files or carry out other damaging actions.

7.9
Severity

(5) Created scheduled task/job

Attackers create scheduled tasks that automatically restart ransomware payloads after system reboots or at specific intervals. Ensures that even if initial detection mechanisms stop the ransomware, it will attempt to re-execute later.

7.9
Severity

(5) Emulated Log deletion

Adversaries may clear event logs to hide their intrusive activity. For example, Windows Event Logs are records of a computer's alerts and notifications, there are 3 system-defined sources of events: System, Application, and Security, with 5 event types: Error, Warning, Information, Success Audit, and Failure Audit. In Linux the authentication logs record information about user login and authentication events, including details such as the username, source IP address, timestamp, and success or failure status.

7.9
Severity

(5) Emulated deletion of shadow copies

Adversaries may turn off system recovery services or delete volume shadow copies to compound the effects of data encrypted for impact.

7.9 (5) Emulated AV/EDR uninstallation

Severity

Adversaries may modify and/or disable security tools to avoid possible detection of their malware, tools and activities and cover up their tracks. This activity can take on many forms, such as killing security software processes or services, modifying or even deleting Registry keys or configuration files so that tools do not operate properly. These are only examples or many methods attackers can interfere with scanning and reporting activities of security tools.

7.9 (5) Emulated EDR termination

Severity

Adversaries may modify and/or disable security tools to avoid possible detection of their malware, tools and activities and cover up their tracks. This activity can take on many forms, such as killing security software processes or services, modifying or even deleting Registry keys or configuration files so that tools do not operate properly. These are only examples or many methods attackers can interfere with scanning and reporting activities of security tools.

7.0 (10) Extracted user hash from host

Severity

Attackers can grab hashed user passwords from the shadow file in order to crack them offline and thereby gain authorized access to further their attacks

6.0 (1) Established Network Tunnel

Severity

3.4 (8) Uploaded malware to host over network protocol

Severity

An attacker can execute arbitrary malicious code on a host to extract sensitive data, manipulate the system, or use it to further advance the attack.

3.3 (57) Opened remote control channel on the host

Severity

An attacker may establish a connection to a remote malicious payload on a victim's machine in order to control the payload remotely. This allows an attacker to receive information from the payload and instruct it with additional commands. The connection method could be either Bind (the attacker connects to the remote payload) or Reverse (the remote payload connects to the attacker).

1.8 (45) Initiated RCE on host with CNC

Severity

1.2 (33) Payload established connection with Pentera's C2 server

Severity

An attacker may establish a connection to a remote malicious payload on a victim's machine in order to control the payload remotely. This allows an attacker to receive information from the payload and instruct it with additional commands. The connection method could be either Bind (the attacker connects to the remote payload) or Reverse (the remote payload connects to the attacker).

1.0 (4) Generated Encryption key

Severity

Adversaries may generate a random key for encrypting files.

Indicators of Compromise (IOCs)

ClOp

Command and Control URLs and IPs

Monitor your network for URLs related to the ClOp (TA505) campaign. The list of URLs is provided in our Remediation Wiki

Malware Samples

Detect malware samples found to be related to ClOp campaigns. The list of hashes is provided in our Remediation Wiki

Credentials Extraction

ClOp (TA505) affiliates have been observed employing a range of freeware and open-source tools in their intrusions. These tools are used to obtain credentials to leverage for various techniques, including reconnaissance, lateral movement, privilege escalation, and persistency on the infected hosts.

EDR Termination

During the execution of the ClOp (TA505) campaign, attackers may modify and/or disable security tools to avoid possible detection of their malware, tools, and activities that cover up their tracks. This activity can take on many forms, such as killing security software processes or services such as CrowdStrike Falcon, VMware Carbon Black, Microsoft Defender, SentinelOne, and more.

Log Deletion

Deleting logs may remove evidence of malicious activities, making it more difficult for security professionals to trace the attacker's actions, understand their techniques, and comprehend the extent of the attack. This ultimately delays an effective response and any recovery efforts, and may also prevent effective forensic analysis.

Shadow Copies Deletion

ClOp (TA505) campaigns delete shadow copies and disable Windows Recovery features on Windows hosts to undermine the ability to recover data from the encryption process.
All of the above is usually achieved by executing the following command line example:

```
"%WINDIR%System32cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
```

Schedule Task Creation

The ClOp ransomware campaign uses scheduled tasks to maintain persistence on compromised systems, ensuring the malware runs after reboots.
The above is usually achieved by executing the following command line example:

```
schtasks /create /sc minute /mo 1 /tn Server /tr $user\$temp/Server.exe
```

MITRE ATT&CK Matrix for Enterprise - Heat Map

MITRE | ATT&CK®

Total Patterns

1175

Most Common Technique

Defense Evasion / Credential Access

Command and Control	Exfiltration	Impact	Credential Access	Discovery	Execution	Defense Evasion
Application Layer Protocol T1071	Exfiltration Over Alternative Protocol T1048	Resource Hijacking T1496	OS Credential Dumping T1003	Remote System Discovery T1018	Command and Scripting Interpreter T1059	System Services T1569
Web Protocols T1071.001	Exfiltration Over Unencrypted Non-... T1048.003	Service Stop T1489	/etc/passwd and /etc/shadow T1003.008	Network Service Discovery T1046	Unix Shell T1059.004	Service Execution T1569.002
File Transfer Protocols T1071.002			Unsecured Credentials T1552	Network Share Discovery T1135		Indicator Removal T1070
Non-Application Layer Protocol T1095			Credentials In Files T1552.001	System Information Discovery T1082		File Deletion T1070.004
Ingress Tool Transfer T1105			Bash History T1552.003	File and Directory Discovery T1083		Clear Windows Event Logs T1070.001
						Clear Linux or Mac System Logs T1070.002
						Impair Defenses T1562
						Disable or Modify Tools T1562.001

Suggested Mitigation Steps

Apply Security Patches

Patch known vulnerabilities: Prioritize patching for internet-facing applications such as MOVEit, Citrix, Fortinet VPNs, RDP services, and Exchange servers.
Automate patch management: Use vulnerability management tools to identify and remediate unpatched systems on a regular basis.
Monitor for exploits: Track CVEs commonly exploited by Cl0p actors (e.g., CVE-2023-34362 for MOVEit).

Use Multi-Factor Authentication (MFA)

Enforce MFA across all accounts, especially for privileged users and remote access tools.
Use phishing-resistant MFA methods (e.g., hardware tokens, authenticator apps) where possible.
Monitor for legacy authentication protocols that bypass MFA.

Disable Unused or Risky Services

Disable RDP or restrict it to a VPN with strict access controls.
Implement Network Level Authentication (NLA) for any remaining RDP use.
Disable unused SMB shares, remote WMI, and PowerShell remoting if not needed.

Network Segmentation

Separate critical assets (e.g., backups, domain controllers, industrial control systems) using VLANs or firewalls.
Enforce least privilege access between network zones.
Prevent lateral movement by limiting admin account use across systems.

Endpoint Detection and Response (EDR)

Deploy advanced EDR/XDR solutions capable of detecting:
Suspicious PowerShell commands
Tools like Cobalt Strike, Mimikatz, or RClone
Attempts to create scheduled tasks for persistence or exfiltration

Block execution of unsigned or obfuscated scripts

Monitor for:
vssadmin.exe delete shadows
wbadmin delete catalog
schtasks.exe /create with suspicious arguments