REDLab Product Security Newsletter

Cohesity REDLab is a fully isolated security testing environment, hosted and managed by Cohesity, designed for comprehensive malware research and analysis. Within REDLab, live malware is executed to rigorously stress test Cohesity solutions, ensuring that products are resilient against real-world cyber threats. This process enhances the understanding of effective data protection and security methodologies. The insights gained provide valuable guidance to both security and data protection teams, reinforcing confidence in data safety and the cyber resilience offered by Cohesity solutions.

This newsletter provides monthly updates on the most impactful ransomware strains evaluated in REDLab, along with comprehensive findings concerning detection and recovery procedures.

Cohesity DataProtect and NetBackup in REDLab

REDLab incorporates both Cohesity DataProtect and Cohesity NetBackup platforms to enable extensive testing against malware and sophisticated cyberattacks. Through live malware execution, advanced exploit simulation, and modern attack techniques, REDLab examines the practical robustness of Cohesity's solutions. The air-gapped nature of REDLab ensures comprehensive threat assessment under controlled conditions.

- **Proven Confidence:** Backup and recovery solutions undergo rigorous validation against active, high-level cyber threats, not just theoretical threats or synthetic data.
- **Hardened Defense:** Testing in REDLab verifies that DataProtect and NetBackup offer strong security capabilities, elevating them beyond standard recovery tools to proactive defense mechanisms.
- **Future-Ready:** REDLab continually broadens its testing scope to encompass advanced threat detection and threat hunting, ensuring ongoing adaptability and resilience in response to evolving threats.

REDLab Findings

During this month, a series of malware listed below were intentionally detonated to evaluate product efficacy of Cohesity DataProtect and NetBackup.

Name	Ransomware family
BackLock	BackLock Ransomware Family
Deep	Phobos ransomware family
WarLock	WarLock Group
LeakDB	LeakDB Variant

1. BackLock

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Windows Management Instrumentation (WMI)	T1047	Execution
Process Injection	T1055	Defense Evasion, Privilege Escalation
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Modify Registry	T1112	Defense Evasion
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Hijack Execution Flow	T1574	Persistence, Privilege Escalation, Defense Evasion
Access Token Manipulation	T1134	Defense Evasion, Privilege Escalation
OS Credential Dumping	T1003	Credential Access
File and Directory Discovery	T1083	Discovery

Malware impact post execution

BackLock encrypted user and system data, renaming each file with a unique victim ID and ".backlock" extension. It dropped README.TXT as its ransom note and actively killed processes holding open database, document and productivity files to maximize encryption coverage. BackLock is commonly delivered through phishing, drive-by downloads and RDP brute-force attacks. It has also been observed in campaigns abusing vulnerabilities in MOVEit Transfer and Citrix NetScaler environments.

Results

After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client it encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated.

2. Deep

Technique Name	MITRE ATT&CK ID	Tactic(s)
Scheduled Task/Job	T1053	Persistence, Privilege Escalation
Command and Scripting Interpreter	T1059	Execution
Hidden Files and Directories	T1564.001	Defense Evasion
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Access Token Manipulation	T1134	Defense Evasion, Privilege Escalation
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Indicator Removal on Host	T1070	Defense Evasion
Impair Defenses	T1562	Defense Evasion
File and Directory Permissions Modification	T1222	Defense Evasion

Malware impact post execution

Deep (Phobos) appends a victim ID and attacker email to filenames followed by the ".deep" extension. It drops info.hta and info.txt as ransom notes. This strain is known for terminating database, Office and mail client processes to unlock files for encryption. It is typically deployed via RDP intrusion, SmokeLoader-based loaders, phishing attachments and brute-force credential attacks.

Results

After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client it encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated.

3. WarLock

Technique Name	MITRE ATT&CK ID	Tactic(s)
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Software Packing	T1027.002	Defense Evasion
NTFS File Attribute Abuse	T1564.004	Defense Evasion
Impair Defenses	T1562	Defense Evasion
Credential Dumping	T1003	Credential Access
Unsecured Credentials	T1552	Credential Access
System Service Discovery	T1007	Discovery
Network Share Discovery	T1135	Discovery
File and Directory Discovery	T1083	Discovery
Peripheral Device Discovery	T1120	Discovery
Data Encrypted for Impact	T1486	Impact
Service Stop	T1489	Impact

Malware impact post execution

WarLock is a modern double-extortion ransomware used by the group tracked as GOLD SALEM / Storm-2603. It commonly exploits Microsoft SharePoint zero-day vulnerabilities (ToolShell chain: CVE-2025-49704, -49706, -53770/71) to gain initial access. Attackers deploy ASPX web shells (spinstall0.aspx), extract ASP.NET MachineKeys, harvest credentials via Mimikatz and move laterally using PsExec and WMI. The payload encrypts files with “.x2anylock” and drops How to decrypt my data.txt.

Results

After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client it encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated.

4. LeakDB

Technique Name	MITRE ATT&CK ID	Tactic(s)
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Access Token Manipulation	T1134	Defense Evasion, Privilege Escalation
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Indicator Removal on Host	T1070	Defense Evasion
File and Directory Permissions Modification	T1222	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
Impair Defenses	T1562	Defense Evasion
Credential Dumping	T1003	Credential Access
File and Directory Discovery	T1083	Discovery
Network Share Discovery	T1135	Discovery
Application Layer Protocol	T1071	Command and Control
Inhibit System Recovery	T1490	Impact

Malware impact post execution

LeakDB is an enterprise-targeted Phobos variant that appends victim ID + attacker email + ".LEAKDB". It terminates processes using open database, document and mail files to accelerate encryption. It drops info.hta and info.txt in all affected directories. LeakDB also deletes Volume Shadow Copies to prevent local recovery and maintains persistence via %LOCALAPPDATA% copies and registry Run keys.

Results

After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client it encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated.

Summary

- For all the ransomware strains described earlier, in the case of the Data Protect, Client backup operations remained unaffected. Despite the ransomware attack, backups were executed successfully, demonstrating the platform's resilience and ability to maintain data protection under adverse conditions and recovery was validated as successful.

- In case of BackLock, Deep, WarLock and LeakDB ransomware strains, data on NetBackup client is encrypted along with NetBackup configuration files and a backup anomaly that detects unusual behavior with respect to offline clients was generated.

For more information on REDLab please visit https://cohesity.com/redlab