COHESITY REDLab

NEWSLETTER | August 2025

What's new?

Welcome to the REDLab newsletter that provides you with monthly updates on the Cohesity REDLab initiative.

REDLab is a fully isolated security testing facility, hosted and managed by Cohesity, to research and study ransomware and malware. The Cohesity REDLab stress tests our solutions to ensure that our products are hardened against attacks, protecting both the backup data and administrative interfaces. This helps drive a deeper understanding of how to secure your data protection processes and data. It provides meaningful and actionable insights to both security teams and data protection teams when anomalies are detected. This ensures that the data is safe, protected, and that you can be confident in the cyber resilience that Cohesity solutions offer.

Video: Cohesity REDLab helps build stronger defenses against ransomware

Cohesity Trust Center: Learn more about Cohesity REDLab

Now validating Cohesity DataProtect in REDLab

To deepen our commitment, we've expanded the scope of Cohesity REDLab, our proprietary lab, to include Cohesity DataProtect. REDLab is where we rigorously test the real-world resilience of our products using live malware, advanced exploits, and modern attack techniques. Our REDLab is an air-gapped environment designed to allow full-spectrum threat testing while protecting Cohesity infrastructure.

For IT and security leaders, this means confidence that your backup and recovery solutions have been tested to deliver the highest levels of data security. They're hardened and tested components of your cybersecurity strategy.

Since REDLab was built in early 2023, the focus has been on validating Cohesity NetBackup software and NetBackup appliances. With the addition of DataProtect, we're raising the bar,ensuring that more of our platform is hardened against advanced threats before they reach your environment.

We now continuously validate DataProtect's product security postureand will expand to include threat detection and threat hunting in the future,all under real-world and fully isolated conditions.

Here are few of the latest ransomware families and their behavioral patterns that were studied in the REDLab:

Name	Ransomware family	Behavioral pattern
MakOp	Phobos Ransomware group	Phishing, External Remote Services, PowerShell, Registry Run Keys / Startup Folder, Process Injection, Obfuscated Files or Information, File and Directory Discovery, Remote Desktop Protocol, Data from Local System, Web Protocols, Data Encrypted for Impact, Inhibit System Recovery
ViceSociety	ViceSociety Ransomware Gang	PowerShell, Registry Run Keys / Startup Folder, Process Injection, Obfuscated Files or Information, Credential Dumping, System Information Discovery, Remote File Copy, Data from Local System
Cephalus	Cephalus Ransomware Group	Execution, Defense evasion, Credential access, PowerShell, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies using vssadmin utility
Handala	Handala Ransomware Group	Disk Structure Wipe, Spear Phishing Attachment, Command and Scripting Interpreter, Obfuscated Files or Information, Time Based Evasion, AutoHotKey & AutoIT, Delete shadow copies

REDLab findings:

- **MakOp (attack on NetBackup and Data Protect client):**
    - **Family**: Phobos Ransomware group | **Behavior pattern**: Phishing, External Remote Services, PowerShell, Registry Run Keys / Startup Folder, Process Injection, Obfuscated Files or Information, File and Directory Discovery, Remote Desktop Protocol, Data from Local System, Web Protocols, Data Encrypted for Impact, Inhibit System Recovery
    - **Know Me**: Makop ransomware is actively targeting organizations including critical sectors. Makop ransomware encrypts the files on the victim's systems and asks for ransom payment in bitcoin. Makop is an offshoot of the PHOBOS ransomware variant and operates under an affiliate structure but has GUI based interface. Makop Ransomware leverages different techniques to enter organizations' networks and inject the payload. Makop Ransomware uses AES-256 algorithm for encrypting files and typically adds the “.makop” extension to the encrypted files.
    - **Attack Pattern**: After the attack, this ransomware encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated. Also, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully.

- **ViceSociety (attack on NetBackup and Data Protect client):**
    - **Family**: ViceSociety Ransomware Gang | **Behavior pattern**: PowerShell, Registry Run Keys / Startup Folder, Process Injection, Obfuscated Files or Information, Credential Dumping, System Information Discovery, Remote File Copy, Data from Local System
    - **Know Me**: Vice Society is a multi-pronged extortion and ransomware group which emerged in early to mid 2021. Vice Society Ransomware uses AES and RSA encryption. After the attack, it encrypted files and appended with a ".v-society.[victim's_ID]" extension. For example, a file that was initially titled "security.pdf" would appear as "security.pdf.v-society.923-C3D-30D". Once this process is complete, a ransom note named "!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT" is created.
    - **Attack Pattern**: After the attack, this ransomware encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated. Also, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully.

REDLab findings:

- **Cephalus (attack on NetBackup and Data Protect client):**
    - **Family**: Cephalus Ransomware group | **Behavior pattern**: Execution, Defense evasion, Credential access, PowerShell, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies using vssadmin utility
    - **Know Me**: Cephalus, a ransomware group with no clear geopolitical alignment, revealed its operations during two coordinated attacks in mid-August 2025. The breaches exploited weak Remote Desktop Protocol (RDP) credentials lacking multi-factor authentication. The attackers exfiltrated data using the MEGA cloud storage platform and files were encrypted and appended with a ".sss" extension. For example, a file named "securitycomm.docx" would appear as "securitycomm.docx.sss" after encryption. The ransom note, typically named recover.txt, began with "We're Cephalus".
    - **Attack Pattern**: After the attack, this ransomware encrypted the user data. A Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated. Also, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully.

- **Handala (attack on NetBackup and Data Protect client):**
    - **Family**: Handala Ransomware Group | **Behaviour pattern**: Disk Structure Wipe, Spear Phishing Attachment, Command and Scripting Interpreter, Obfuscated Files or Information, Time Based Evasion, AutoHotKey & AutoIT, Delete shadow copies
    - **Know Me**: Handala is a pro-Palestinian hacktivist group, exposed its destructive capabilities during a coordinated campaign targeting Israeli infrastructure between June and July 2024. During our tests post attack, Handala executed a destructive wiper payload that overwrote files using randomized 4096-byte blocks followed by zero-filled segments, effectively rendering them unrecoverable. Unlike traditional ransomware, Handala did not append any extension to the wiped files.
    - **Attack Pattern**: After the attack, this ransomware encrypted the user data. A Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated**.** Also, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully.

Impact of attacks by the given ransomware families

- In case of MakOp and ViceSociety ransomwares, data on NetBackup client is encrypted along with NetBackup configuration files or communication between NetBackup client and primary server is compromised that resulted in failures of backup jobs.

- While in case of Cephalus and Handala ransomwares, Job Metadata and Image Entropy anomalies are observed, the backup of application data is successful. In the attack mentioned earlier, user's application files are encrypted but NetBackup configuration files are not compromised.

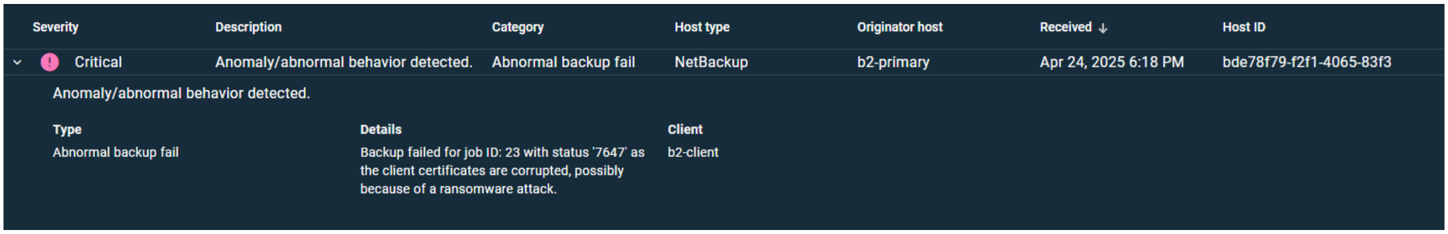
- For all the ransomware strains described earlier, in the case of the Data Protect, Client backup operations remained unaffected. Despite the ransomware attack, backups were executed successfully, demonstrating the platform's resilience and ability to maintain data protection under adverse conditions.

Recommended solutions:

Data on NetBackup client is encrypted along with NetBackup configuration files

- Client Offline backup anomaly detects unusual network communication behaviour between NetBackup primary servers and clients. It checks the health of certificates that are deployed on the NetBackup client and starts the anomaly detection process.
- When the anomaly is detected, the Client Offline anomaly creates a critical audit event that indicates failed communication with the NetBackup client.

The following screenshot shows the data from REDLab:



Severity	Description	Category	Host type	Originator host	Received ↓	Host ID
Critical	Anomaly/abnormal behavior detected.	Abnormal backup fail	NetBackup	b2-primary	Apr 24, 2025 6:18 PM	bde78f79-f2f1-4065-83f3

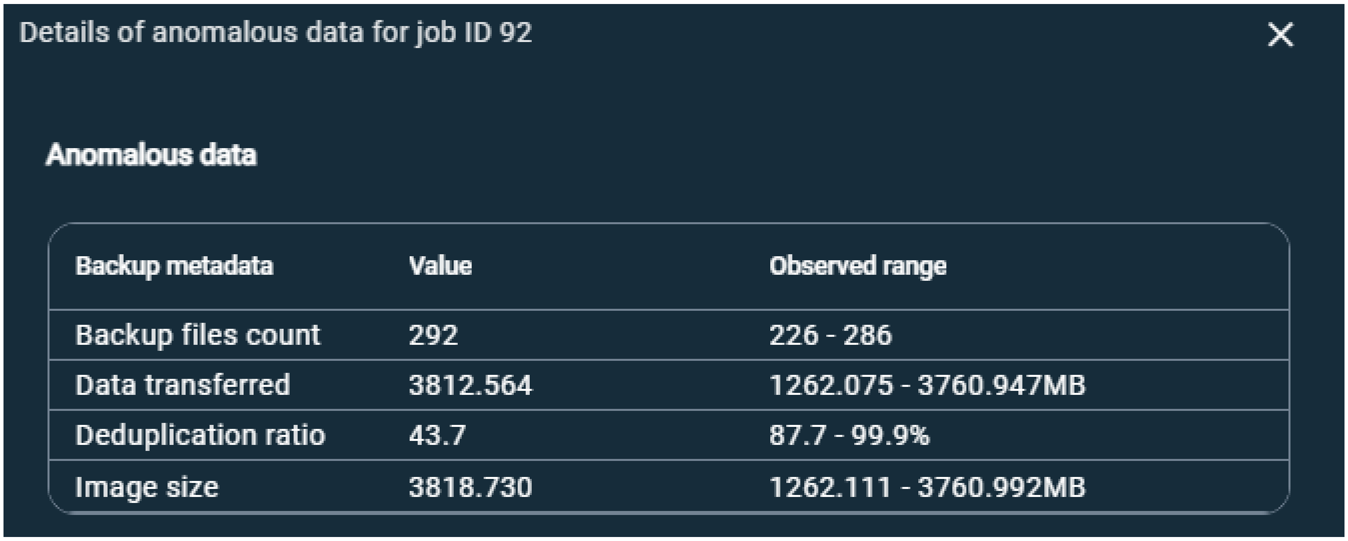
Anomaly/abnormal behavior detected.

Type	Details	Client
Abnormal backup fail	Backup failed for job ID: 23 with status '7647' as the client certificates are corrupted, possibly because of a ransomware attack.	b2-client

Data on NetBackup client is encrypted however NetBackup configuration files are intact and backup jobs are successful.

- **Job Metadata Anomaly:**
    - NetBackup uses machine learning (ML)-driven anomaly detection to detect anomalies. In this case, the change of backup file count, data transferred, data deduplication rate, image size and total time are detected by the ML algorithm, and an alert is generated.

Refer to the following screenshot:



Details of anomalous data for job ID 92

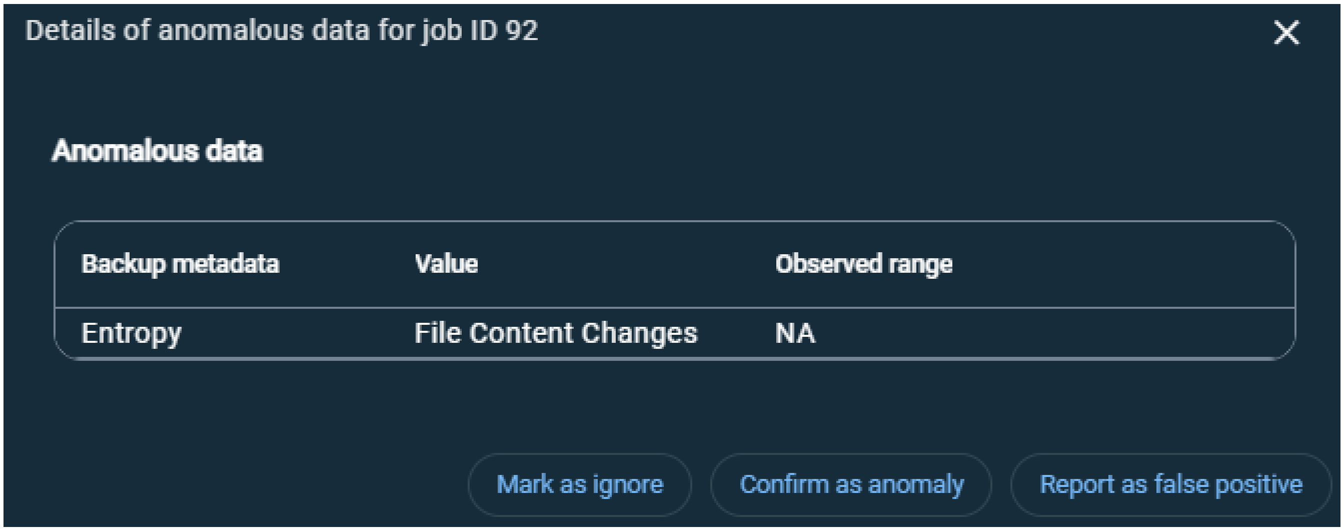
Anomalous data

Backup metadata	Value	Observed range
Backup files count	292	226 - 286
Data transferred	3812.564	1262.075 - 3760.947MB
Deduplication ratio	43.7	87.7 - 99.9%
Image size	3818.730	1262.111 - 3760.992MB

See more information about the Job Metadata anomaly here.

- **Image Entropy Data Anomaly:**
    - NetBackup computes an additional risk signal in-line, called entropy. It improves the quality of detected anomalies. Entropy is a measure of randomness of file contents. Threat vectors that encrypt files tend to abruptly change the entropy.
    - The entropy metric is used with the anomaly detection mechanism to help detect potential malicious activity. When this indicates anomaly activities, it is recommended to check the system for potential malicious actors. If suspicious activities are found, do not use those images as a recovery point.

Refer to the following screenshot:



Backup metadata	Value	Observed range
Entropy	File Content Changes	NA

See more information about the Image Entropy Data anomaly here.

Security Feature Overview

Detection of database corruption in Oracle and Microsoft SQL Server

NetBackup 11.0 and later versions can detect database corruption scenarios in Oracle and Microsoft SQL Server. After detecting database corruption, the associated backup job fails with status code 5464. To generate an alert for such a scenario, configure the Monitor database corruption in workloads during job failures anomaly detection option.

Configuring Detection of database corruption in Oracle and Microsoft SQL Server:

After you enable anomaly detection, anomaly data gathering, detection service, and events are enabled. You can configure specific settings to detect system anomalies in your domain.

See About system anomaly detection.

To configure detection of database corruption system anomaly detection settings:

1. Sign in to the NetBackup web UI.
2. On the left, click Detection and reporting > Anomaly detection.
3. On the top right, click Anomaly detection settings > System anomaly detection configuration.
4. On the System anomaly detection configuration screen, configure the following settings:
    - System anomaly detection > Monitor database corruption in workloads during job failures

About Detection of database corruption in Oracle and Microsoft SQL Server:

- This anomaly monitors database corruption in workloads like Microsoft SQL Server and Oracle during backup job failures.
- Select the checkbox to generate an anomaly alert when NetBackup detects backup job failures because of database corruption in workloads like Microsoft SQL Server and Oracle.
- If database corruption in a workload is detected, status code 5464 is attributed to the parent job that is displayed in the Activity monitor > Jobs tab.
- Click the status code number to view information about this status code in the Cohesity Knowledge Base. (See the NetBackup Status Codes Reference Guide)

Note: For detecting database corruption in Microsoft SQL Server, the 'Microsoft SQL Server checksum' option must be set to 'Fail on Error' during MS SQL Server policy configuration.

More information around detection of database corruption can be found in the NetBackup™ Security and Encryption Guide.

Research references:

- https://www.cisa.gov – Threat intelligence data and most pressing issues that CISA tracks, and notifications issued by government organizations.
- https://www.virustotal.com – Intelligence data, ransomware, or malware samples, discover threat commonalities and track new variants of surveilled malware families.
- https://www.hybrid-analysis.com – Malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.
- https://www.enigmasoftware.com/ - PC security alerts & news and Advanced Analytics
- https://www.cyborgsecurity.com/ - Provides a library of expertly crafted constantly updated threat hunting news and content.
- https://www.avertium.com/ - Threat Summary and Blogs
- https://unit42.paloaltonetworks.com/ - Research blogs and Analysis of strains
- https://www.cert-in.org.in/ - Collection, forecast, and alerts of cyber security incidents.
- https://www.pcrisk.com/ - Latest digital threats and malware infections
- https://thecyberexpress.com/ - Intelligence data and news around latest ransomware attacks
- https://www.blackfog.com – Get monthly news around attacks and details of impacted organizations.
- https://www.bleepingcomputer.com – Daily news of recent activities carried out by ransomware gangs and methods used to infiltrate enterprises.
- https://www.truesec.com/ - Blogs and IOC’s
- https://www.csk.gov.in/ - Threat Alerts and Security Announcements
- https://www.sentinelone.com – Analytics data from various security vendors and insights around behavior pattens for each ransomware family
- https://decoded.avast.io/ - Latest threat research, ransomware analysis and IOC’s