COHESITY REDLab

NEWSLETTER | MAY, 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.

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

Name	Ransomware family	Behavioral pattern
Scrypt	Scrypt malware family	Deobfuscate/Decode Files or Information, Debugger Evasion, Defacement, File and Directory Discovery, File and Directory Permissions Modification, Impair Defenses, Inhibit System Recovery, Masquerading
Snatch	Snatch ransomware group	Obfuscated Files or Information, Data Encrypted for Impact, Disk Content Wipe, Indicator Removal, Inhibit System Recovery, Modify Registry, Network Share Discovery, Permission Groups Discovery

REDLab findings:

- **Scrypt (attack on NetBackup client):**
  - **Family**: Scrypt malware family | **Behavior pattern**: Deobfuscate/Decode Files or Information, Debugger Evasion, Defacement, File and Directory Discovery, File and Directory Permissions Modification, Impair Defenses, Inhibit System Recovery, Masquerading
  - **Know Me:** Scrypt ransomware belongs to Scrypt malware group. It employs AES-256 bit to encrypt files and demand payment for their decryption. Post attack, this ransomware encrypted files and appended their filenames with a ".scrypt" extension. For example, a file initially named "b2.jpg" looked like "b2.jpg.scrypt", "edr.pdf" like "edr.pdf.scrypt", etc. After the encryption process was completed, a ransom-demanding message titled "readme.txt" was also dropped. This note lacked critical information, which suggests that this iteration of Scrypt is still in development.
  - **Attack Pattern:** After the attack, this ransomware encrypted the user data and system files. A system anomaly that detected unusual behaviour with respect to offline clients was generated.

- **Snatch (attack on NetBackup client):**
  - **Family:** Snatch ransomware group | **Behavior pattern**: Obfuscated Files or Information, Data Encrypted for Impact, Disk Content Wipe, Indicator Removal, Inhibit System Recovery, Modify Registry, Network Share Discovery, Permission Groups Discovery
  - **Know Me:** Snatch ransomware is a strain known for its distinct approach and operational tactics. After an attack, files that were previously named something like "report.docx" are renamed to an encrypted format, for example, “report.docx.snatch”, clearly indicating encryption by the ransomware. Victims are left with a ransom note typically named something like “HOW TO RESTORE YOUR FILES.TXT”, which instructs them to reach out to the attackers through specific email addresses for decryption steps. A notable feature of Snatch is its capability to force a system reboot into Safe Mode, where many security tools and antivirus programs are disabled, making it easier for ransomware to execute without interference. Additionally, it attempts to delete Volume Shadow Copies, which prevents victims from restoring their files using built-in Windows recovery features.
  - **Attack Pattern:** After the attack, this ransomware encrypted the user data and system files. A system anomaly that detected unusual behaviour with respect to offline clients was generated.

Impact of attacks on NetBackup by the given ransomware families

The following observations are noted when a targeted ransomware attack is carried out on a NetBackup client:

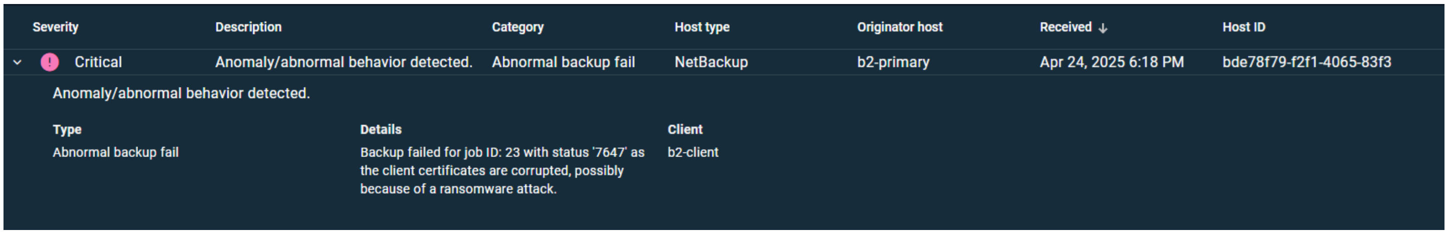
- Data on NetBackup client is encrypted along with NetBackup configuration files or communication between NetBackup client and primary server is compromised that resulted in failures of backup jobs.

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.

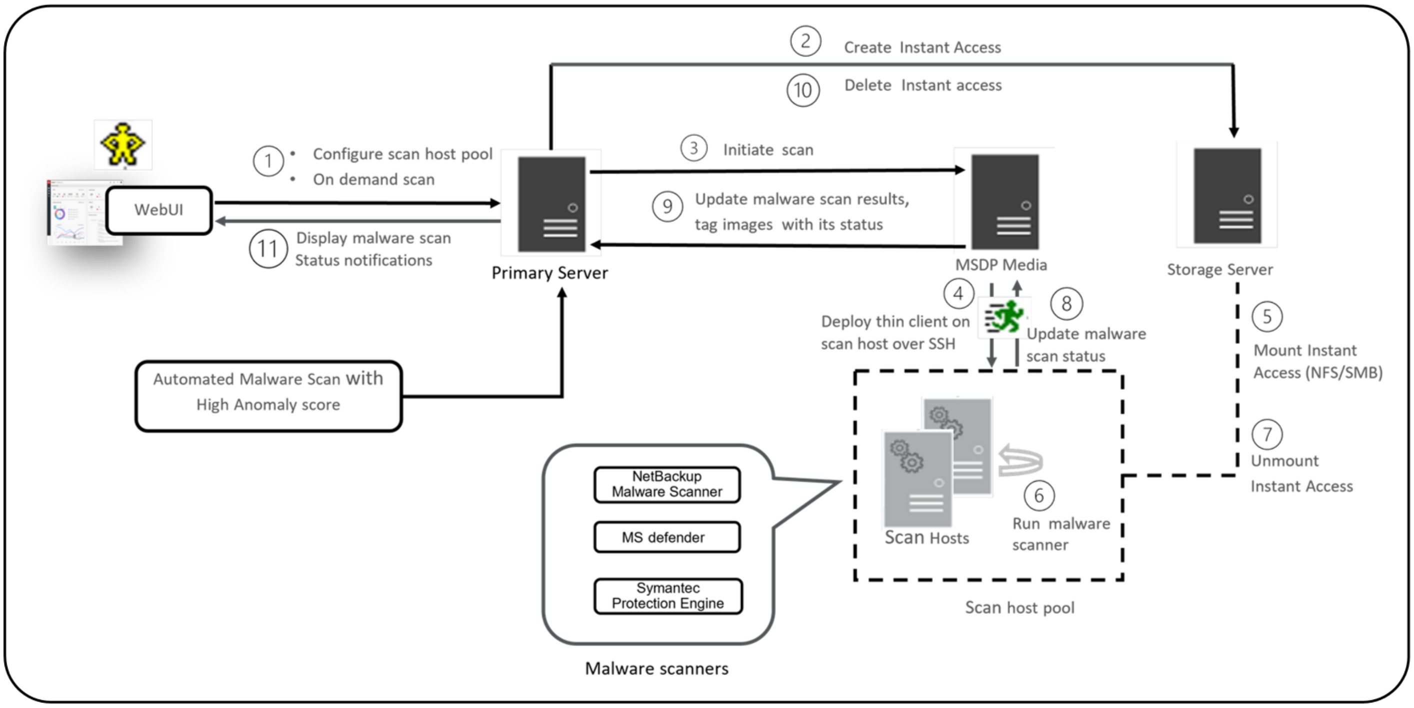
Type	Details	Client
Abnormal backup fail	Backup failed for job ID: 23 with status '7647' as the client certificates are corrupted, possibly because of a ransomware attack.	b2-client

NetBackup feature overview

Malware scanning support for MSDP backup images using Agentless host as the scan host

NetBackup 11.x and later provides support for Agentless host as the scan host to perform the malware scan.

The following figure displays the workflow of malware scanning for MSDP backup images:


2 Create Instant Access
10 Delete Instant access
1 • Configure scan host pool
• On demand scan
WebUI
11 Display malware scan Status notifications
3 Initiate scan
9 Update malware scan results, tag images with its status
Primary Server
MSDP Media
Storage Server
4 Deploy thin client on scan host over SSH
8 Update malware scan status
5 Mount Instant Access (NFS/SMB)
7 Unmount Instant Access
Automated Malware Scan with High Anomaly score
NetBackup Malware Scanner
MS defender
Symantec Protection Engine
Malware scanners
Scan Hosts
6 Run malware scanner
Scan host pool

The following steps depict the workflow for malware scanning for MSDP backup images:

1. After triggering On Demand Scan, primary server will validate backup images and create scan jobs for each eligible backup image and identify available scan host for them. The backup images are validated based on the following criteria:

   - Backup image must be supported for malware detection.
   - Backup image must have a valid Instant Access copy.
   - For an on-demand scan, no existing scan must be running for same backup image. For DNAS the related streams are also considered.
   - Malware detection does not support media server associated with storage.
   - Unable to get information for backup image from catalog.

2. After the backup images are queued for an on-demand scan, the primary server identifies the storage server. An instant access mount is created on the storage server of the configured share type that is specified in scan host pool.

   Note: Currently the primary server starts 50 scan threads at a time. After the thread is available, it processes the next job in the queue. Until then the queued jobs are in the pending state.

   For NetBackup 10.3 and later, large backups are scanned in batches of 500K files. Each batch is scanned by a separate scan thread. For recovery time scan, scan in batches feature is not supported.

3. Primary server identifies available and supported MSDP media server and instructs the media server to initiate the malware scan.

   If the scan host connectivity type is Agentless host, then it instructs the media server to initiate the malware scan.

4. MSDP media server deploys the thin client on the scan host over SSH.

5. Thin client mounts the instant access mount on the scan host.

6. Scan is initiated using the malware tool that is configured in the scan host pool.

   Media server fetches the progress of scan from scan host and updates the primary server.

7. After the scan is completed, the scan host unmounts the instant access mount from the scan host.

8. Malware scan status is updated to the media server over SSH. Scan logs are copied to the media server log directory.

9. Media server updates the scan status and the infected file list along with skipped file list (if any infected files) to the primary server.

10. Primary server updates the scan results and deletes instant access.

11. Malware scan status notification is generated.

12. Malware scan will timeout in case there is no update on scan. Default timeout period is 48 hours.

Malware detection performs an automated cleanup of eligible scan jobs that are older than 30 days.

You can download a malware scanner from the Microsoft Azure Marketplace and the AWS Marketplace. Follow the instructions on how to install, configure, and use the malware scanner for AWS and Azure.
AWS: AWS Marketplace and NetBackup Marketplace Deployment on AWS Cloud
Microsoft Azure: Microsoft Azure Marketplace and Microsoft Azure Marketplace

More information around workflow for malware scanning can be found in the NetBackup™ Web UI Administrator's 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://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.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