COHESITY REDLab

NEWSLETTER | June, 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
Lynx	Lynx Ransomware group	Data exfiltration, Terminating processes and Services, Directory enumeration and encryption of files, Deleting Shadow copies, Encrypting all mounted drives and shared folders, Changing the background image
Prince	Prince Ransomware (OS)	Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Collection, Command and Control, Impact, Process Discovery, File and Directory Permissions Modification, Data Encrypted for Impact

REDLab findings:

- **Lynx (attack on NetBackup client):**
    - **Family**: Lynx Ransomware group | **Behavior pattern**: Data exfiltration, Terminating processes and Services, Directory enumeration and encryption of files, Deleting Shadow copies, Encrypting all mounted drives and shared folders, Changing the background image
    - **Know Me**: Lynx ransomware is a sophisticated malware threat that is active since mid-2024. Post attack, Lynx encrypted the files, appending a '.lynx' extension to the filenames. It also deleted backup files such as shadow copies to hinder recovery efforts. For example, a file initially named "document.docx" appears as "document.docx.lynx" after encryption. This malware shares similarities with the previous INC ransomware, indicating that the attackers may have acquired the INC ransomware source code. Lynx ransomware is designed to target enterprises, making it a significant threat to business operations.
    - **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.

- **Prince (attack on NetBackup client):**
    - **Family**: Prince Ransomware (OS) | **Behavior pattern**: Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Collection, Command and Control, Impact, Process Discovery, File and Directory Permissions Modification, Data Encrypted for Impact
    - **Know Me**: Prince ransomware employs a unique combination of cryptographic techniques, a mixture of ChaCha20 and ECIES cryptography to encrypt files securely so that they cannot be recovered by traditional recovery tools. Unlike many ransomware variants that repurpose existing code, Prince is written entirely from scratch in the Go programming language. After attack, it encrypted files and appended their filenames with a ".ran" extension. For example, a file originally named "b2.jpg" looked like "b2.jpg.ran" and dropped a ransom note titled "Decryption Instructions.txt"
    - **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**.**

Impact of attacks on NetBackup by the given ransomware families

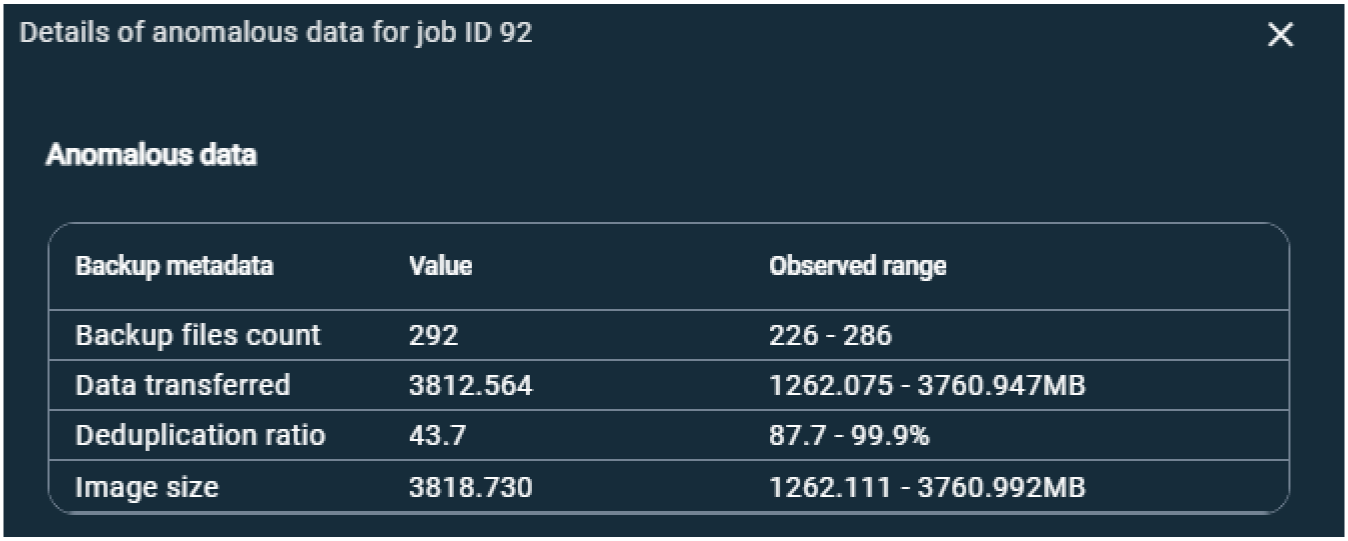
- In certain attacks, NetBackup configuration files are not compromised, but the application data is encrypted. The backup of application data is successful. Job Metadata and Image Entropy anomalies are observed.

Recommended solution:

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:



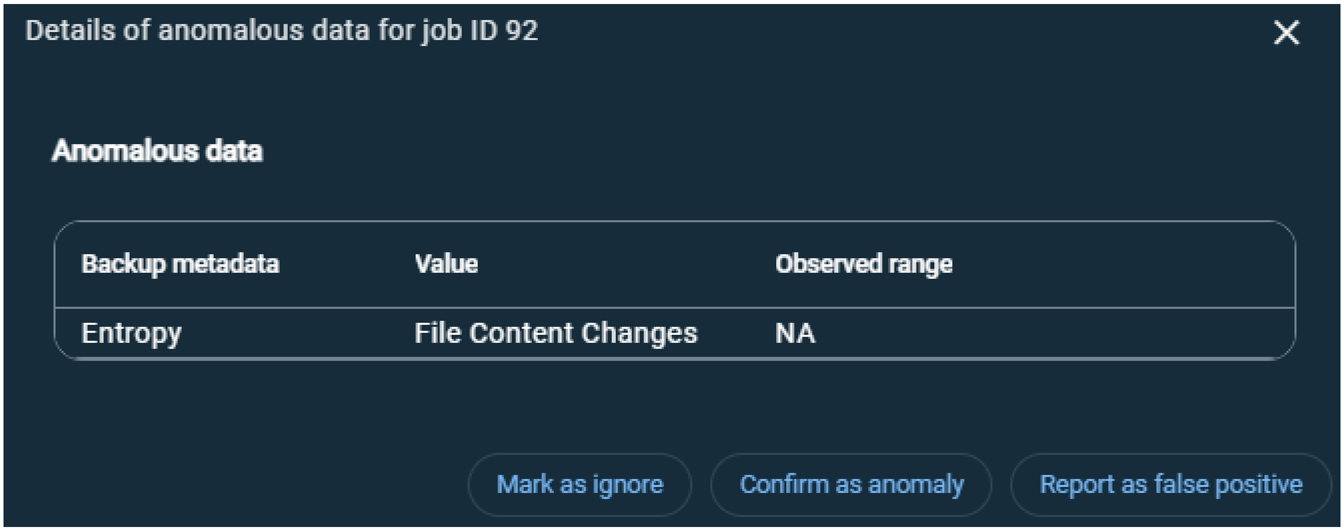
Details of anomalous data for job ID 92

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

- **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:



Details of anomalous data for job ID 92

Anomalous data

Backup metadata	Value	Observed range
Entropy	File Content Changes	NA

See more information about the Job Metadata anomaly here.

See more information about the Image Entropy Data anomaly here.

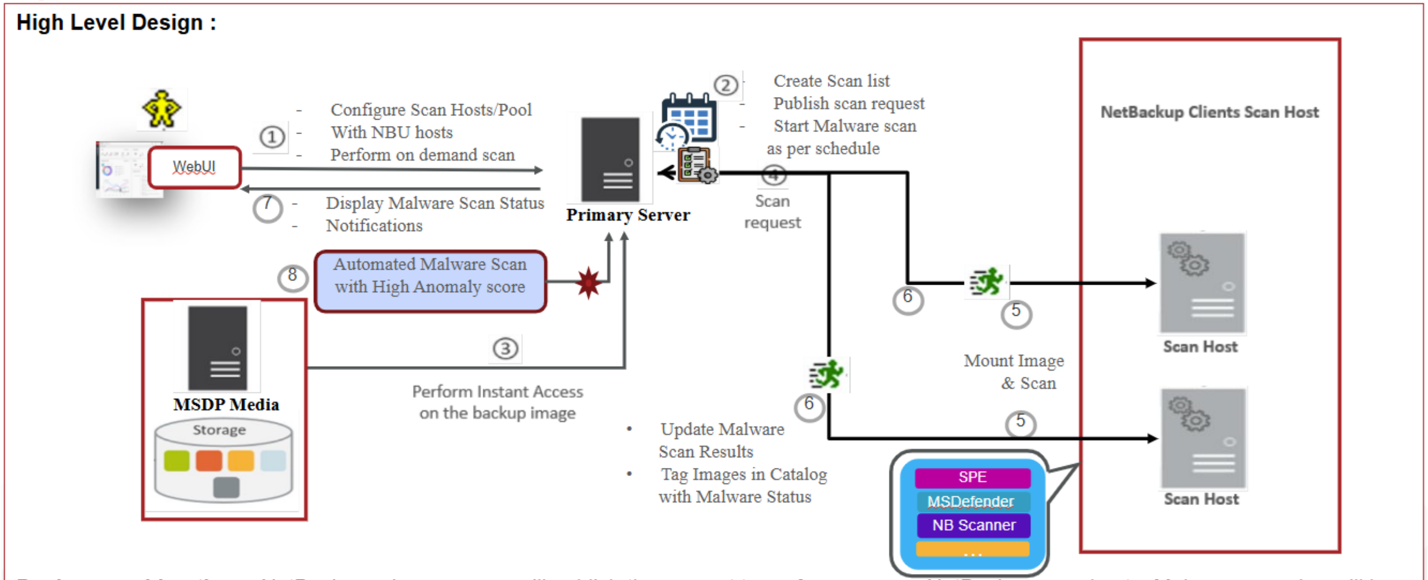
NetBackup feature overview

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

NetBackup 11.0 and later versions provide support for NetBackup client and Agentless host as the scan host to perform the malware scan.

The Agentless host requires SSH credentials to connect and perform the scan through thin client. The NetBackup client uses client secure communication and performs the scan.

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


High Level Design :
WebUI
1
- Configure Scan Hosts/Pool
- With NBU hosts
- Perform on demand scan
7
- Display Malware Scan Status
- Notifications
Primary Server
2
- Create Scan list
- Publish scan request
- Start Malware scan as per schedule
4
Scan request
8
Automated Malware Scan with High Anomaly score
3
Perform Instant Access on the backup image
MSDP Media
Storage
6
5
Mount Image & Scan
6
5
• Update Malware Scan Results
• Tag Images in Catalog with Malware Status
SPE
MSDefender
NB Scanner
...
NetBackup Clients Scan Host
Scan Host
Scan Host

Design considerations: NetBackup primary server will publish the request to perform scan on NetBackup scan hosts. Malware scanning will be performed with supported malware tools.

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. 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.
    - Catalog must have details of backup image.

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 versions, 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 the available and supported MSDP media server and instructs the media server to initiate the malware scan.

    If the scan host connectivity type is NetBackup client, then the primary server identifies the available NetBackup client scan host from the scan host pool and instructs the NetBackup client scan host to initiate the malware scan.

4. NetBackup client as the scan host:
   - NetBackup client mounts the instant access mount on the scan host.
   - Scan is initiated using the malware tool that is configured in the scan host pool.
   - NetBackup client performs the scan operation and updates the progress of scan from scan host to the primary server.

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

NetBackup client as the scan host:

- Malware scan status is updated to the primary server. Scan logs are copied to the NetBackup client scan host log directory (nbmalwarescanner).
- NetBackup client scan host updates the scan status and the infected file list along with the skipped file list (if any infected files) to the primary server.

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

7. Malware scan status notification is generated.

8. Malware scan will timeout if there is no update on scan. The default timeout period is 48 hours.

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

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