

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 posture and 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
Gagakick	Gagakick Ransomware group	Data Encrypted for Impact, Disk Content Wipe, Indicator Removal, Inhibit System Recovery, Modify Registry, Network Share Discovery, Permission Groups Discovery, File and Directory discovery, Process Discovery
LockBit 5.0	Lockbit Ransomware Gang	Execution, Obfuscation, Lateral movement, Disables windows event tracing, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies, Double-extortion, privilege escalation.
Interlock	Interlock Ransomware Group	Indicator Removal from Tools, Masquerading, Obfuscated Files or Information, System Information Discovery, Virtualization/Sandbox Evasion, Data Encrypted for Impact
Gunra	Gunra Ransomware Group	Execution, Defense evasion, Anti Debugging, Credential access, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies using WMI utility, Double-extortion, Privilege escalation.

REDLab findings:

- **Gagakick (attack on NetBackup and Data Protect client):**

- **Family:** Gagakick Ransomware group | **Behavior pattern:** Data Encrypted for Impact, Disk Content Wipe, Indicator Removal, Inhibit System Recovery, Modify Registry, Network Share Discovery, Permission Groups Discovery, File and Directory discovery, Process Discovery
- **Know Me:** Gagakick is a relatively new ransomware variant that emerged in late 2024, operating as part of the ransomware-as-a-service (RaaS) ecosystem. The malware employs sophisticated encryption using AES-256 algorithm. Gagakick typically appends the "[Unique-Victim-ID].gagakick" extension to encrypted files and creates ransom notes named "README.TXT" in each affected directory. The group is known for targeting small to medium enterprises through compromised RDP connections and phishing campaigns.
- **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.

- **Lockbit 5.0 (attack on NetBackup and Data Protect client):**

- **Family:** Lockbit Ransomware Gang | **Behavior pattern:** Execution, Obfuscation, Lateral movement, Disables windows event tracing, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies, Double-extortion, privilege escalation.
- **Know Me:** LockBit 5.0 represents the latest evolution of the prolific LockBit ransomware family, featuring enhanced evasion techniques and faster encryption speeds. This variant utilizes ChaCha20 encryption algorithm for improved performance and employs advanced anti-analysis measures including ETW (Event Tracing for Windows) disabling to evade detection. LockBit 5.0 appends a randomized 16-character alphanumeric extension following the pattern ".[0-9a-z]{16}" to encrypted files and drops ransom notes named "ReadMeForDecrypt.txt". The group operates a sophisticated RaaS model with leak sites for double extortion, threatening to publish stolen data if ransoms aren't paid.
- **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:

- **Interlock (attack on NetBackup and Data Protect client):**

- **Family:** Interlock Ransomware group | **Behavior pattern:** Indicator Removal from Tools, Masquerading, Obfuscated Files or Information, System Information Discovery, Virtualization/Sandbox Evasion, Data Encrypted for Impact
- **Know Me:** InterLock is a sophisticated ransomware variant first observed in mid-2024, distinguished by its advanced evasion capabilities and targeted approach. The malware employs multiple layers of obfuscation and anti-analysis techniques, including virtual machine detection and sandbox evasion mechanisms. InterLock uses AES-256 encryption with a unique key derivation process and typically appends the ".interlock" extension to encrypted files and creates a ransom notes named "RECOVERY_INSTRUCTIONS.txt".
- **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.

- **Gunra (attack on NetBackup and Data Protect client):**

- **Family:** Gunra Ransomware Group | **Behaviour pattern:** Execution, Defense evasion, Anti Debugging, Credential access, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies using WMI utility, Double-extortion, privilege escalation.
- **Know Me:** Gunra is an emerging ransomware family that surfaced in early 2024, characterized by its sophisticated anti-debugging and analysis resistance features. The malware utilizes a hybrid encryption approach combining Salsa20 stream cipher with RSA-2048 for key protection, offering both speed and security. Gunra appends the ".ENCRT" extension to encrypted files and creates ransom notes titled "R3ADM3.txt" in affected directories.
- **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 Gagakick, Lockbit 5.0 and Interlock 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 Gunra ransomware, 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.

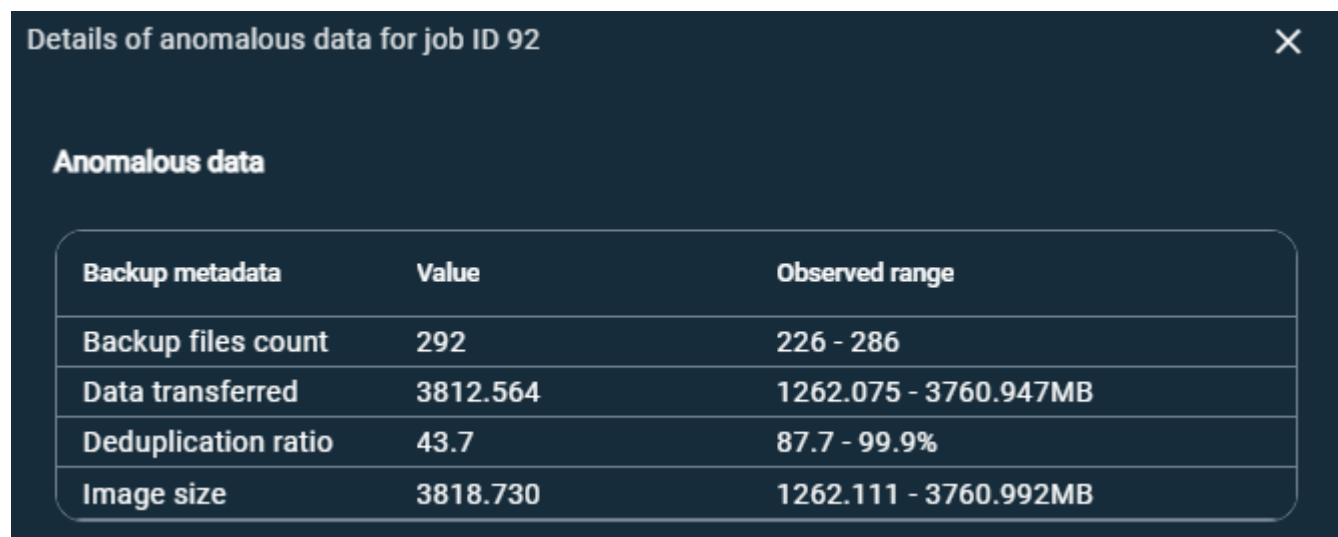
The following screenshot shows the data from REDLab:

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:



The screenshot shows a window titled "Details of anomalous data for job ID 92" with a close button (X) in the top right corner. Below the title is a section labeled "Anomalous data" containing a table with three columns: "Backup metadata", "Value", and "Observed range". The table lists four items: Backup files count (292, range 226 - 286), Data transferred (3812.564, range 1262.075 - 3760.947MB), Deduplication ratio (43.7, range 87.7 - 99.9%), and Image size (3818.730, range 1262.111 - 3760.992MB).

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:



See more information about the Image Entropy Data anomaly [here](#).

Security Feature Overview

Support for Trend Micro malware detection tool

NetBackup 11.0 and later versions now provides support for malware scanning using the Trend Micro Malware Scanner.

Configuring Trend Micro Malware Scanner

Note: The Trend Micro Malware Scanner is currently only supported for Linux

To configure Trend Micro Malware Scanner for Linux :

1. Install Trend Micro Deep Security Manager and Agent from [Trend Business Software Download Center](#).

Note the following:

- Deep Security Manager can be installed on another setup other than the scan host.
 - Deep Security Agent must be installed on the scan host.
 - The minimum required version of Deep Security Agent is 20.0.1-690.
2. Trend Micro Malware Scanner supports malware scanning only through root user. This is due to the following support of `dsa_scan` command in Trend Micro:

If you have root access rights on Linux, you can use the `dsa_scan` command to execute a scan task with specified files or directories, including the subdirectories.

3. Set the environment variable TREND_MICRO_AGENT_PATH in .bashrc file as follows:
For example: `export TREND_MICRO_AGENT_PATH=/opt/ds_agent`

Note:

If you are using NetBackup client as the scan host, then it is recommended to add the same entry in `/usr/opensv/netbackup/bp.conf` configuration file

For example, `TREND_MICRO_AGENT_PATH=/opt/ds_agent`

4. Run the following command on command prompt and verify the output:

```
/opt/ds_agent/dsa_scan --action pass --target <path to scan>
```

More information around support for Trend Micro malware detection tool 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 patterns for each ransomware family
- <https://decoded.avast.io/> - Latest threat research, ransomware analysis and IOC's