

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
Nebula	Nebula Ransomware group	Deobfuscate/Decode Files or Information, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies using vssadmin utility
SatanLocker	Babuk Ransomware group	Obfuscated Files or Information, Data Encrypted for Impact, Disk Content Wipe, Indicator Removal, Inhibit System Recovery, Modify Registry, Deobfuscate Files or Information, File and Directory Discovery

REDLab findings:

- **Nebula (attack on NetBackup client):**

- **Family:** Nebula Ransomware group | **Behavior pattern:** Deobfuscate/Decode Files or Information, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies using vssadmin utility
- **Know Me:** Nebula, a group with pro-Ukrainian agenda, inadvertently exposed its activities during a breach of Russian software company Insoft.ru. The leaked screenshots revealed Meterpreter shells accessing Insoft's infrastructure, likely originating from IPs owned by LimeNet in the Netherlands. During our tests post attack, Nebula encrypted the files using the AES-CBC algorithm, appending a '.lnk.nebula' extension to the filenames. It also deleted backup files such as shadow copies. For example, a file initially named "securitycomm.docx" appears as "securitycomm.docx.lnk.nebula" after encryption.
- **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.

- **SatanLocker (attack on NetBackup client):**

- **Family:** Babuk Ransomware Group | **Behavior pattern:** Obfuscated Files or Information, Data Encrypted for Impact, Indicator Removal, Inhibit System Recovery, Modify Registry, Deobfuscate Files or Information, File and Directory Discovery
- **Know Me:** SatanLock has been active since early April 2025 and is known for its aggressive tactics. SatanLock is linked to several other notorious ransomware families, including Babuk-Bjorka and GD Lockersec. These connections suggest the group is part of a much larger cybercriminal network. After attack, it encrypted files and appended their filenames with a ".satan" extension. For example, a file originally named "offsec.pdf" looked like "offsec.pdf.satan" and dropped a ransom note titled "README_Satanlock.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

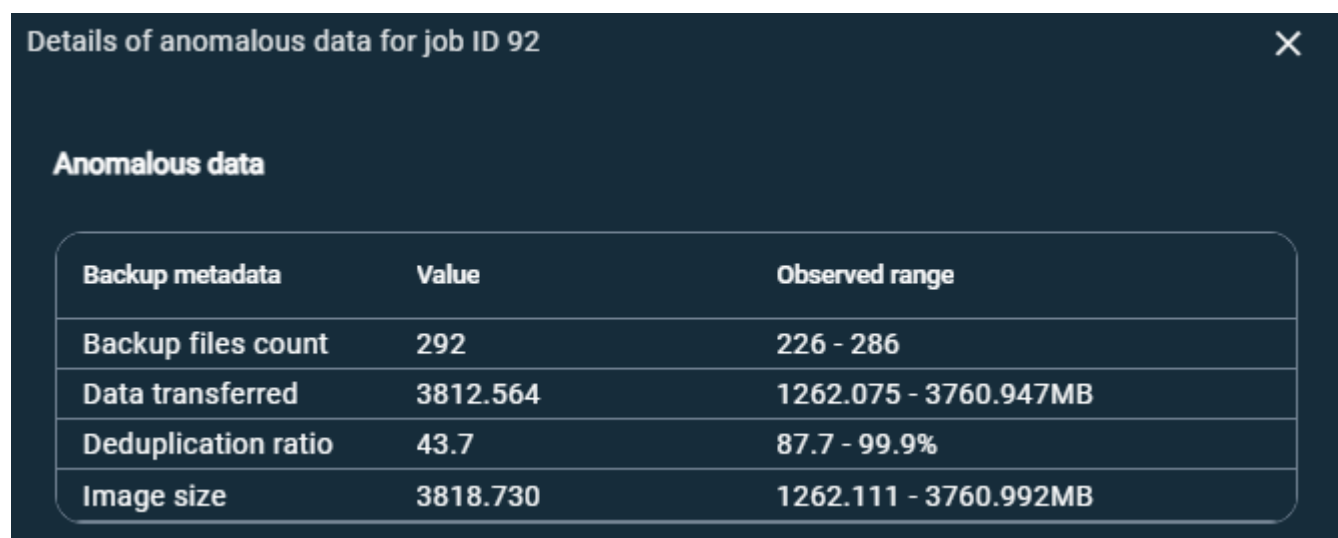
- The backup of application data is successful. In attack mentioned above user's application files are encrypted but NetBackup configuration files are not compromised. Job Metadata and Image Entropy anomalies are observed.

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:



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:



See more information about the Job Metadata anomaly [here](#).

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

NetBackup feature overview

Post-Quantum Cryptography (PQC) support in NetBackup

Starting NetBackup 11.0 now supports Post-Quantum Cryptography (PQC) for TLS 1.3 communication using the Open Quantum Safe (OQS) provider. This enhancement is a step toward preparing NetBackup for a quantum-safe future.

About Post-Quantum Cryptography (PQC):

Post-Quantum Cryptography (PQC) aims to construct public key cryptosystems that are believed to be secure even against quantum computers. While traditional public-key cryptographic systems like RSA, ECC, and DH rely on the computational difficulty of problems like integer factorization and discrete logarithms, quantum computers that leverage Shor's algorithm can solve these problems efficiently.

- PQC focuses on algorithms based on mathematical problems that are resistant to quantum computing attacks, such as lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and hash-based cryptography.
- PQC is crucial for securing communications in a future where quantum computers become practical.
- Adversaries can now intercept and store encrypted communications with the intent to decrypt them in the future when quantum computers are capable of breaking current cryptographic systems.

The transition to quantum-safe cryptography is a proactive measure to ensure long-term confidentiality and security of your data and domain.

PQC support for TLS communication:

NetBackup supports Post-Quantum Cryptography (PQC) for TLS 1.3 communication using the Open Quantum Safe (OQS) provider.

While the OQS provider prepares you for a quantum-safe future, it is currently widely used in experimental and research environments.

Note: It is recommended that you thoroughly assess all associated risks and ensure that the use of the OQS provider aligns with your organization's security policies and compliance requirements before enabling PQC in NetBackup.

- PQC is supported for TLS 1.3 communication using hybrid KEMs.

By default, NetBackup uses x25519_kyber768 TLS group.

- NetBackup does not support PQC in FIPS mode.
- NetBackup 11.0 or later hosts support PQC.

Communication with NetBackup hosts earlier than 11.0 is in a traditional way.

- In NetBackup 11.0, PQC is supported only for RHEL and Windows platforms.
- PQC is currently supported for communication with the following NetBackup components:
 - Secure comms proxies (vnetd proxies)
 - Data In-Transit Encryption (DTE)
 - KMIP
 - cURL clients (libnbcurl, CRL downloader, ckms, cloud plugins, shelteredharbor)
 - MSDP (except deduplication to cloud communication)

Configuring PQC in NetBackup:

The **NB_PQC_MODE** option enables the use of Post Quantum Cryptography (PQC) algorithm in TLS 1.3 Hybrid Key Exchange.

See [About Post-Quantum Cryptography \(PQC\)](#).

Note: The PQC mode is supported only if the FIPS mode is disabled.

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	<p>Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option.</p> <p>For information about these commands, see the <i>NetBackup Commands Reference Guide</i>.</p> <p>By default, the NB_PQC_MODE option is disabled.</p> <p>To enable the option, use the following format:</p> <p>NB_PQC_MODE = ENABLE</p> <p>To disable the option, use the following format:</p> <p>NB_PQC_MODE = DISABLE</p> <p>After you enable or disable PQC in NetBackup, restart the NetBackup service on the server and the client using the following commands:</p> <p>For UNIX, run the following commands:</p> <p>/usr/opensv/netbackup/bin/bp.kill_all /usr/opensv/netbackup/bin/bp.start_all</p> <p>For Windows:</p> <p>install_path\NetBackup\bin\bpdown install_path\NetBackup\bin\bpup</p>
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

Caution:

NetBackup leverages the Open Quantum Safe (OQS) provider to support PQC for secure communications. While the provider is a significant step towards preparing for a quantum-safe future, it is widely used in experimental and research environments. It is recommended that you thoroughly assess all the associated risks and ensure that its usage aligns with your organization's security policies and compliance requirements before you enable the NB_PQC_MODE option.

The cluster failover or restarting services through cluster console does not restart the **vnetd** or **bpcd** service that is already running on cluster nodes.

Restart the **vnetd** service manually on each cluster node to reflect the changes in the PQC mode.

On UNIX, do the following:

To stop **vnetd** service on UNIX, run the following command:

/usr/opensv/netbackup/bin/vnetd -terminate

To start **vnetd** service on UNIX, run the following command:

/usr/opensv/netbackup/bin/vnetd -standalone

On Windows, restart 'NetBackup Legacy Network Service' using the Service Control Manager (SCM).

More information around workflow for malware scanning 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.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