COHESITY REDLab

NEWSLETTER | October 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 posture and will expand to include threat detection and threat hunting in the future, all under real-world and fully isolated conditions.

Critical Threat Updates - October 2025

The Cohesity Threat Library is updated daily to enhance detection of active attacks. REDLab conducts deeper investigations into high-profile threats and contributes additional detection capabilities to the library. In October, support for several notable threats was added as noted below and more details are available at: https://www.cohesity.com/trust/redlab/advisories/

- Qilin Ransomware Escalates Global Campaign: The Qilin group launched devastating attacks across multiple sectors in October, hitting major targets including Japan's Asahi Group Holdings (disrupting beer production for weeks), Spain's Tax Administration Agency, and Volkswagen Group France. Using their AGENDA and AGENDA.RUST variants, attackers employ sophisticated "living off the land" techniques and double extortion tactics. Action Required: Monitor ML-based anti-ransomware alerts and run threat scans with custom YARA rules.

- Oracle E-Business Suite Under Mass Attack: CL0P actors are mass-exploiting Oracle EBS vulnerabilities (CVE-2025-61882, CVE-2025-61884) through crafted XSL template injections. Attackers target internet-facing EBS instances, store malicious payloads in application databases, and execute Java-based exploits for data theft and extortion. Immediate Response: Patch EBS instances and scan backups of web directories and extracted templates.

- Akira Ransomware Evolves with BYOVD Tactics: Updated Akira variants now exploit compromised firewall appliances as entry points, then deploy "Bring Your Own Vulnerable Driver" techniques to disable EDR protections. This kernel-level evasion allows undetected data theft and rapid encryption. Protection Strategy: Enhance firewall monitoring and implement driver-based threat detection in backup scans.

REDLab recommendations:

- Enable continuous anti-ransomware monitoring in Security Center
- Schedule regular threat scans using updated threat libraries
- Implement periodic file-hash scanning for dormant malware detection
- Review and quarantine suspicious backup snapshots before recovery

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

Name	Ransomware family	Behavioral pattern
DarkSide	DarkSide Ransomware Group	Command and Scripting Interpreter, Create or Modify System Process, Data Encrypted for Impact, File and Directory Discovery, File and Directory Permissions Modification, Masquerading
Fog	Fog Ransomware Group	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.
Conti	Conti Ransomware Group	Command and Scripting Interpreter, Create or Modify System Process, Data Encrypted for Impact, Defacement, File and Directory Discovery, File and Directory Permissions Modification, Deobfuscate/Decode Files or Information
Termite	Babuk Ransomware Gang	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:

- **DarkSide (attack on NetBackup and Data Protect client):**
    - **Family**: DarkSide Ransomware Group | **Behavior pattern**: Command and Scripting Interpreter, Create or Modify System Process, Data Encrypted for Impact, File and Directory Discovery, File and Directory Permissions Modification, Masquerading
    - **Know Me**: DarkSide is a sophisticated ransomware variant which was first discovered in late 2024, operating under a ransomware-as-a-service (RaaS) model. It gained global attention following its attack on Colonial Pipeline, highlighting its capability to disrupt critical infrastructure. The malware uses a hybrid encryption scheme, combining Salsa20 for file encryption and RSA-1024 for key protection. It appends a victim-specific ID as a file extension to encrypted files. For example file named “sec.jpg" become "sec.jpg.d0be6d88". DarkSide drops a ransom note named README.[victim_ID].TXT in every folder containing encrypted files.
    - **Attack Pattern**: After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully.
      Also, in the case of NetBackup Client it encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated.

- **Fog (attack on NetBackup and Data Protect client):**
    - **Family**: Fog Ransomware Group | **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**: Fog is a sophisticated ransomware variant first observed in April 2024, known for its double extortion tactics and cross-platform targeting of both Windows and Linux environments. Initially focused on the education and recreation sectors, Fog has since expanded to target financial services, manufacturing, and healthcare organizations. Fog ransomware encrypts files using multi-threaded AES-based encryption and it drops a ransom note named “readme.txt” in each encrypted directory, instructing victims to communicate via a Tor-based portal.
    - **Attack Pattern**: After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully.
      Also, in the case of NetBackup Client it encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated.

REDLab findings:

- **Conti (attack on NetBackup and Data Protect client):**
    - **Family**: Conti Ransomware group | **Behavior pattern**: Command and Scripting Interpreter, Create or Modify System Process, Data Encrypted for Impact, Defacement, File and Directory Discovery, File and Directory Permissions Modification, Deobfuscate/Decode Files or Information
    - **Know Me**: Conti is a highly sophisticated ransomware strain, developed by the Wizard Spider cybercrime group based in Russia. It operates under a ransomware-as-a-service (RaaS) model, allowing affiliates to deploy the malware while the core team manages infrastructure and development. Conti encrypts files using a combination of AES-256 and RSA-4096 encryption algorithms, making decryption without the attacker's key virtually impossible. During encryption, it appends the ".CONTI" extension to affected files.
    - **Attack Pattern**: After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully.
      Also, in the case of NetBackup Client it encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated.

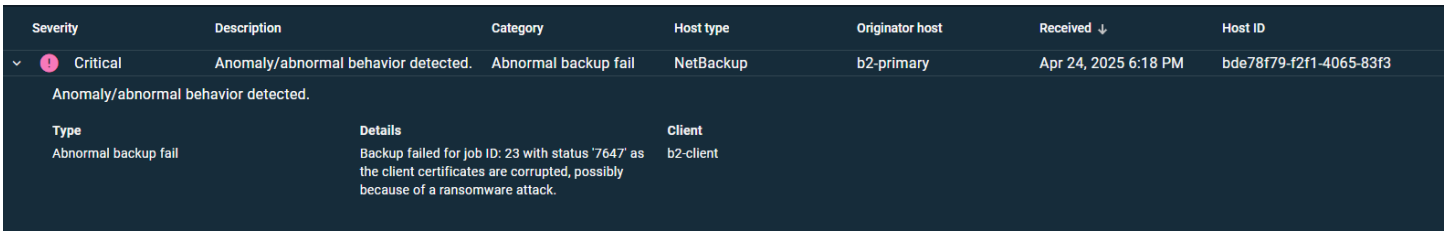
- **Termite (attack on NetBackup and Data Protect client):**
    - **Family**: Babuk Ransomware Gang | **Behaviour pattern**: Process Discovery, System Network Connections Discovery, Data Encrypted for Impact, Inhibit System Recovery, Service Stop
    - **Know Me**: Termite is a relatively new ransomware variant first identified in early 2025, believed to be a descendant of the Babuk ransomware family. It leverages modified Babuk source code, which was leaked in 2021. Termite encrypts files using AES-256 encryption, appends the ".termite" extension to filenames and drops a ransom note titled "How To Restore Your Files.txt" in each affected directory. For example: "security.pdf" becomes "security.pdf.termite". Termite has quickly gained notoriety for its targeted attacks on high-profile organizations across industries including supply chain and manufacturing.
    - **Attack Pattern**: After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully.
      Also, in the case of NetBackup Client it encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated.

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:



Impact of attacks by the given ransomware families

- In case of the earlier above ransomware strains, 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.
- 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.

More information around Client can be found in the NetBackup™ Security and Encryption Guide.

Security Feature Overview

FIPS compliance in NetBackup

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The FIPS 140-2 standard specifies the security requirements for cryptographic modules. It describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing. For more information about the FIPS 140-2 standard and its validation program, see the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program website at the following location:

http://csrc.nist.gov/groups/STM/cmvp

About FIPS support in NetBackup

By default, FIPS mode is disabled in NetBackup.

The following workloads are supported in FIPS-compliant mode: Oracle, MS-SQL, SAP HANA, DB2, VMware,

- Hyper-V, RHV, Nutanix, DynamicNAS, MongoDB, Hadoop, HBase, MySQL, PostgreSQL, SQLite, MariaDB, SharePoint
- Cassandra, Sybase, Informix, MS-Exchange, Enterprise Vault, BMR, Universal Shares, OpenStack (cloud-based solution)

The following operating system-level support is available in FIPS mode:

- Once you enable FIPS mode on RHEL 8, the operating system requires that each RPM package has a SHA-256 digest. RPMs that do not have this digest will fail to install. The RPMs that are built using the native toolchain present on RHEL 6 or RHEL 7 platforms do not include a SHA-256 digest and therefore can fail to install on RHEL 8 when FIPS mode is enabled. This issue affects NetBackup 9.1 and earlier setups as packages for these versions are built using the OS native toolchain on RHEL 7 or earlier.

Starting with NetBackup 10.0, the packages are built using a toolchain that adds the SHA-256 digest, and these can be installed on RHEL 8 with FIPS mode enabled.

The following components, configurations, or operations are not supported in FIPS mode:

- Client-side encryption
  Note: To perform a backup with client-side encryption, you need to disable FIPS mode on the client host.
- NDMP backups
- Scripts (Perl, batch, shell, python) that are executed within NetBackup
- Binaries or utilities: restore_spec_utility, nbcallhomeproxyconfig, nbbsdtar, nbrepo
- NetBackup domain with NBAC enabled
  If NBAC is configured in the NetBackup domain, it is recommended that you do not enable FIPS mode.
- The MQBROKER processes do not support NetBackup-level FIPS configuration on Windows.
- MIT Kerberos used by Hadoop and HBase does not operate with a FIPS-enabled OpenSSL. To perform backup with Kerberos authentication, you need to disable FIPS on the backup host.
- NetBackup CloudPoint does not support the CloudPoint host that is configured in FIPS mode.
- SharePoint internally uses encryption algorithms that do not comply with FIPS standards. The Windows FIPS policy blocks the MD5 hashing algorithms that SharePoint uses. Therefore, the OS-level FIPS policy should be disabled for the SharePoint restores for successful operation.

Note that NetBackup-FIPS is supported for protecting SharePoint. See the following articles for more details:

FIPS and SharePoint Server

SharePoint 2016 and FIPS

Prerequisites

Review the given prerequisites before you configure FIPS in your NetBackup environment.

- Ensure the following before FIPS mode is enabled in the NetBackup domain and on the NetBackup clients.
    - The NetBackup primary server and media servers are 10.0 or later.
    - NetBackup clients are 8.1 or later.
    - You have reviewed FIPS support information.
      See About FIPS support in NetBackup.

Note:
If FIPS mode is enabled and the backups are targeted to the media server deduplication pool (MSDP), the CPU consumption of your system may increase.

- For seamless SSL communication among the NetBackup processes while FIPS mode is enabled, ensure the following:
    - The NetBackup CA private key is in a FIPS-compliant encryption format that is PKCS 8.
    - The private key is generated with a FIPS-compliant algorithm for example, RSA.
    - The private key strength of the NetBackup CA is set to 2048 or 3072 bits.

      If the private key strength does not match the supported value, migrate the CA.

      See Migrating NetBackup CA.

      If you have configured external CA, contact the concerned security administrator.

      See About external CA support in NetBackup.
    - The ongoing NetBackup CA migration process is complete.

Warning:

If the prerequisites are not met, some of the NetBackup functions may not work.

Configure FIPS mode in your NetBackup domain

This section provides steps to enable FIPS mode in your NetBackup domain. Before proceeding with the steps, ensure that the prerequisites are met in your environment.

Configure FIPS mode on NetBackup during installation

You can configure FIPS mode on NetBackup during installation. Refer to the following topics:

1. See Enable FIPS mode on NetBackup during installation.

2. See Enable FIPS mode for the NetBackup Administration Console.

Configure FIPS mode on NetBackup after installation

You can configure FIPS mode on NetBackup after installation.

Note: Ensure that the required configuration steps are carried out on every NetBackup host as applicable.

1. Enable FIPS mode for each host in the NetBackup domain.
   See Enable FIPS mode on a NetBackup host after installation.
2. (Conditional step) You must carry out the following step if the host is a primary server:
   You must enable FIPS mode for the NetBackup Authentication Broker (AT) by updating the VRTSatlocal.conf configuration file on the primary server.

   See Enable FIPS mode for the NetBackup Authentication Broker service.

3. Enable FIPS mode for the NetBackup Administration Console.

   See Enable FIPS mode for the NetBackup Administration Console.

More information around support for FIPS compliance in NetBackup 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