



November 2023



## What's new?

Welcome to the recurring Veritas REDLab newsletter that provides you with the latest updates on the Veritas REDLab initiative.

The Veritas REDLab is a fully isolated security testing facility that is built in-house by Veritas to conduct thorough research and study ransomware and malware attacks first-hand and as they occur. The Veritas 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 we can best protect your primary data and provide meaningful signals to both security teams and data protection teams when an anomaly is detected. This ensures that the data is safe, protected, and that you can be confident in the cyber resilience that Veritas solutions offer.

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

Name	Ransomware family	Behavioral pattern
Akira	Akira	Phishing emails, ZeroLogon vulnerability windows
Rhysida	Rhysida	Phishing emails, Cobalt Strike and PowerShell

## NetBackup Feature:

### Anomaly detection of ransomware file extension

1. During a backup operation, NetBackup 10.3 checks all the file extensions, compares them with the ransomware extension list, and generates an anomaly if there is a match.



November 2023

Anomaly is generated for each ransomware extension that is found in a particular backup.

- a. Ransomware attacks typically encrypt files, and after the encryption it renames files with a different extension. For example, lockbit attack renames a file with the extension: “.lockbit”
  - b. This anomaly detection indicates a possible ransomware attack on the system.
2. The anomaly is generated per job per extension that is found in the job. Alternatively, user can mark the given anomaly as false positive if the given file extension is not changed because of the ransomware attack.

## REDLab findings:

- **Akira (Attack on VMware infrastructure protected by NetBackup):**

- **Family:** Akira | Behavior pattern: Phishing emails, ZeroLogon vulnerability windows
- **Know Me:** The Indian Computer Emergency Response Team (CERT-In) recently issued an advisory reporting the emergence of the new ransomware virus. The Akira ransomware is a new ransomware family that emerged in March 2023. This ransomware is designed to encrypt the data on the infected computers and manipulate filenames by appending the “. akira" extension. The ransomware family claims to have hit at least 63 organizations since its launch – mostly in the US.
- **Observations:** After the attack, it encrypts the user data as well as system files. The system can reboot after it is infected. We can also observe the difference in the image entropy values at VM level before and after the attack.



November 2023

○ **Impact of the attack on NetBackup:**

Post ransomware attack, a system anomaly of type ransomware file extension was generated:

47B98030-75C0-11EE-AAED-90AF842E5819    Ransomware extension detection    High    Anomaly detection extension 'akira' for Ransomware is detected for job ID : 116    Oct 29, 2023 12:01 AM    Not reviewed

Anomaly ID	Anomaly type	Review status
47B98030-75C0-11EE-AAED-90AF842E5819	Ransomware extension detection	Not reviewed

Anomaly details

Backup id	Client name	Details	Policy name	Ransomware extension
50196033-b9aa-48d3-033a-11726bd50989_1698517828	50196033-b9aa-48d3-033a-11726bd50989	Anomaly detection extension 'akira' for Ransomware is detected for job ID : 116	BACKUPNOW+6451d0ff-fb4-47ed-831e-9d7b391be3f0	akira

**Malware scan result – Infected**

● **Rhysida (Attack on VMware infrastructure protected by NetBackup):**

- **Family:** Rhysida malware family | Behavior pattern: Phishing emails, Cobalt Strike and PowerShell scripts
- **Know me:** The Rhysida ransomware gang, which is part of Rhysida malware family. For encryption, Rhysida uses a 4096-bit RSA key with the ChaCha20 algorithm. Rhysida encrypts files and appends their filenames with a “. rhysida” extension.

**Observations:** After the attack it encrypts the user data and system files. The system can reboot after it is infected. We can also observe the difference in in the image entropy values at VM level before and after the attack.

○ **Impact of attack on NetBackup:**



November 2023

Post ransomware attack, a system anomaly of type ransomware file extension was generated:

<input type="checkbox"/> FE6ABDF2-703F-11EE-9D88-12EAAD4514C3		Ransomware extension detection	High	Anomaly detection extension 'rhysida' for Ransomware is detected for job ID : 81	Oct 31, 2023 12:01 AM	Not reviewed
<b>Anomaly ID</b> FE6ABDF2-703F-11EE-9D88-12EAAD4514C3	<b>Anomaly type</b> Ransomware extension detection	<b>Review status</b> Not reviewed				
<b>Anomaly details</b>						<input type="button" value="Mark as ignore"/> <input type="button" value="Confirm as anomaly"/> <input type="button" value="Report as false positive"/>
<b>Backup id</b> 50196033-b9aa-48d3-033a-11726bd5d989_1697913031	<b>Client name</b> 50196033-b9aa-48d3-033a-11726bd5d989	<b>Details</b> Anomaly detection extension 'rhysida' for Ransomware is detected for job ID : 81	<b>Policy name</b> vmwarebkp+6451d0ff-ftb4-47ed-831e-9d7b391be3f0	<b>Ransomware extension</b> rhysida		

Malware Scan result – Infected

# Recommended solutions

## VMware Recovery

We can perform recovery of a VM to its original location where it existed when it was backed up or to a different location. We can choose to recover from the last know-good copy of the existing malware scanned backup image.

Refer to the Veritas NetBackup VMware Administrator’s Guide for recovery details:

[https://www.veritas.com/content/support/en\\_US/doc/21902280-161976672-0/v19545942-161976672](https://www.veritas.com/content/support/en_US/doc/21902280-161976672-0/v19545942-161976672)

[https://www.veritas.com/content/support/en\\_US/doc/21902280-161976672-0/v75741283-161976672](https://www.veritas.com/content/support/en_US/doc/21902280-161976672-0/v75741283-161976672)



November 2023

# New feature overview - NetBackup 10.3

## NetBackup rules engine

- NetBackup supports rules-based engine that can trigger certain threshold-based detection use cases. This is a generic engine that supports different kinds of rules. An anomaly can be detected based on various rules such as: if multiple policies are modified or deleted within a given timestamp. For example, if more than 10 policies are deleted in the last 15 minutes, an anomaly is generated.
- The rule engine detects abnormal activities through NetBackup audit data.
- Rules are available on the Veritas Download Center to be downloaded and injected in NetBackup.
- After the rules are made available in NetBackup, the NetBackup web UI can be used to enable or disable certain rules.

Rules-based anomaly detection 10 of 10 rules enabled ^

**Detect anomalies using NetBackup anomaly detection rules** Upload rules ⓘ  
Select and enable anomalies from the list of anomaly rules

Search... 🔍 ⚙️ ↻ 🗪

<input type="checkbox"/> Rule name	Description	Severity	Version	Enabled	
<input type="checkbox"/> Storage server is set to null STU	Storage server is set to null STU	High	1	Yes	⋮
<input type="checkbox"/> Clients removed from the policy	One or more clients are removed ...	High	1	Yes	⋮
<input type="checkbox"/> Backup selection is modified	One or more files or directories a...	High	1	Yes	⋮
<input type="checkbox"/> Multiple policies deleted by user	Detects if multiple policies are d...	Medium	1	Yes	⋮
<input type="checkbox"/> SLP modified multiple times	Detects if an SLP is modified, or r...	Medium	1	Yes	⋮
<input type="checkbox"/> Multiple policies deactivated by ...	Detects if multiple policies are d...	Medium	1	Yes	⋮
<input type="checkbox"/> Multiple SLPs deleted or deactiv...	Detects if multiple SLPs are delet...	Medium	1	Yes	⋮
<input type="checkbox"/> Disk pool brought down by user	Detects if the disk pool state is c...	Medium	1	Yes	⋮



November 2023

- When rules are enabled, if there is any unusual behavior, NetBackup generates system anomalies.

Anomaly detection Anomaly detection settings ▾

Backup anomalies System anomalies

Search...

<input type="checkbox"/> Anomaly ID	Anomaly type	Severity	Description	Detected on	Re
<input checked="" type="checkbox"/> E283A46E-796D-11EE-8FD5-A81E1E1E1E1E	Disk pool brought down by user	Medium	Detects if the disk pool state is cha	Nov 2, 2023 4:22 PM	Nc

**Anomaly ID**  
E283A46E-796D-11EE-8FD5-A81EDF7AF046

**Anomaly type**  
Disk pool brought down by user

**Review status**  
Not reviewed

---

**Anomaly details**

<b>Additional note</b> Detects if the disk pool state is changed to DOWN in the given timeframe.	<b>Report from date</b> Nov 2, 2023 4:12 PM	<b>Report to date</b> Nov 2, 2023 4:22 PM
---	--	--

## Research references

- <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.sentinelone.com> – Analytics data from various security vendors and insights around behavior patterns for each ransomware family
- <https://www.cisa.gov> – Threat intelligence data and most pressing issues that CISA tracks, and notifications issued by government organizations.



November 2023

- <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.cyborgsecurity.com/> - Provides a library of expertly crafted, constantly updated threat hunting news and content.