VERITAS

VERITAS REDLab

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.

VERITAS

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):**

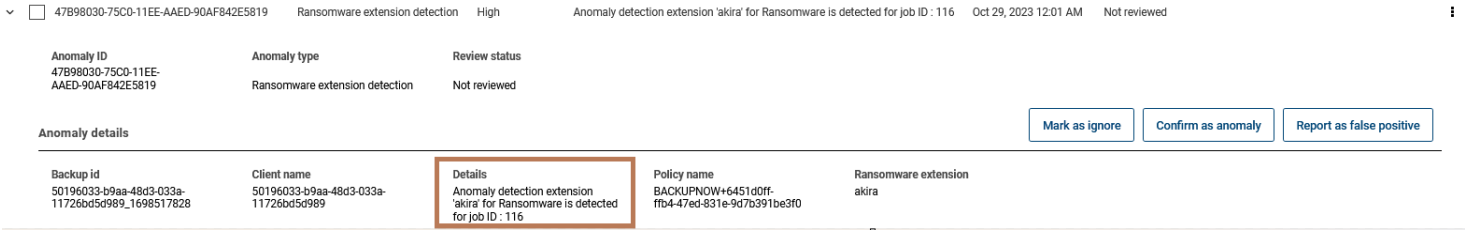
  - **Family**: Akira | Behavior pattern: Phishing emails, ZeroLogon vulnerability windows

  - **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.

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

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



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.

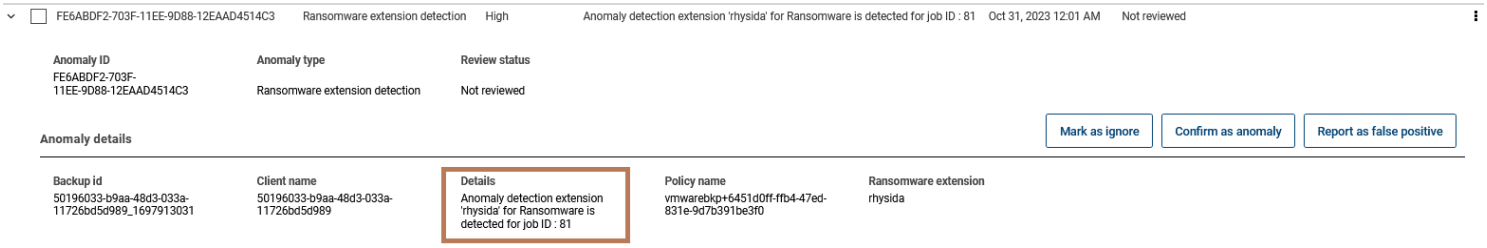
  - **Impact of attack on NetBackup:**

VERITAS

VERITAS REDLab

November 2023

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



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/v75741283-161976672

VERITAS

VERITAS

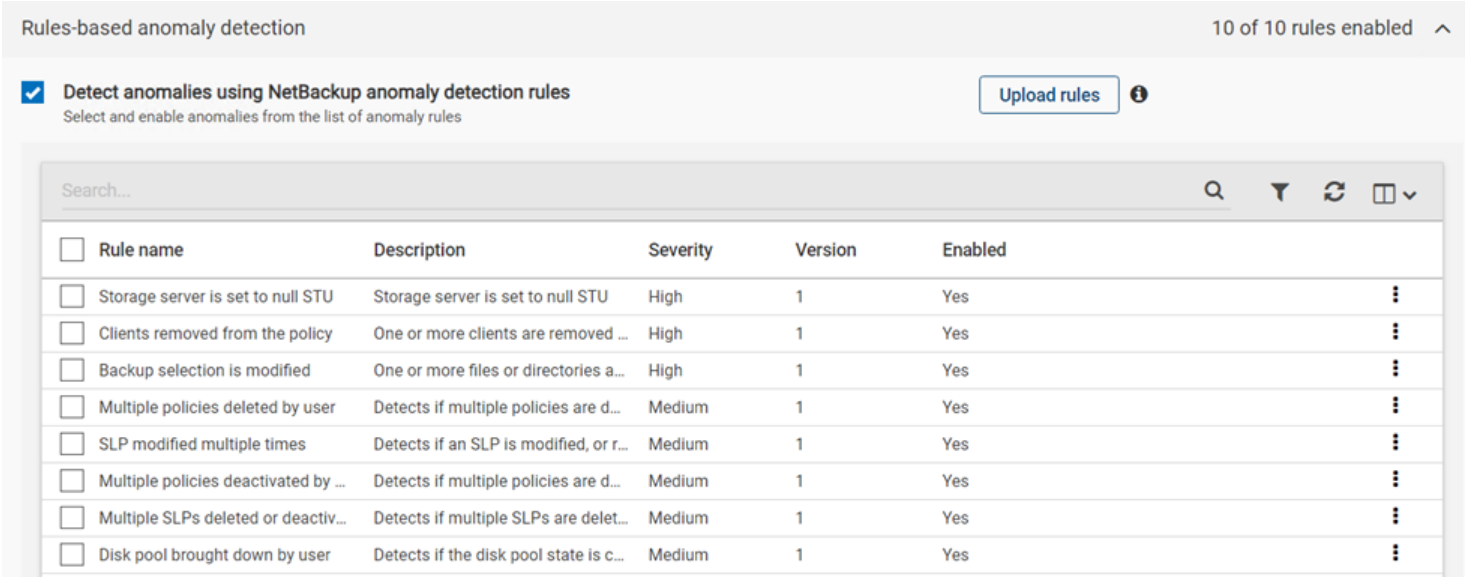
VERITAS REDLab

November 2023

New feature overview - NetBackup 10.3

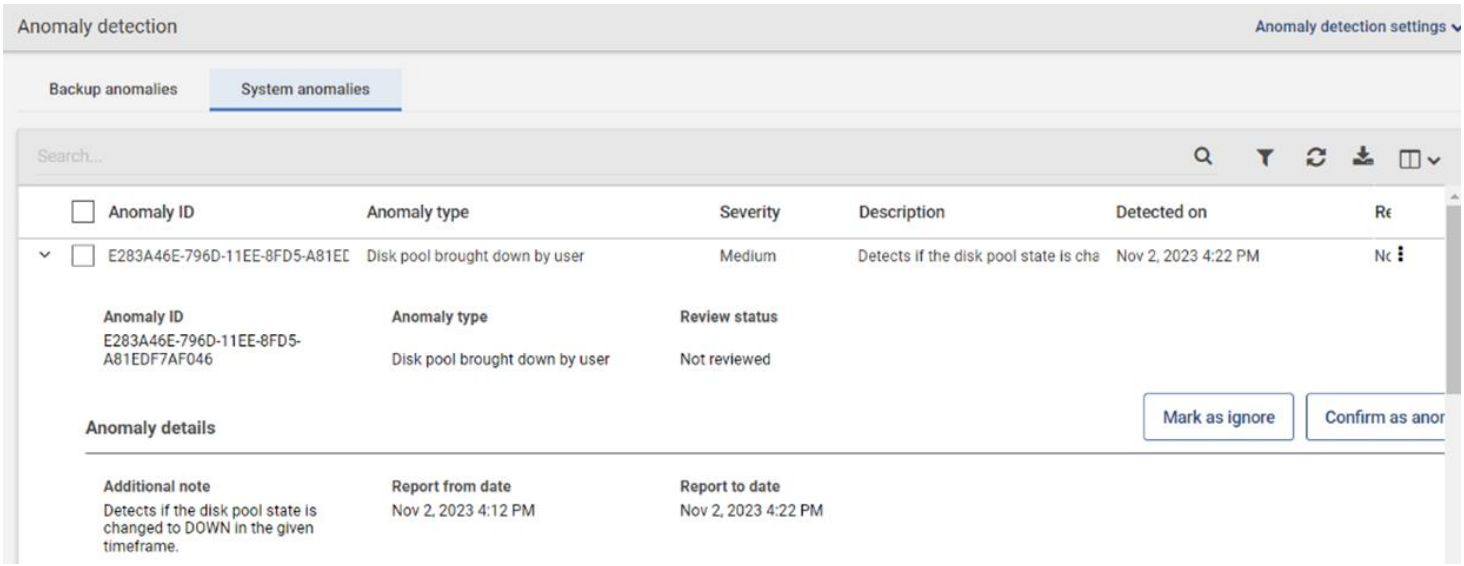
NetBackup rules engine

- 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.



VERITAS

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



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 pattens for each ransomware family
- https://www.cisa.gov – Threat intelligence data and most pressing issues that CISA tracks, and notifications issued by government organizations.

VERITAS REDLab

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.