VERITAS

VERITAS REDLab

June 2024

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, hosted and managed by Veritas, to research and study ransomware and malware. The Veritas REDLab stress tests our solutions to ensure that our products are hardened against attacks, protecting both the backup data and administrative interfaces. These tests drive a deeper understanding of how to secure your data protection processes and data and provide 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 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
Black Basta	Black Basta ransomware family	Command and Scripting Interpreter, Create or Modify System Process, Data Encrypted for Impact, Debugger Evasion, Defacement, File and Directory Discovery, File and Directory Permissions Modification, Impair Defences, Inhibit System Recovery, Masquerading
BlackCat	ALPHV/BlackCat/Noberus ransomware family	Abuse Elevation Control Mechanism, Access Token Manipulation, Account Discovery, Data Encrypted for Impact, Disk Content Wipe, Indicator Removal, Inhibit System Recovery, Lateral Tool Transfer, Modify Registry, Network Share Discovery, Permission Groups Discovery

VERITAS

VERITAS

VERITAS REDLab

June 2024

REDLab findings:

- **Black Basta (attack on NetBackup client):**
    - **Family**: Black Basta ransomware family | **Behavior pattern**: Command and Scripting Interpreter, Create or Modify System Process, Data Encrypted for Impact, Debugger Evasion, Defacement, File and Directory Discovery, File and Directory Permissions Modification, Impair Defences, Inhibit System Recovery, Masquerading
    - **Know Me: The** BlackBasta affiliates employ various techniques to disrupt critical systems after infiltration. These include encrypting files, disabling network services, and rendering servers and workstations inaccessible. Strong symmetric encryption algorithms such as AES (Advanced Encryption Standard) are employed to encrypt files on the victim's system. After successful encryption, BlackBasta displays a ransom note demanding ransom money in cryptocurrency (usually Bitcoin).
    - **Attack Pattern:** After the attack, this ransomware encrypted the user data and system files. A system anomaly that detected unusual behaviour with respect to offline clients was generated.

- **BlackCat (attack on NetBackup client):**
    - **Family:** ALPHV/BlackCat/Noberus ransomware family | **Behavior pattern**: Abuse Elevation Control Mechanism, Access Token Manipulation, Account Discovery, Data Encrypted for Impact, Disk Content Wipe, Indicator Removal, Inhibit System Recovery, Lateral Tool Transfer, Modify Registry, Network Share Discovery, Permission Groups Discovery
    - **Know Me:** BlackCat operates as a Ransomware-as-a-Service (RaaS), where developers provide the malware to affiliates. The affiliates then customize and deploy it against specific targets. BlackCat relies on stolen credentials that are obtained through initial access brokers. These credentials grant the attackers entry into the victim's network. BlackCat also relies on AES for file encryption, it generates a unique encryption key for each victim and encrypts files using this key. It maintains a public data leak site that is accessible via the internet. Attackers post excerpts of exfiltrated data, putting additional pressure on victims to pay the ransom.
    - **Attack Pattern:** After the attack, this ransomware encrypted the user data and system files. A system anomaly that detected unusual behaviour with respect to offline clients was generated.

VERITAS

VERITAS

VERITAS REDLab

June 2024

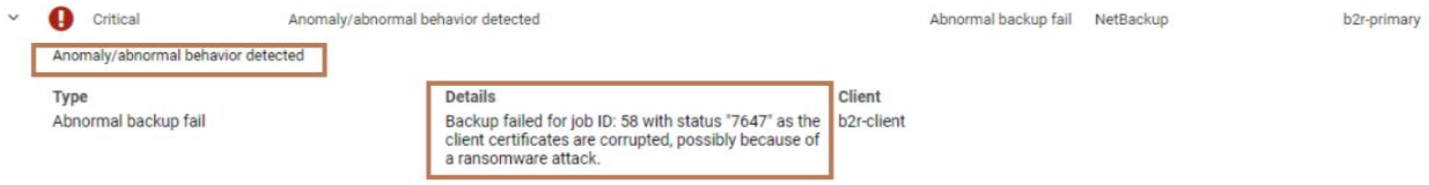
Impact of attacks on NetBackup by the given ransomware families

- The production data source of the NetBackup client is encrypted along with NetBackup configuration files, or communication between NetBackup client and primary server is compromised, resulting in failures of backup jobs.

Recommended solution:

- Veritas NetBackup **Client Offline** system anomaly detects a change in the health of host certificates that are deployed on the NetBackup client. When the host certificate of a NetBackup client is compromised, a system anomaly is detected, and the Client Offline system anomaly creates a critical audit event that indicates failed communications between the NetBackup services and the impacted client.

The following screenshot shows the data from REDLab:



VERITAS

VERITAS

VERITAS REDLab

June 2024

New feature overview - NetBackup 10.4

Risk engine-based anomaly detection

The NetBackup risk engine detects certain system anomalies in a proactive manner and sends appropriate alerts. It helps you take corrective action before you face any security threat in your environment.

- **Steps to configure Risk Engine Anomaly Detection:**

To configure the risk engine-based anomaly detection in your NetBackup environment, you need to follow the below steps:

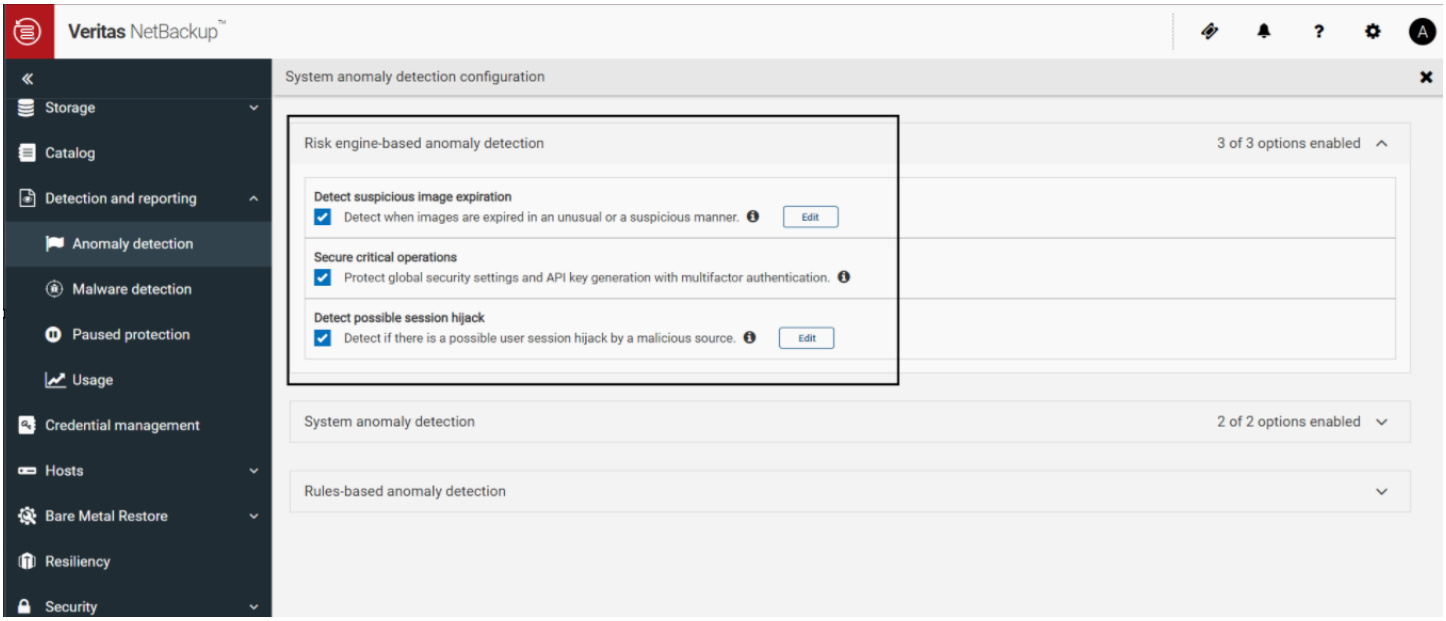
1. Sign into the NetBackup web UI.
2. On the left, click Detection and reporting > Anomaly detection.
3. On the top right, click Anomaly detection settings > System anomaly detection configuration.
4. On the Risk engine-based anomaly detection dropdown, configure the following anomaly detection settings:
    a. Select the “Detect suspicious image expiration” check box to generate an anomaly when NetBackup detects when images are expired in an unusual or a suspicious manner.
    b. Select the “Secure critical operations” check box to generate an anomaly, to protect global security settings and API key generation with multifactor authentication in NetBackup.
    c. Select the “Detect possible session hijack” check box to generate an anomaly when NetBackup detects if there is a possible user session hijack by a malicious source.

VERITAS

VERITAS

VERITAS REDLab

June 2024

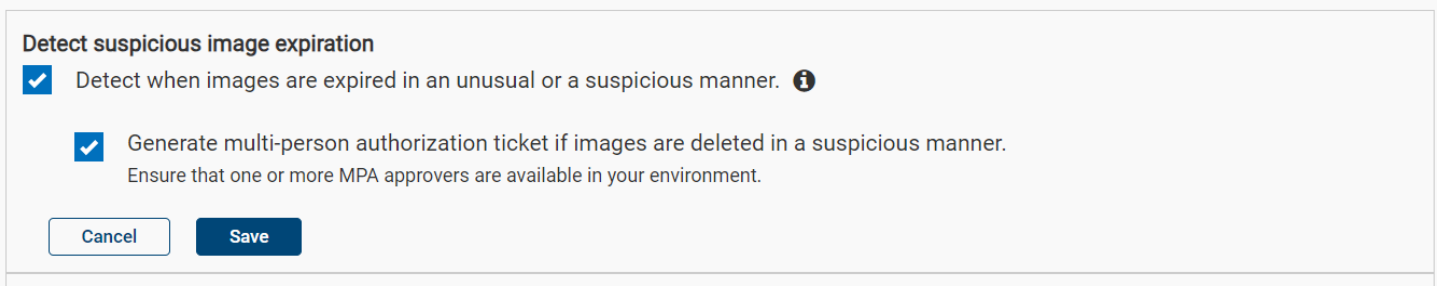


You can configure the following options that the risk engine uses to detect anomalies in case of the given operations:

- **Detect suspicious image expiration:**

  - Use this option to detect when images are expired in an unusual or a suspicious manner.
  - By default, a system anomaly is generated when the risk engine detects an unusual or a suspicious image expiration attempt and allows the operation to proceed.
  - However, for additional security, you can configure multi-person authorization for such image expiration attempts, where an MPA (Multi Person Authorization) approver needs to approve the operation.

VERITAS



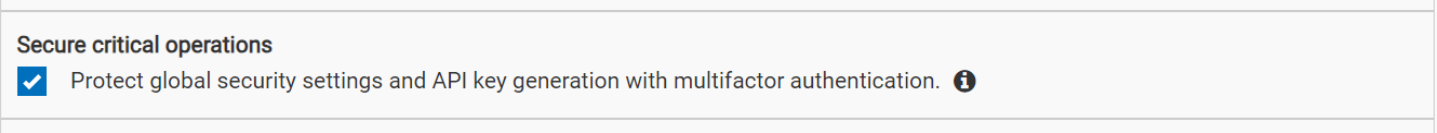
- Click Edit and select the check box to generate a multi-person authorization ticket if images are deleted in a suspicious manner option.

Note: To successfully review the multi-person authorization tickets, ensure that one or more MPA approvers are available in your environment.

About multi-person authorization.
RBAC (Role Based Access Control) roles and permissions for multi-person authorization.

- **Secure critical operations:**

- Use this option to protect critical operations such as modifying global security settings and creating API key.
- When you select this option, you are required to reauthenticate yourself by entering the one-time password that you see in the authenticator application on your smart device before you perform the given critical operations.



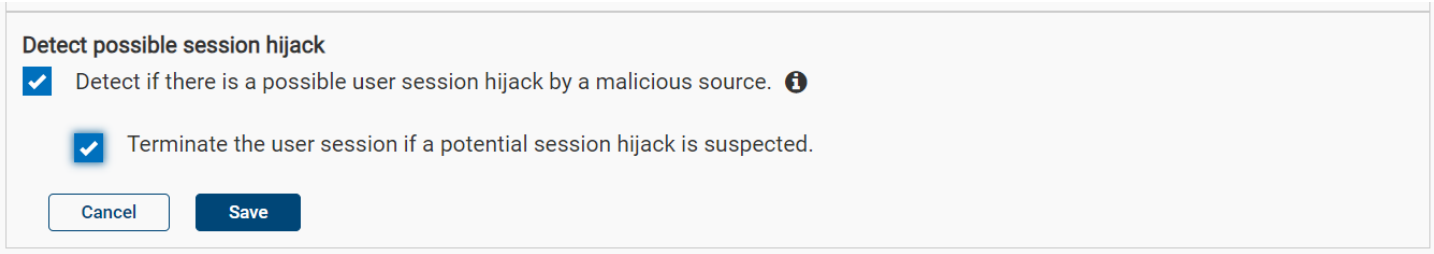
- Ensure that you have configured multifactor authentication for your user account. If multifactor authentication is not configured, you are not prompted to reauthenticate.

Note: It is strongly recommended that you configure multifactor authentication in your environment to prevent security threats by malicious sources.

More Information around - [Configure multifactor authentication for your user account](#).

- ## Detect possible session hijack:

  - Use this option to detect if there is a possible user session hijack by a malicious source.
  - The risk engine detects if the same user session token is used by another IP addresses and sends a maximum of 10 alerts per day.
  - Click Edit and select the check box to terminate the user session when the risk engine detects that there is a possible session hijack.



For more information on Risk Engine, see the [NetBackup™ Web UI Administrator's Guide.](#)

VERITAS

VERITAS REDLab

June 2024

Research references:

- https://www.cisa.gov – Threat intelligence data and most pressing issues that CISA (Cybersecurity and Infrastructure Security Agency) 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://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://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.akamai.com/ - Comprehensive blogs and security research reports
- https://www.truesec.com/ - Blogs and IOC’s
- https://vox.veritas.com/ - VOX (Veritas Open eXchange)
- https://www.sentinelone.com – Analytics data from various security vendors and insights around behavior pattens for each ransomware family
- https://www.barracuda.com/ - In-depth analysis and insights on emerging threats in their blogs
- https://decoded.avast.io/ - Latest threat research, ransomware analysis and IOC’s

VERITAS