



April 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. This helps 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
Trigona	Trigona ransomware family	MSSQL vulnerability, Splashtop remote access, Ransomware, Crypto Virus, Files locker
WannaCry 3.0	WannaCryptor ransomware family	Indicator Removal, EternalBlue, SMB protocol, System Information Discovery, File and Directory Permissions Modification



April 2024



## REDLab findings:

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

- **Family:** Trigona ransomware family | **Behavior pattern:** MSSQL vulnerability, Splashtop remote access, Ransomware, Crypto Virus, Files locker
- **Know Me:** Trigona is ransomware that encrypts files and appends the ".\_locked" extension to filenames. It adds the "how\_to\_decrypt.hta" file that opens a ransom note. An example of how Trigona renames files: it renames "1.jpg" to "1.jpg.\_locked", "2.png" to "2.png.\_locked", and so forth. It embeds the encrypted decryption key, the campaign ID, and the victim ID in the encrypted files and utilizes AES algorithm for encryption. A few additional parameters are embedded in each locked file.
- **Attack Pattern:** After the attack, this ransomware encrypted the user data. A system anomaly was generated, which detected ransomware file extension issue with respect to a file.

- **WannaCry 3.0 (attack on NetBackup client):**

- **Family:** WannaCryptor ransomware family | **Behavior pattern:** Indicator Removal, EternalBlue, SMB protocol, System Information Discovery, File and Directory Permissions Modification
- **Know Me:** WannaCry 3.0 is a new variant of the WannaCry ransomware. It is based on the open-source Crypter (Python) ransomware. Malware within the ransomware category is designed to encrypt data and demand payment for its decryption. It encrypted files and appended their filenames with a ".wncry" extension (which is also used by the real WannaCry). For example, a file originally named "1.jpg" appeared as "1.jpg.wncry", "2.png" as "2.png.wncry", etc. Additionally, the program deleted Volume Shadow Copies. Afterward, WannaCry 3.0 changed the desktop wallpaper and created a pop-up window; both contained ransom notes.
- **Attack Pattern:** After the attack, this ransomware encrypted the user data. A system anomaly was generated, which detected ransomware file extension issue with respect to a file.



April 2024



## Impact of attacks on NetBackup by the given ransomware families

The following observations are noted when a targeted ransomware attack is carried out on a NetBackup client:

- Data on NetBackup client is encrypted the data that can be in the form of document files such as pdf, doc, excel or text files. After the ransomware attack, an extension is added to the encrypted file.
- In case of WannaCry ransomware, it renamed all the encrypted files with extension as “<file\_name>.WNCRY “ after the attack.

### Recommended solution:

#### Data on NetBackup client is encrypted after the attack:

Ransomware file extension-based anomaly detection is a feature in NetBackup 10.3 and later that detects anomalies during the backup process based on certain pre-defined well known ransomware file extensions.

A typical ransomware attacks the data and encrypts it. After the file encryption, it renames the files with a specific extension such as .lockbit. During a backup operation, NetBackup checks all the file extensions, compares them with the ransomware file extension list, and generates an anomaly if there is a match.

The following screenshot shows the data from REDLab :

<input type="checkbox"/> 343624B3-85B3-4AA1-A54F-2366FDC24CBE Ransomware extension detection High		Anomaly detection extension 'WNCRY' for Ransomware is detected for job ID : 2971		Nov 4, 2023 6:30 AM	Not reviewed	⋮
<b>Anomaly ID</b> 343624B3-85B3-4AA1-A54F-2366FDC24CBE	<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> b2x-client1.esx10.local_1699059426	<b>Client name</b> b2x-client1.esx10.local	<b>Details</b> Anomaly detection extension 'WNCRY' for Ransomware is detected for job ID : 2971	<b>Policy name</b> b2_policy_client1	<b>Ransomware extension</b> WNCRY		

Feedbacks and more information around Ransomware file extension solution can be found in [Technical Blog](#)



April 2024



## NetBackup feature overview

### Veritas Client Health System Anomaly Detection:

Veritas Client Health system 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 Health system anomaly creates a critical audit event that indicates failed communication with the NetBackup client. This audit event generates an alert and reports the affected client name to NetBackup IT Analytics or the SIEM/XDR platform.

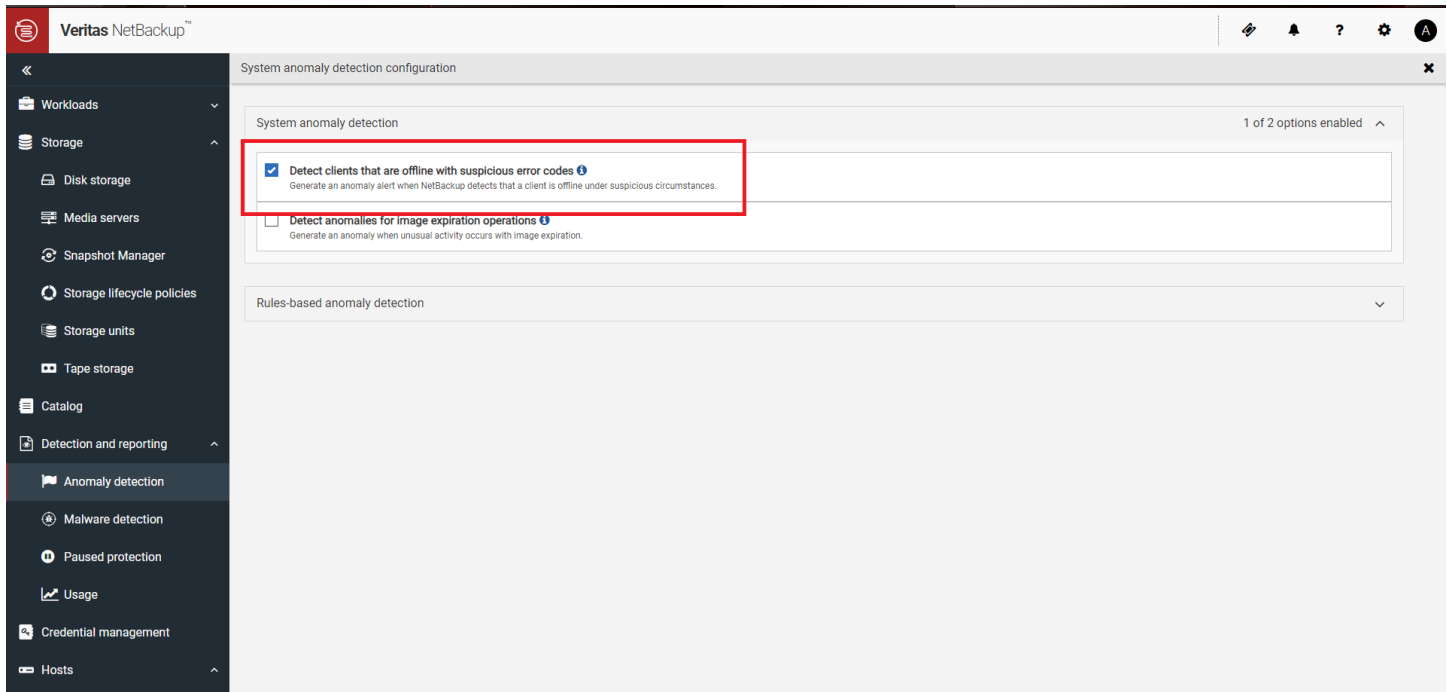
#### • **Configuring Client Health System Anomaly:**

To configure the Client Health System Anomaly 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 System anomaly detection configuration screen, configure the following System anomaly detection settings:
  - a. Select the “Detect clients that are offline with suspicious error codes” check box to generate an anomaly alert when NetBackup detects that a client is offline under suspicious circumstances.



April 2024



## • Viewing anomaly generated due to Client Health System Anomaly

Suppose there is an attack where ransomware encrypts the user data as well as system files. In this case a Client Health System Anomaly that detects unusual behavior with respect to offline clients and a critical notification is generated.

You can view the critical notification generated by clicking on the bell icon (top right corner), after logging into the NetBackup web UI:



April 2024

The screenshot shows the Veritas NetBackup web interface. On the left is a navigation menu with options like Dashboard, Activity monitor, Recovery, Protection, Workloads, Storage, Catalog, Detection and reporting, Anomaly detection, Malware detection, Paused protection, Usage, and Credential management. The main area displays an 'Events' log. A table lists various events with columns for Severity, Description, Category, Host type, Originator host, and Received. The first event is highlighted with a red box:

Severity	Description	Category	Host type	Originator host	Received
Critical	Anomaly/abnormal behavior detected.	Abnormal backup fail	NetBackup	b2x-primary.esx10.local	Oct 14, 2023 8:25 AM
Type		Details	Client		
Abnormal backup fail		Backup failed for job ID: 119 with status '7647' as the client certificates are corrupted, possibly because of a ransomware attack.	b2x-client1.esx10.local		

Below this event, other events are listed, including backup image failures, malware scans, and service status updates.

To get detailed information about the above anomaly notification generated:

1. Sign into the NetBackup web UI.
2. On the left, click Detection and reporting > Anomaly detection.
3. Under Anomaly Detection, click on System anomalies.
4. On the System anomalies page, by clicking on the drop-down option you can view the details of the Client Health Anomaly generated.



April 2024

The screenshot shows the Veritas NetBackup web interface. On the left is a navigation sidebar with options like Dashboard, Activity monitor, Recovery, Protection, Workloads, Storage, Catalog, Detection and reporting, Anomaly detection, Malware detection, Paused protection, Usage, and Credential management. The main content area is titled 'Anomaly detection' and has tabs for 'Backup anomalies' and 'System anomalies'. A table lists anomalies with columns for Anomaly ID, Anomaly type, Severity, Description, Detected on, and Review status. One anomaly is highlighted with a red box, showing details for a 'Client offline anomaly' detected on Oct 14, 2023. The details section includes fields for Client (b2c-client1.esx10.local), Details (Backup failed for job ID: 119 with status '7647' as the client certificates are corrupted, possibly because of a ransomware attack.), and Type (Abnormal backup fail). There are buttons for 'Mark as ignore' and 'Confirm as anomaly'.

Anomaly ID	Anomaly type	Severity	Description	Detected on	Review sta...
7147F6D2-EF6F-4B09-9BE3-8FDCE	Client offline anomaly	High	Backup failed for job ID: 119 with s	Oct 14, 2023 8:25 AM	Not reviewed

**Anomaly details**

Anomaly ID	Anomaly type	Review status
7147F6D2-EF6F-4B09-9BE3-8FDCE	Client offline anomaly	Not reviewed

**Anomaly details**

Client	Details	Type
b2c-client1.esx10.local	Backup failed for job ID: 119 with status '7647' as the client certificates are corrupted, possibly because of a ransomware attack.	Abnormal backup fail

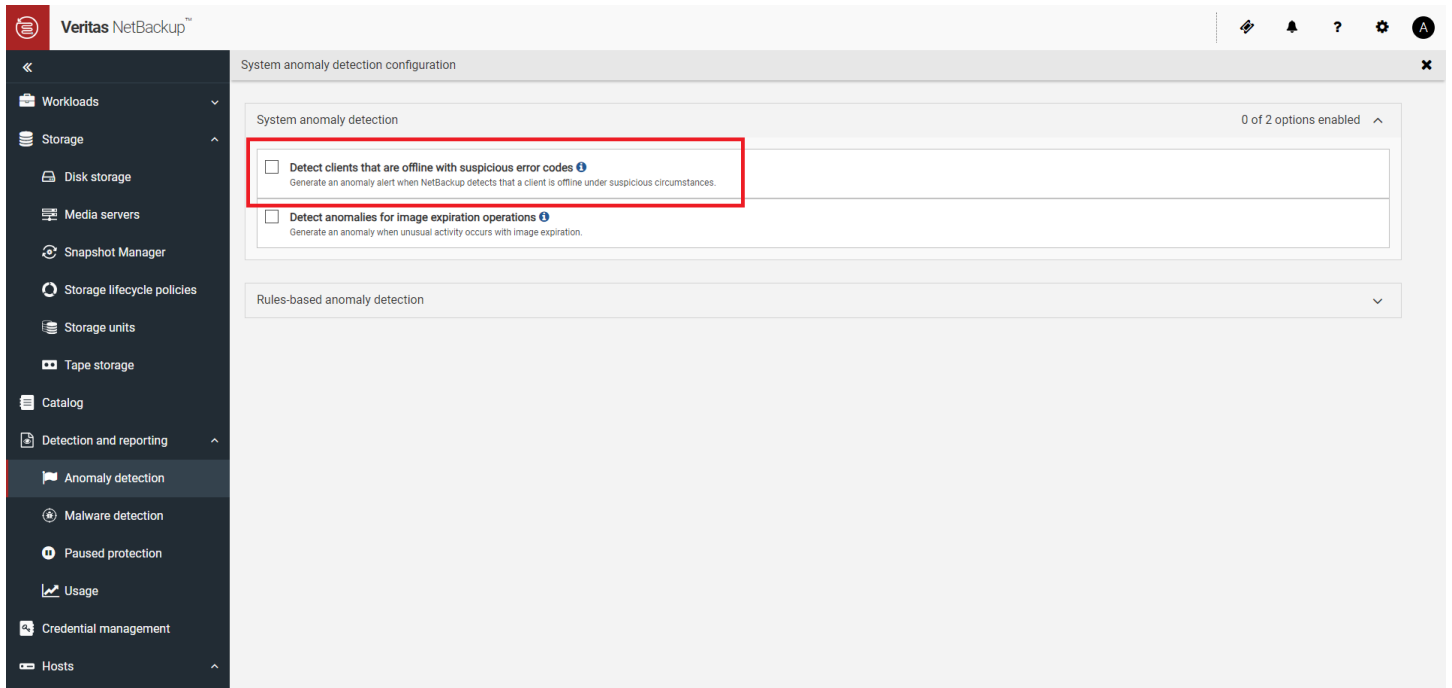
## • Disabling Client Health System Anomaly:

In case the user wants to disable this functionality (not recommended), you can 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 System anomaly detection configuration screen, configure the following system anomaly detection settings:
  - a. Clear the “Detect clients that are offline with suspicious error codes” check box.



April 2024



More information about Anomaly Detection can be found in the [NetBackup™ Security and Encryption Guide](#)





April 2024



## 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://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.truesec.com/> - Blogs and IOC's
- <https://vox.veritas.com/> - VOX (Veritas Open eXchange) – [Technical Blog](#)
- <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