VERITAS

VERITAS REDLab

February 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
Lucky	Phobos ransomware family	Command and Scripting Interpreter, Obfuscated Files or Information, Registry Run Keys / Startup Folder, File Deletion, Masquerading
MuskOff	Chaos Ransomware family	File and Directory Discovery, Process Discovery, File and Directory Permissions Modification, Deobfuscate/Decode Files or Information

VERITAS

VERITAS REDLab

February 2024

REDLab findings:

- **Lucky (attack on NetBackup client):**
    - **Family**: Phobos ransomware family | **Behavior pattern**: Command and Scripting Interpreter, Obfuscated Files or Information, Registry Run Keys / Startup Folder, File Deletion, Masquerading
    - **Know Me:** Lucky Ransomware is a variant of the Phobos Ransomware family that encrypts files and modifies their original filenames by appending a unique ID, the email address of the cyber criminals, and a '. Lucky' extension. For example, a file originally named '1.doc' appears as '1.doc.id[8BHGA73E-6712].[dopingen@rambler.ru]. Lucky,' and so on. Once the encryption process is completed, this ransomware creates ransom notes in a pop-up window ('info.hta') and a text file ('info.txt'). The note in the pop-up window provides more information regarding the infection. It clarifies that the victim **has** to pay a ransom in Bitcoin cryptocurrency for the data decryption. Before paying, the victim can test decryption by sending the cyber criminals up to five encrypted files (within certain specifications).
    - **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.

- **MuskOff (attack on NetBackup client):**
    - **Family:** Chaos Ransomware family | **Behavior pattern**: File and Directory Discovery, Process Discovery, File and Directory Permissions Modification, Deobfuscate/Decode Files or Information
    - **Know Me:** MuskOff is a ransomware-type program that encrypts files and demands payment for their decryption. When executed on a compromised system, it initiates the encryption process, modifying filenames by appending a '.MuskOff' extension. For example, a file originally labeled '1.jpg' transforms into '1.jpg.MuskOff'. Following the completion of the encryption process, it generates a ransom note named 'read_it.txt' to communicate the file encryption to the victim and demand payment for the decryption key. It's worth noting that MuskOff is derived from the Chaos Ransomware family, indicating a connection to this particular strain of harmful software.
    - **Attack Pattern:** After the attack, this ransomware encrypted the user data. A backup anomaly that detected the change in deduplication ratio was generated. Malware scan of the backup image detected the infection and tagged the image as 'Infected', and a critical notification of this status was generated.

VERITAS

VERITAS REDLab

February 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:

- Scenario 1: 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.

- Scenario 2: In certain attacks, NetBackup configuration files are not compromised, but the application data is encrypted. The backup of application data is successful, however, a reduction in data deduplication rate is observed.

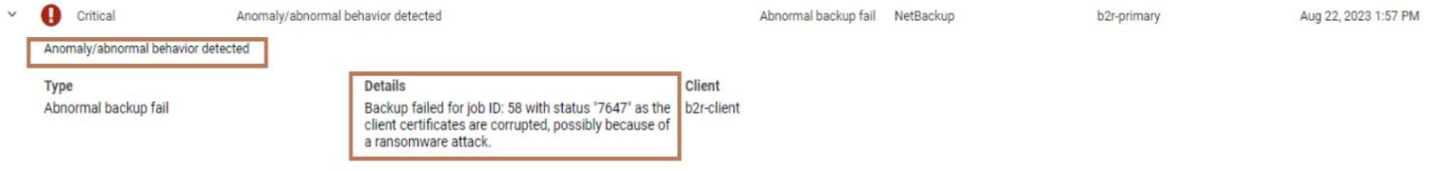
Recommended solutions:

Scenario 1: Data on NetBackup client is encrypted along with NetBackup configuration files.

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.

The following screenshot shows the data from REDLab:



VERITAS

VERITAS

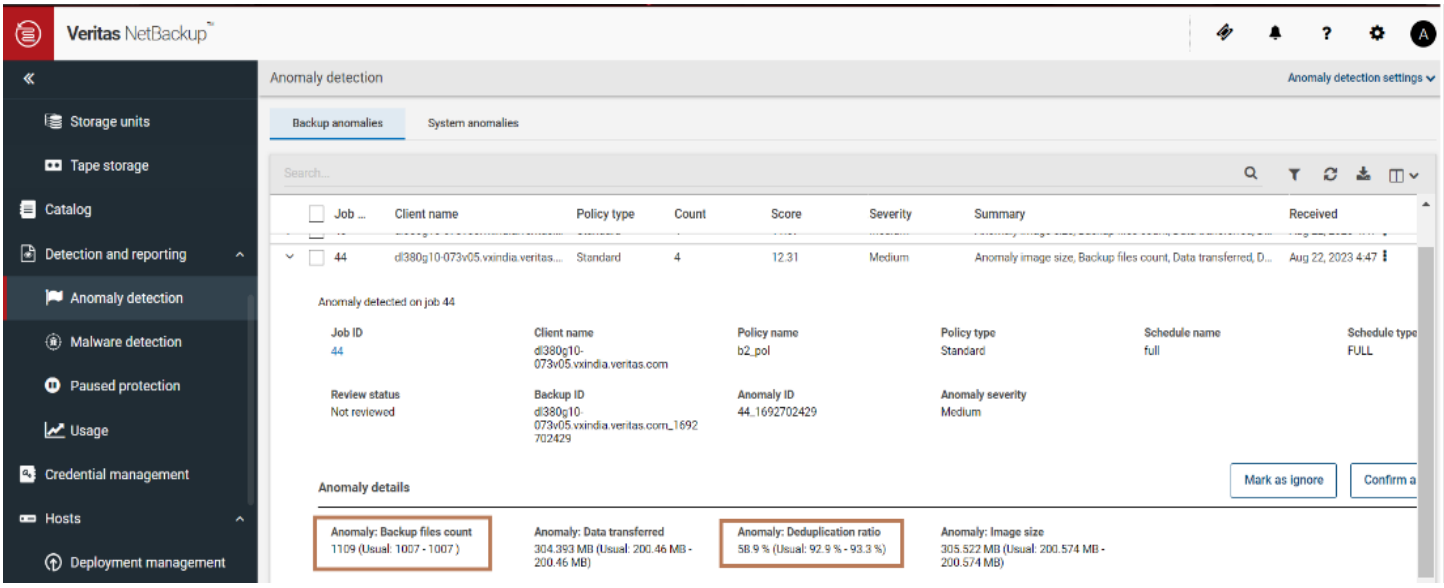
VERITAS REDLab

February 2024

Scenario 2: Data on NetBackup client is encrypted however NetBackup configuration files are intact and backup jobs are successful.

NetBackup uses machine learning (ML)-driven anomaly detection to detect anomalies using statistical data clustering analysis to calculate anomaly score. In this case, the change of data deduplication rate is detected by the ML algorithm and generates an alert. It also starts an automatic malware scan of the backup image.

See the following screenshot from REDLab:



VERITAS

VERITAS

VERITAS REDLab

February 2024

NetBackup feature overview

Data-in-transit encryption (DTE)

The security policies require the Backup Administrators to ensure that the channel on which NetBackup clients send metadata and data to NetBackup servers be secure. In NetBackup 10.0 and later, the data and metadata are encrypted over the wire. This feature is referred to as data channel encryption or data in-transit encryption (DTE).

- ### About the data channel

The following channels are classified as data channels:

Tar stream - client to media server: Over this channel, the tar / data stream flows between the client and the media server. During a backup operation, the media server receives the data from the client and sends it to storage (for example, an OST plug-in). The direction is reversed during a restore.

Tar stream - media server to media server: This channel is used during duplication.

Catalog information - client to media server: Over this channel, the catalog information and control commands are transferred between the client and the media server. The amount of data that is transmitted over this channel is proportional to the number of files and directories that are part of the backup. The media server sends the catalog information that the client has sent to the primary server.

Catalog information - media server to primary server: Over this channel, the catalog information is transferred from the media server to the primary server.

VERITAS

Note: In case of fresh NetBackup 10.3 installation, the data in-transit encryption is set to **Preferred On** by default. In case of upgrade, the previous setting is retained. You can configure data in-transit encryption at various levels: global level (primary server-level) and client level.

- ## Configuring the global data-in-transit encryption setting:

To configure the data-in-transit encryption (DTE) in your NetBackup environment, you need to first set the global DTE configuration setting (or global DTE mode) and then the client DTE mode.

Data-in-transit encryption decision for various NetBackup operations is carried out based on the global DTE mode, the client DTE mode, and the image DTE mode.

The supported values for the global DTE mode are as follows:

> **Preferred Off:** Specifies that the data-in-transit encryption is disabled in the NetBackup domain. This setting can be overridden by the NetBackup client setting.
>
> **Preferred On:** Specifies that the data-in-transit encryption is enabled only for NetBackup 9.1 and later clients.
>
> **Enforced:** Specifies that the data-in-transit encryption is enforced if the NetBackup client setting is either 'Automatic' or 'On'. With this option selected, jobs fail for the NetBackup clients that have the data-in-transit encryption set to 'Off' and for the hosts earlier than 9.1.

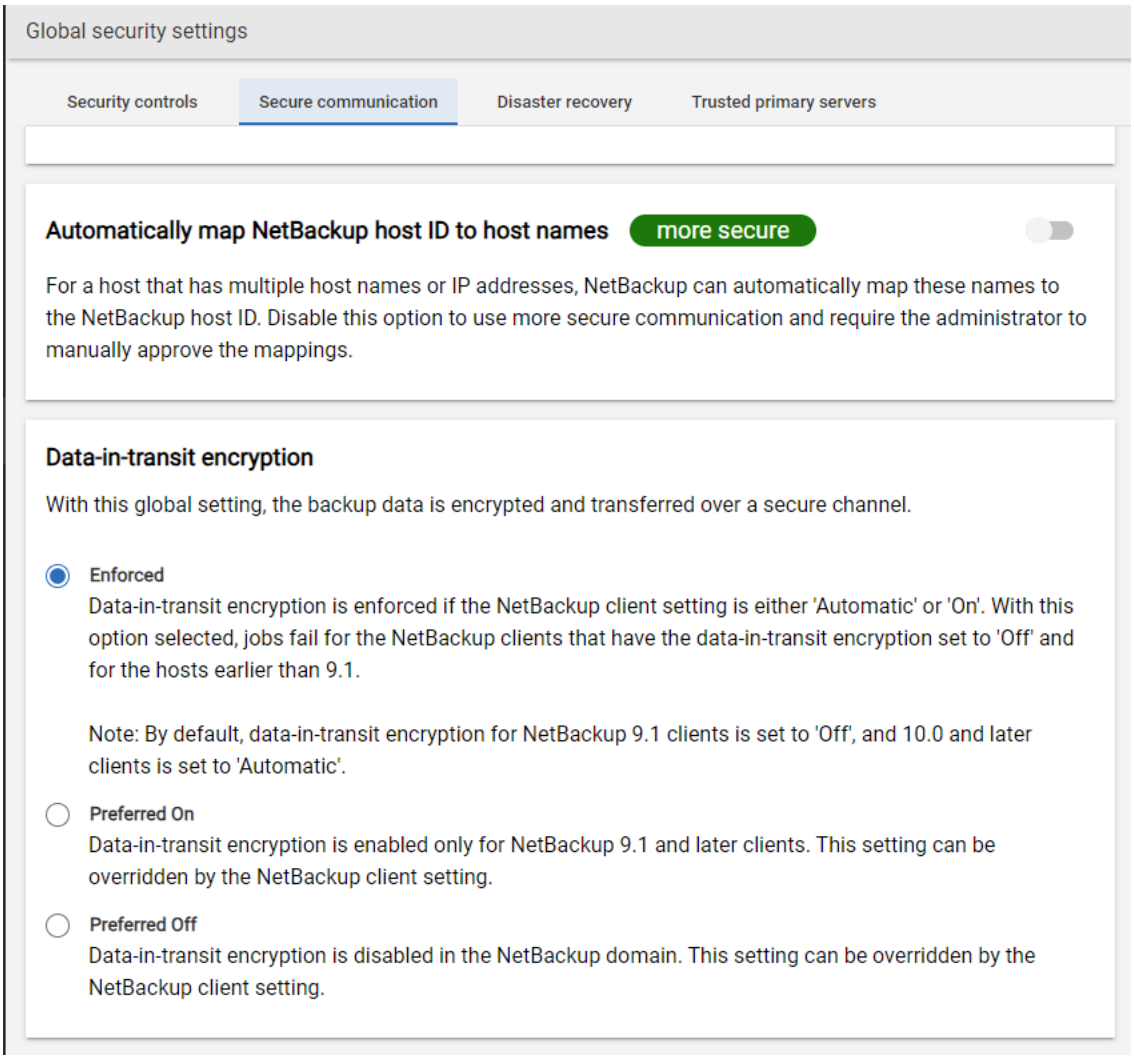
Note: By default, the DTE mode for 9.1 clients is set to **Off** and for 10.0 and later clients, it is set to **Automatic**. See DTE_CLIENT_MODE for clients.

RESTful API to be used for the global DTE configuration:

- GET - /security/properties
- POST - /security/properties

To set or view the global DTE mode using the NetBackup WEB UI

1. Sign into the NetBackup web UI.
2. At the top right, select **Security > Global security**.
3. On the **Secure communication** tab, select one of the following global DTE settings:
    - Preferred Off
    - Preferred On
    - Enforced



To set and view the global DTE mode using the command-line interface:

1. Run the following command to set the global DTE mode:
   `nbseccmd -setsecurityconfig -dteglobalmode 0|1|2`

   Where the value 0 represents **Preferred Off**, 1 represents **Preferred On**, and 2 represents **Enforced**.

2. Run the following command to view the value that is set for the global DTE mode:
   `nbseccmd -getsecurityconfig -dteglobalmode`

- Viewing the DTE mode of a NetBackup job:

Primarily, the global DTE mode and the client DTE mode decide whether the data-in-transit encryption takes place or not for a NetBackup operation. If the data is encrypted when a NetBackup job runs, the 'DTE mode' attribute of the job is set to **On**.

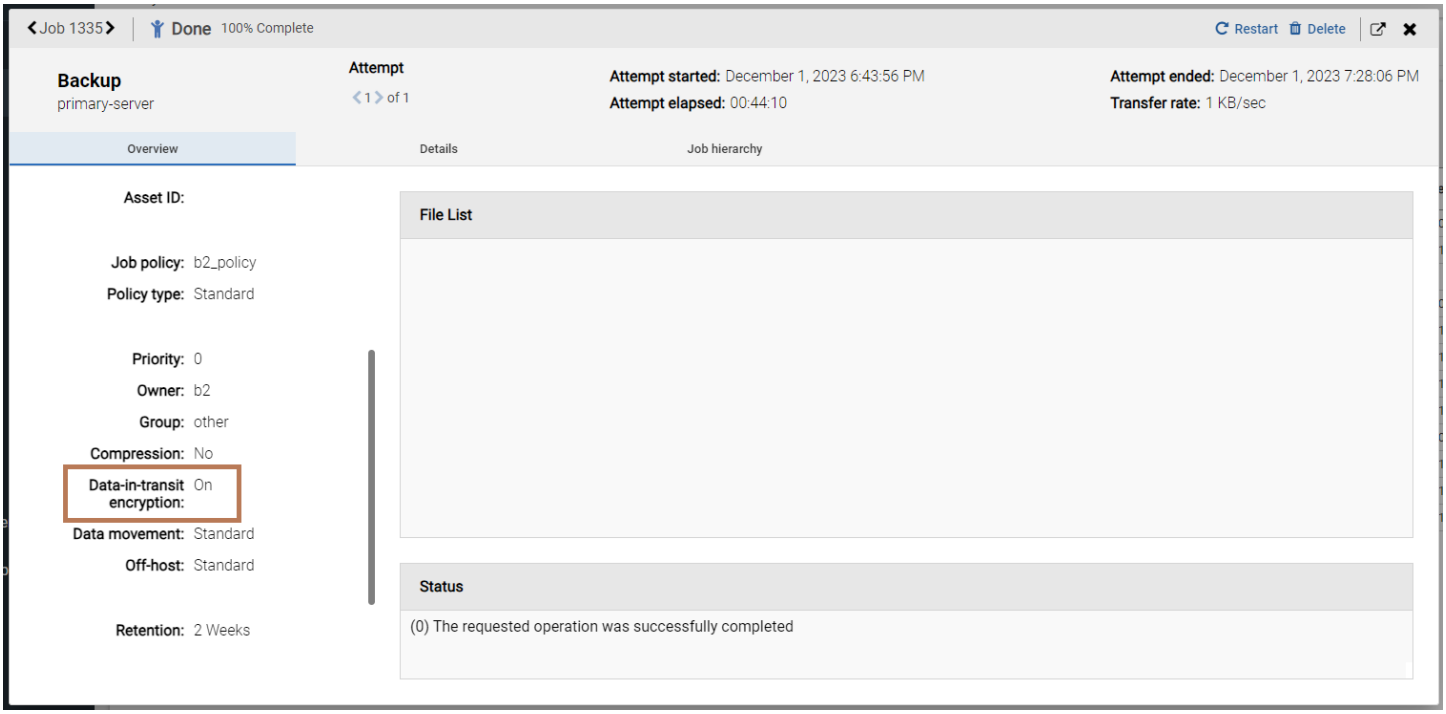
If the data is not encrypted when a NetBackup job runs, the 'DTE mode' attribute of the job is set to Off.

RESTful API to view the DTE mode of a job:

- GET - /admin/jobs
- GET - /admin/jobs/{jobId}

To view the DTE mode of a job using the NetBackup web UI:

1. Sign into the NetBackup web UI.
2. On the left, select **Activity Monitor > Jobs**.
3. You can see the **Data-in-transit encryption** column that determines the DTE mode of the job.



To view the DTE mode of a job using the command-line interface

- Run the following command:
  `bpdbjobs -dtemode Off|On`

Additionally, the data-in-transit encryption (DTE) mode can be set on NetBackup Client and NetBackup Media Server:

- Configure the DTE mode on a client
- Configure the DTE mode on the media server

More information about data-in-transit encryption (DTE) can be found in the NetBackup™ Security and Encryption Guide.

VERITAS

VERITAS REDLab

February 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://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

VERITAS