VERITAS REDLab

March 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
LostTrust	LostTrust ransomware family	Abuse Elevation Control Mechanism, File and Directory Permissions Modification, Deobfuscate/Decode Files or Information, File and Directory Discovery, Process Discovery, Windows Service
LeakDB	Phobos ransomware family	Data from Local System, Command and Scripting Interpreter, Registry Run Keys / Startup Folder, System Network Configuration Discovery, Taint Shared Content, Network Share Discovery, Virtualization/Sandbox Evasion

VERITAS REDLab

March 2024

REDLab findings:

- **LostTrust (attack on NetBackup client):**
    - **Family**: LostTrust ransomware family | **Behavior pattern**: Abuse Elevation Control Mechanism, File and Directory Permissions Modification, Deobfuscate/Decode Files or Information, File and Directory Discovery, Process Discovery, Windows Service
    - **Know Me:** The LostTrust ransomware operation is a new multi-extortion threat that emerged in early Spring of 2023. The purpose of LostTrust is to encrypt data to make it inaccessible to victims. Also, LostTrust appends the ".losttrustencoded" extension to filenames and delivers a ransom note ("!LostTrustEncoded.txt"). An example of how LostTrust modifies filenames: it changes "1.jpg" to "1.jpg.losttrustencoded", "2.png" to "2.png.losttrustencoded", and so forth. LostTrust victims are presented with a ransom note that attempts to portray the gang as providing a service, a fake veneer that is commonly adopted by cybercriminals perpetrating intrusions.
    - **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.

- **LeakDB (attack on NetBackup client):**
    - **Family:** Phobos ransomware family | **Behavior pattern**: Data from Local System, Command and Scripting Interpreter, Registry Run Keys / Startup Folder, System Network Configuration Discovery, Taint Shared Content, Network Share Discovery, Virtualization/Sandbox Evasion
    - **Know Me:** LeakDB Ransomware is a variant of the Phobos Ransomware family that encrypts files and alters their titles. Original filenames were appended with a unique ID assigned to the victim, the cyber criminals' email address, and a ".LEAKDB" extension. For example, a file initially named "1.jpg" appeared as "1.jpg.id[7QFGCA87T-2778].[pcsupport@skiff.com].LEAKDB". After the encryption process was concluded, ransom notes were created in a pop-up screen ("info.hta") and a text file ("info.txt"), which were dropped into every encrypted directory and on the desktop. Based on the messages therein, it is evident that LEAKDB targets organizations rather than home users.
    - **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.

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 along with NetBackup configuration files, or communication between NetBackup client and primary server is compromised that resulted in failures of backup jobs.

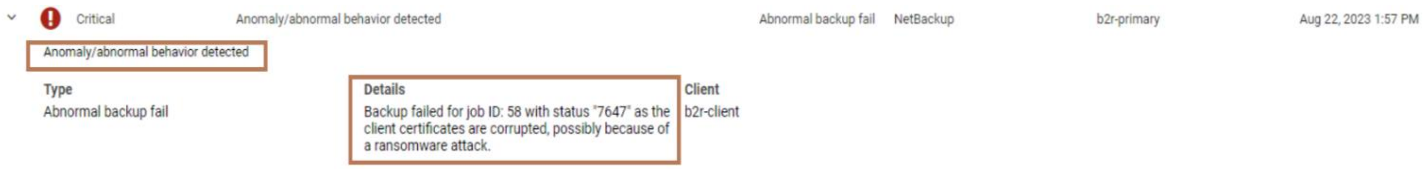
Recommended solution:

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:



Critical | Anomaly/abnormal behavior detected | Abnormal backup fail | NetBackup | b2r-primary | Aug 22, 2023 1:57 PM

Anomaly/abnormal behavior detected

Type
Abnormal backup fail

Details
Backup failed for job ID: 58 with status "7647" as the client certificates are corrupted, possibly because of a ransomware attack.

Client
b2r-client

NetBackup feature overview

Detect file extensions associated with Ransomware

Typically, when a ransomware attacks a system, it encrypts the data that can be in the form of document files such as pdf, doc, excel or text files. Those attacks add extension to the encrypted file. For example, a WannaCry attack after attack renames all the encrypted files with extension as <file_name>.WannaCry

Having ransomware specific extension to the impacted file enables you to identify if there is any attack or not, comparing the extension of the file with known ransomware extensions. For example, during backup, you can check if the extension of the file that is being backed up matches the extension with known ransomware extensions.

- ### NetBackup support for detection of known Ransomware aware extension:

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

<u>How the known ransomware known extension list captured?</u>

- NetBackup ships with pre-captured known ransomware extensions. The extensions are captured from different public repositories such as:

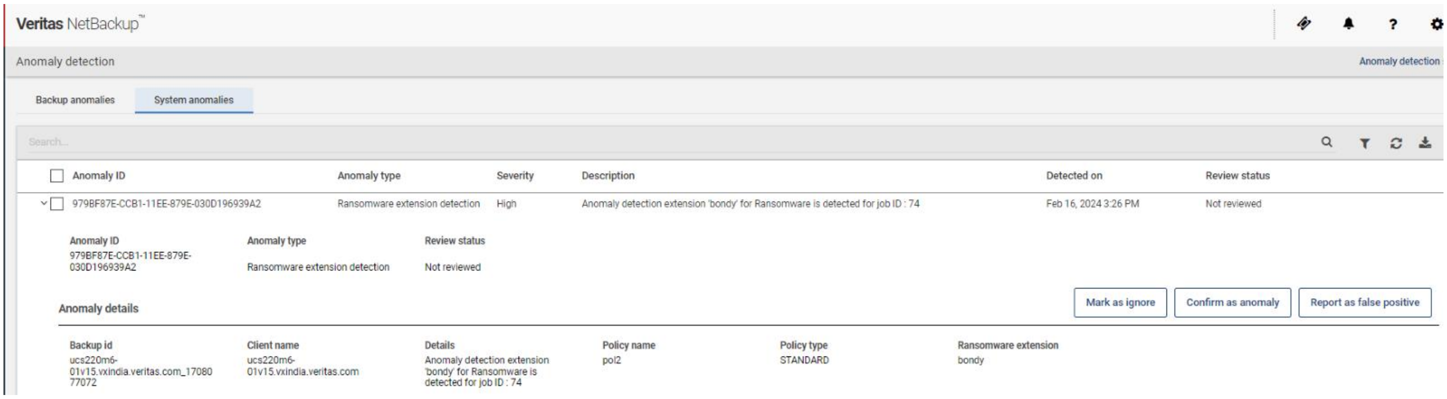
  Ransomware encrypted file extensions list (file-extensions.org)

<u>How NetBackup detects known ransomware extensions?</u>

- During backup, NetBackup captures the extensions of files that are being backed up. It then compares extensions with known extensions list that is shipped along with NetBackup product.

VERITAS REDLab

March 2024



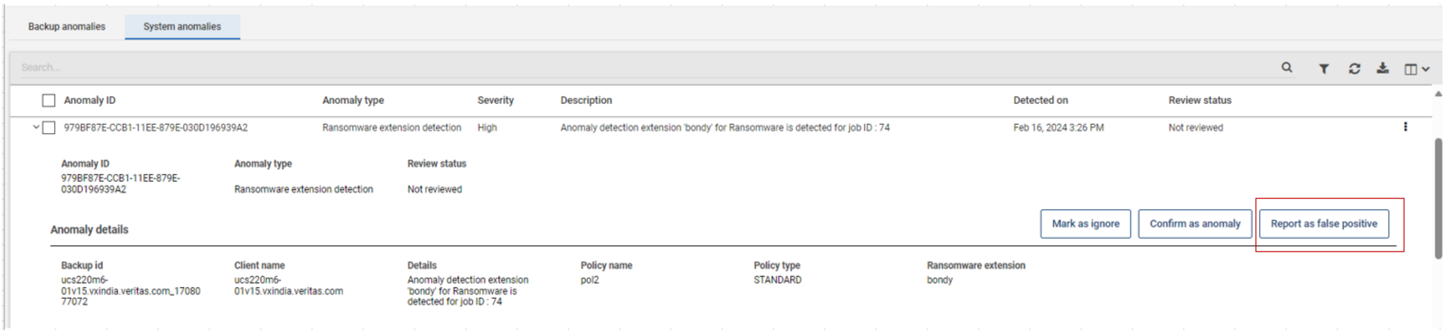
Anomaly ID	Anomaly type	Severity	Description	Detected on	Review status
979BF87E-CCB1-11EE-879E-030D196939A2	Ransomware extension detection	High	Anomaly detection extension 'bondy' for Ransomware is detected for job ID : 74	Feb 16, 2024 3:26 PM	Not reviewed

Anomaly ID	Anomaly type	Review status
979BF87E-CCB1-11EE-879E-030D196939A2	Ransomware extension detection	Not reviewed

Anomaly details

Backup id	Client name	Details	Policy name	Policy type	Ransomware extension
ucs220m6-01v15.vxindia.veritas.com_1708077072	ucs220m6-01v15.vxindia.veritas.com	Anomaly detection extension 'bondy' for Ransomware is detected for job ID : 74	pol2	STANDARD	bondy

- The extensions mentioned in the known ransomware extension list are relevant to certain attacks. However, there are chances that some of the extensions may be used by legitimate software. Alternatively, in future the software may start using these extensions for its application specific use.
- It is hard to figure out which extensions are relevant to normal use cases for such software and the relevancy may also change per system or customer.
- Therefore, NetBackup provides provision to mark such extensions as false so that during the next backup, the system will not generate the anomalies again for the same extension for the given client and policy combination.
- Note that marking such extensions as false is a one-time activity for the combination of client-policy and hence forth anomalies are not generated.



Anomaly ID	Anomaly type	Severity	Description	Detected on	Review status
979BF87E-CCB1-11EE-879E-030D196939A2	Ransomware extension detection	High	Anomaly detection extension 'bondy' for Ransomware is detected for job ID : 74	Feb 16, 2024 3:26 PM	Not reviewed

Anomaly ID	Anomaly type	Review status
979BF87E-CCB1-11EE-879E-030D196939A2	Ransomware extension detection	Not reviewed

Anomaly details

Backup id	Client name	Details	Policy name	Policy type	Ransomware extension
ucs220m6-01v15.vxindia.veritas.com_1708077072	ucs220m6-01v15.vxindia.veritas.com	Anomaly detection extension 'bondy' for Ransomware is detected for job ID : 74	pol2	STANDARD	bondy

How to disable the Ransomware extension anomalies?

- By default, this feature is enabled to detect ransomware extensions in backup files. If you want to manage the disable/enable functionality of the detection feature, append the below key value pair to `/usr/openv/netbackup/bp.conf` file on a new line accordingly.

  To disable: CHECK_RANSOMWARE_EXTENSIONS = NEVER

  To enable: CHECK_RANSOMWARE_EXTENSIONS = ALWAYS

More information about Anomaly Detection can be found in the NetBackup™ Security and Encryption Guide

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 pattens for each ransomware family
- https://decoded.avast.io/ - Latest threat research, ransomware analysis and IOC’s