VERITAS

VERITAS REDLab

December 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
BianLian	BianLian Ransomware Family	Stealer, Phishing, Command and Control, Ransomware, Crypto Virus, Files locker
NoEscape	Avaddon Malware Family	Replication Through Removable Media, System Shutdown/Reboot, Lateral Movement, Persistence, Delete service, Privilege Escalation

Copyright © 2023 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

VERITAS

VERITAS

VERITAS REDLab

December 2023

REDLab findings:

- **BianLian (attack on NetBackup client):**
    - **Family**: BianLian Ransomware Family | **Behavior pattern**: Stealer, Phishing, Command and Control, Crypto Virus, Files locker
    - **Know Me:** One example of a cybercriminal group and ransomware, which is known as BianLian. According to a cybersecurity advisory released by the FBI, CISA, and Australian Cyber Security Centre, BianLian has been targeting critical infrastructure and organizations across the U.S. and Australia since June 2022. After data encryption, the ransomware appends the '.bianlian' extension and drops a ransom note called 'Look' at this instruction.txt into each folder on the system.
    - **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.

- **NoEscape (attack on NetBackup client):**
    - **Family:** Avaddon Malware Family| Behavior pattern: Replication Through Removable Media, System Shutdown/Reboot, Lateral Movement, Persistence, Delete service, Privilege Escalation
    - **Know Me:** NoEscape ransomware has emerged in May of 2023 and functions as a Ransomware-as-a-Service (RaaS). CERT-In issued an alert for NoEscape ransomware, which is believed to be a rebrand of Avaddon, a ransomware gang that shut down and released its decryption keys in 2021. Previously, the Avaddon encryptor utilized AES for file encryption, while 'NoEscape' ransomware payloads supports multiple encryption modes, including full, fast, or strong, along with leveraging RSA and ChaCHA-20 for the specific file encryption. Encrypted files have a random 10-character extension appended to the filename, which is unique for each attack (for example, 'filename.ENSDHJSSAH')
    - **Attack Pattern:** After the attack, this ransomware encrypted the user data. A backup anomaly (that detected the change in deduplication ratio) was generated. Also, the difference in the image entropy values were observed before and after the attack. Malware scan of the backup image detected the infection and tagged the image as 'Infected' and a critical notification of this status was generated.

Copyright © 2023 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

VERITAS

VERITAS REDLab

December 2023

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 in this case, and a reduction in data deduplication rate is observed.

Recommended solutions:

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

The 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.

Copyright © 2023 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

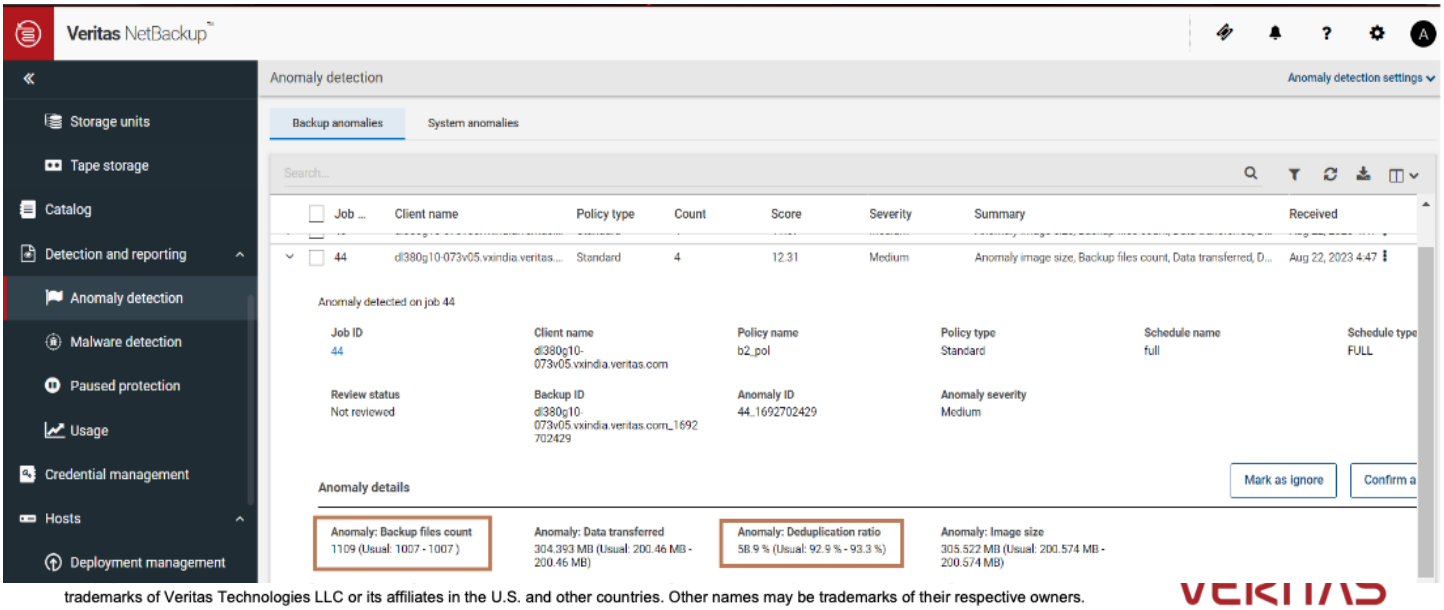
VERITAS

The following screenshot shows the data from REDLab:

Anomaly extensions can be downloaded from the Veritas Download Center and deployed on NetBackup 10.2 or later versions of the NetBackup primary server. Review the NetBackup™ Anomaly Detection Extensions Guide for the steps to deploy and configure these anomaly extensions on the primary server.

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 that generates an alert. It also starts an automatic malware scan of the backup image. See the following screenshot from REDLab:



trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

VERITAS

VERITAS REDLab

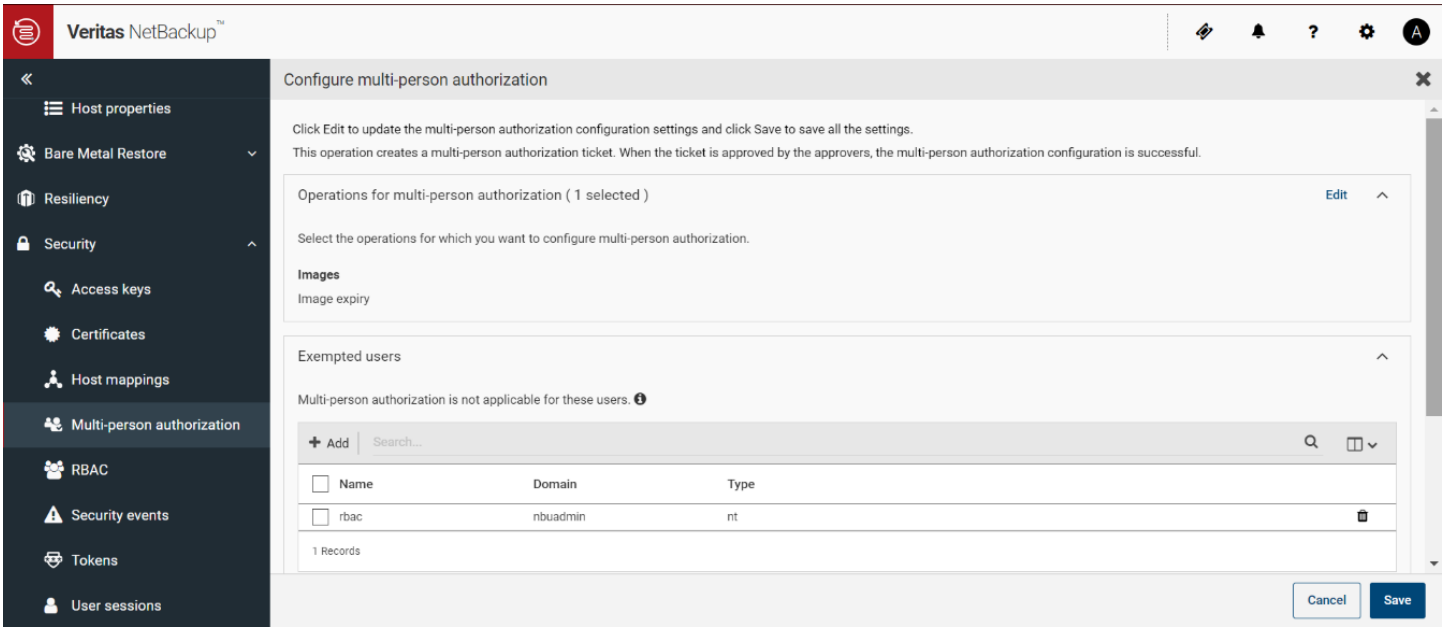
December 2023

New feature overview - NetBackup 10.3

Multi-Person Authorization

- NetBackup Security Administrator can configure multi-person authorization. It proactively protects NetBackup primary servers from an undesirable or a malicious act by ensuring that a second authorized user approves that action before it is allowed to take place.

- If you configure multi-person authorization for a certain operation, you can perform the associated operation only using the NetBackup web UI or REST APIs. You cannot perform the operation using the NetBackup Administration Console.

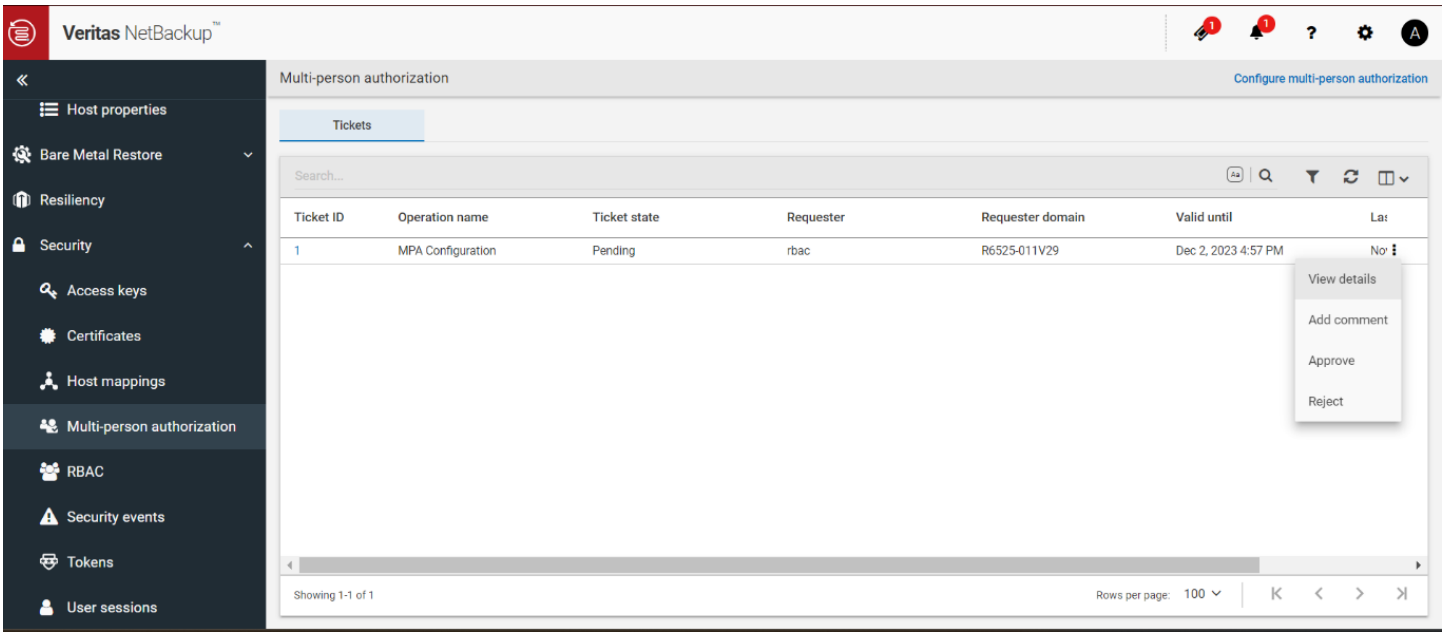


- To bypass multi-person authorization, you can add the associated users as exempted users who do not require approval for performing the required operations.

Copyright © 2023 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

VERITAS

- To configure multi-person authorization in NetBackup, you need to have two users: one is the requester and other is the approver. A requester cannot be an approver of his or her own tickets.



- A multi-person authorization configuration ticket is generated. After the approver approves the ticket, multi-person authorization configuration comes into effect.

- More information about multi-person authorization can be found in the NetBackup™ Security and Encryption Guide.

Copyright © 2023 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

VERITAS

VERITAS REDLab

December 2023

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.
- 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.
- https://www.cert-in.org.in/ - Collection, forecast and alerts of cyber security incidents.
- https://decoded.avast.io/ - Latest threat research, ransomware analysis and IOC's

Copyright © 2023 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

VERITAS