VERITAS

VERITAS REDLab

October 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 the latest Ransomware families and their behavioral patterns that were studied in the REDLab:

Name	Ransomware family	Behavioral pattern
WannaCrypt/ Maze	WannaCryptor	EternalBlue, SMB protocol, RDP lateral movement
NetWalker	NetWalker	Phishing emails, VBScripts, RDP lateral movement
Petya	Petya family	Phishing emails, MBR & MFT encryption
LockBit 3.0	LockBit, formerly "ABCD" ransomware	Compromise RDP/VPN, Cobalt Strike Beacon, MetaSploit, and Mimikatz

VERITAS

VERITAS

VERITAS REDLab

October 2023

REDLab findings

- **LockBit 3.0 Ransomware (attack on NetBackup client):**
  - **Family**: LockBit | Behavioral pattern: Windows Safe Mode and privileged service
  - **Know me:** The LockBit 3.0 ransomware operations function as a Ransomware-as-a-Service (RaaS) model and is a continuation of previous versions of the ransomware, LockBit 2.0, and LockBit. LockBit his highly active in deploying models such as double extortion, initial access broker affiliates, and advertising on hacker forums. They are even known to recruit insiders and make contests in forums for recruiting skilled hackers. Such expansionist policies have attracted numerous affiliates, have victimized thousands of entities, and with that they continue their malicious acts.
  - **Attack pattern:** Along with system files, the malware may also encrypt NetBackup configuration files. A backup anomaly (that detects the change in deduplication ratio) and a system anomaly (that detects unusual behavior with respect to image expiry or offline clients) are generated.

- **WannaCrypt/Maze (attack on NetBackup client):**
  - **Family**: WannaCryptor | Behavioral pattern: Windows Safe Mode and privileged service
  - **Know me:** The WannaCrypt/Maze ransomware attack was a worldwide cyberattack that was propagated using EternalBlue exploit and it encrypted the data and ransom payments were demanded. In addition to encrypting the data, most operators of Maze also copy the data they encrypt and threaten to leak it unless the ransom is paid.
  - **Attack pattern:** Along with system files, the malware may also encrypt NetBackup configuration files. A backup anomaly (that detects the change in deduplication ratio) and a system anomaly (that detects unusual behavior with respect to image expiry or offline clients) are generated.

VERITAS

VERITAS REDLab

October 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. This checks the health of certificates that are deployed on the NetBackup client and starts the anomaly detection process.

Once 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:

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.

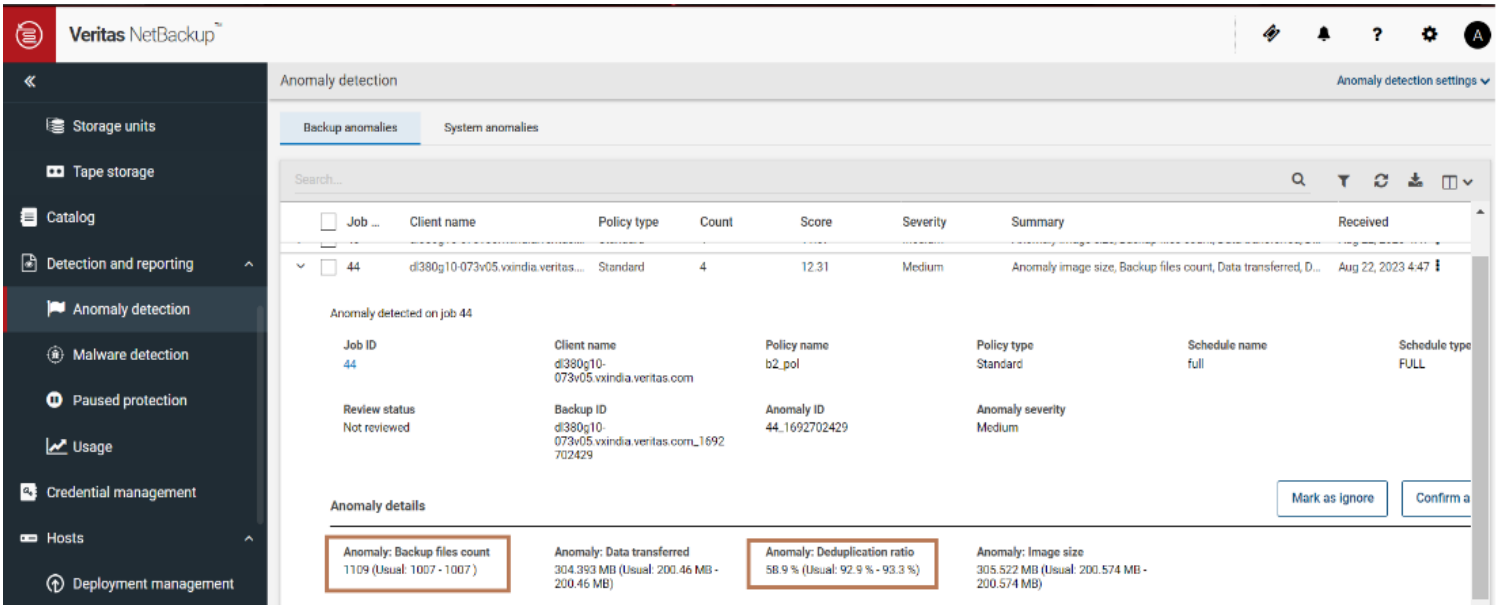
Scenario 2: Data on NetBackup client is encrypted however NetBackup configuration files are intact and backup jobs are successful.

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:

VERITAS

VERITAS REDLab

October 2023



Feature Overview: Role-based access control (RBAC)

RBAC stands for Role-based access control, and lets the administrator configure user access to NetBackup and delegate tasks such as security management, storage management, or workload protection. RBAC follows the principle of **least privilege** that means users are granted only the minimum level of access and permissions necessary to perform their jobs. This helps enhance security by reducing the risk of unintended or unauthorized actions.

RBAC complements the ransomware resiliency posture for data protection. RBAC ensures that access to resources on NetBackup is restricted. Only the users with the Administrator role are authorized to configure and manage NetBackup. RBAC configuration is protected in catalog

VERITAS

backup of master servers and can be recovered through already established catalog recovery processes.

Here's how RBAC works in NetBackup:

1. **Roles**: NetBackup defines different roles, each with a specific set of permissions and responsibilities. These roles are typically associated with various tasks and functions within the NetBackup system.

2. **Permissions**: Each role has a set of permissions that determine the associated user actions.

3. **Users and groups**: Administrators can assign individual users or groups of users to specific roles.

4. **Access control**: RBAC controls access to various parts of the NetBackup management console and command-line interfaces. Users with specific roles can access and perform only those actions that are within their roles' permissions.

6. **Audit trail**: RBAC often includes auditing capabilities that allow administrators to track and monitor user actions. This audit trail can be crucial for compliance and security purposes, as it provides a record of user activities within the NetBackup system.

RBAC in NetBackup enhances security by ensuring that users have the appropriate level of access and control over backup and recovery operations. It helps prevent unauthorized access and minimizes the potential for errors or data breaches caused by users with overly broad permissions.

For more details, please see the Veritas RBAC White Paper.

VERITAS

VERITAS REDLab

October 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 individual ransomware families
- https://www.cisa.gov – Threat intelligence data and most pressing issues CISA is tracking, 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.

VERITAS