VERITAS

VERITAS REDLab

August 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 built by Veritas in-house to conduct our own 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. The following ransomware families are recently validated in the Veritas REDLab:

Name	Ransomware family	Behavioral Pattern
Black Basta	Black Basta	Qakbot trojans, PrintNightmare Exploit
Cl0p	Cl0p/Cryptomix	SQL injection vulnerability
Faust	Phobos ransomware family	Phishing & Social engineering tactics
BlackCat	ALPHV/BlackCat/Noberus	PsExec remote execution, deletes shadow copies
Snatch	Snatch Group	Windows Safe Mode and privileged service
Rhysida	Rhysida Malware Family	Phishing emails, Cobalt Strike and PowerShell scripts
WannaCry	WannaCryptor	EternalBlue, SMB protocol
Trigona	Trigona	MSSQL vulnerability, Splashtop remote access
Ryuk	Ryuk ransomware	Phishing emails, ZeroLogon vulnerability windows"
Royal	The Royal ransomware group	Callback phishing, SEO poisoning, Exposed RDP"
Conti	Conti ransomware group	Spearphishing campaigns and RDP attacks"
Hive	Hive Ransomware Group	phishing emails, leaked VPN credentials"
LockBit	LockBit, formerly "ABCD" ransomware	Compromise RDP/VPN, Cobalt Strike Beacon, MetaSploit, and Mimikatz

VERITAS

VERITAS

VERITAS REDLab

August 2023

Impact of attacks by the given ransomware families on NetBackup

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.
- Communication between NetBackup client and primary server is compromised that resulted in failures of backup jobs.
- 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

Data on NetBackup client is encrypted along with NetBackup configuration files.

The Client Health anomaly detection extension 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 anomaly detection extension 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:

These new 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.

VERITAS

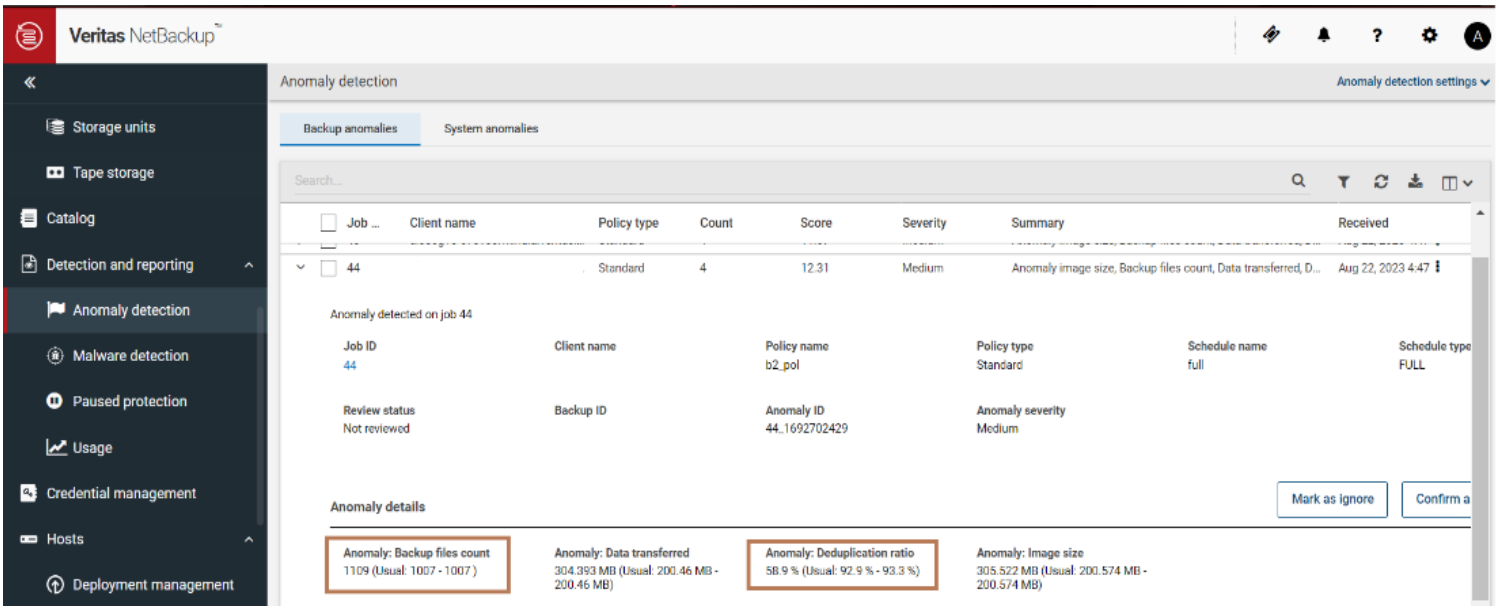
VERITAS

VERITAS REDLab

August 2023

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:



Feature preview: Isolated Recovery Environment (IRE)

NetBackup continues to focus on ransomware protection and as part of it we innovate features that help keep customers' data safe. In this edition we would like to introduce you to an Isolated Recovery Environment (IRE) that enables air-gapped backup copies by disabling network connectivity to a secure copy of your critical data, providing administrators a clean set of files on demand to neutralize the impact from a ransomware attack. NetBackup IRE solution offers a unified, scalable solution with immutability and indelibility. In addition, the

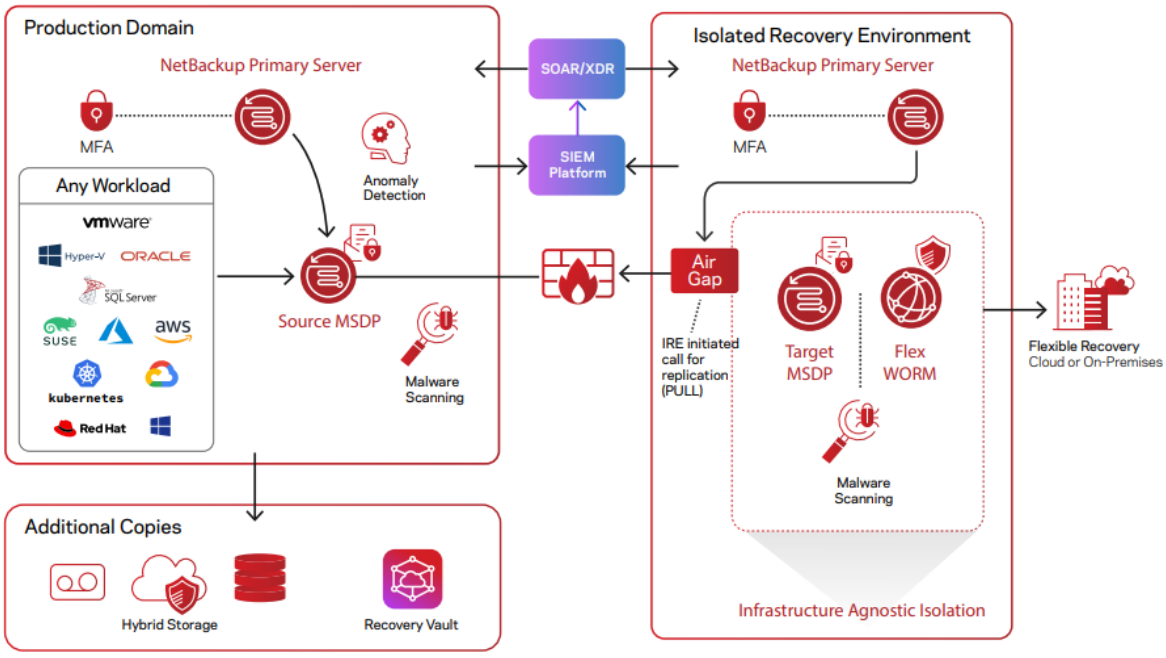
VERITAS

VERITAS

VERITAS REDLab

August 2023

Veritas IRE is based on WORM storage with hardening OS and a zero-trust architecture. NetBackup anomaly and malware detection provides another line of defense against malware propagating in the environment.



For enhanced ransomware resiliency, it is important to not only secure your backup data on immutable storage but also to maintain an isolated copy of your backup data. This is often referred to as an air-gapped copy. An Isolated Recovery Environment (IRE) enables air-gapped backup copies by disabling network connectivity to a secure copy of your critical data. It provides administrators with a clean set of files on demand to neutralize the impact from a ransomware attack.

For more detail, please review the Veritas Isolated Recovery Environment white paper.

VERITAS