Veritas™ REDLab Latest Updates

June 2023

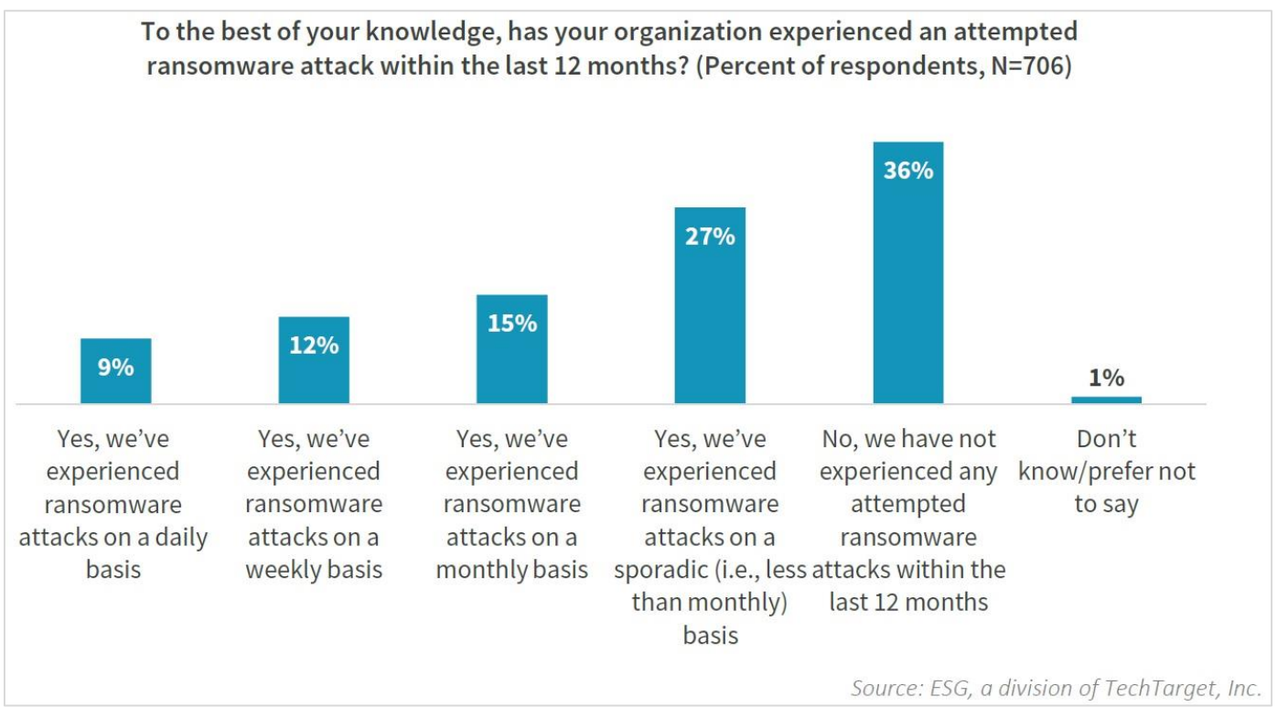
What's New?

Welcome to the latest update from the Veritas REDLab initiative. You might be asking yourself, **what is the Veritas REDLab?** Let us pass along some more information…

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 our products are hardened against attacks, protecting both the backup data and administrative interfaces, to 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 we detect an anomaly. This ensures the data is safe, protected, and that you can be confident in the cyber resilience that Veritas solutions offer.

Ransomware attacks continue to be top of mind for business and IT leaders, and for good reason. They compromise access to an organization's lifeblood— it's data.

ESG research shows that 36% of survey respondents said their organization experienced such probing attacks on at least a monthly basis over the past 12 months, including 9% that were targeted daily and 12% that were attacked weekly.



Veritas has recruited senior security experts with strong cyber security backgrounds to help with the design of the REDLab facility and to assist our team in better understanding the requirements from infrastructure, applications, ransomware identification tools, and debugging. They also helped in defining how to maintain, clean up, rebuild systems quickly, and simulate disaster recovery scenarios.

Check out this white paper for a detailed overview of our journey to get the REDLab up and running.

The growing threat and wide reach of these new attack vectors made it critical for us to engineer new *machine learning (ML)* based extensions that help our customers stay further protected and keeps their operations up and running.

New Rapid Detection Capabilities

NetBackup 10.2 introduced a new anomaly detection framework through which we delivered two new extensions, **Image Expiry** and **Client Health**. Both of these utilize our *machine learning* engine to provide just-in-time detection capabilities keeping our customers one step ahead of the new cyber attacks. These extensions and any new ones will be available in a single package to simplify deployment and will receive regular updates.

Image Expiry

With the new Image Expiry anomaly detection extension, Veritas customers no longer have to worry about unexpected admin behavior. If a malicious individual or bad actor gains elevated NetBackup admin privileges and starts expiring images unexpectedly, NetBackup will detect this condition and immediately raise an alarm drawing attention to this anomaly.

This new capability uses a machine learning based model which creates a baseline of normal administrator activity when it comes to manual expiration of images for operational needs. If a user suddenly starts performing image expirations which the ML model has not seen in the past, it will generate an anomaly alert in NetBackup and relay it to a SIEM/XDR or aggregate enterprise-wide alerts in our IT Analytics suite. The new notification reports the username and when the user carried out the abnormal activity.

Additionally, the extension will soon allow users to configure custom actions such as:

- Pausing the data protection for the compromised clients.
- Stopping image expiration of images of compromised clients.
- Triggering NetBackup recovery of critical workloads.
- Orchestrating blueprints that perform application service recovery.

Client Health

The Client Health anomaly detection extension detects unusual network communication behavior between NetBackup primary servers and clients. This checks the health of certificates deployed on the NetBackup client and triggers the anomaly detection process.

Once the anomaly is detected this extension creates a critical audit event indicating 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.

These new extensions can be downloaded from the Veritas Download Center and deployed on NetBackup 10.2 and later versions of the Primary Servers.

Refer to the June 2023 release of *Veritas Alta* - *What's New?* for more information on extensions. Connect with your Veritas account team if you do not yet have access to Veritas Alta.

Veritas solutions are designed to protect, detect, and recover rapidly at enterprise scale. Our technology delivers the fundamental capabilities needed to strengthen your cyber security posture and keep your data and applications safe and resilient across any environment.

Visit https://www.veritas.com/solution/cybersecurity to learn more about our advanced cyber resiliency solutions.