VERITAS

VERITAS REDLab

May 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
8Base	Phobos ransomware family	Command and Scripting Interpreter, Boot or Logon AutoStart Execution, File and Directory Permissions Modification, System Information Discovery, Virtualization/Sandbox Evasion
Medusa	Medusa ransomware family	Archive Collected Data, Data Encrypted for Impact, Ransomware, Crypto Virus, Files locker, Application Window Discovery, Masquerading, Registry Run Keys / Startup Folder

VERITAS

VERITAS

VERITAS REDLab

May 2024

REDLab findings:

- **8Base (attack on NetBackup client):**
    - **Family**: Phobos ransomware family | **Behavior pattern**: Command and Scripting Interpreter, Boot or Logon AutoStart Execution, File and Directory Permissions Modification, System Information Discovery, Virtualization/Sandbox Evasion
    - **Know Me:** 8base is a ransomware that belongs to the Phobos family. 8Base ransomware enumerates all available local drives, encrypts standard data file extensions in a rapid and efficient manner using AES256 in CBC mode. Any attached share or drive volume is subject to the encryption process. After the encryption, files have the .8base file extension appended to them at times with the victim ID and the attacker email address. Distribution methods for 8Base is done via infected email attachments (macros), torrent websites and malicious advertisements.
    - **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.

- **Medusa (attack on NetBackup client):**
    - **Family:** Medusa ransomware family | **Behavior pattern**: Archive Collected Data, Data Encrypted for Impact, Ransomware, Crypto Virus, Files locker, Application Window Discovery, Masquerading, Registry Run Keys / Startup Folder
    - **Know Me:** Medusa surfaced as a ransomware-as-a-service (RaaS) platform in late 2022 and gained notoriety in early 2023, primarily targeting Windows environments. Medusa should not be confused with a similarly named RaaS, MedusaLocker, which is available since 2019. Our analysis focuses solely on the Medusa ransomware, known since 2023, which impacts organizations' Windows environments. Characterized by multifaceted attacks, each encrypted by Medusa ransomware file bears diverse extensions, with ". MEDUSA" being a distinctive mark.
    - **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.

VERITAS

VERITAS

VERITAS REDLab

May 2024

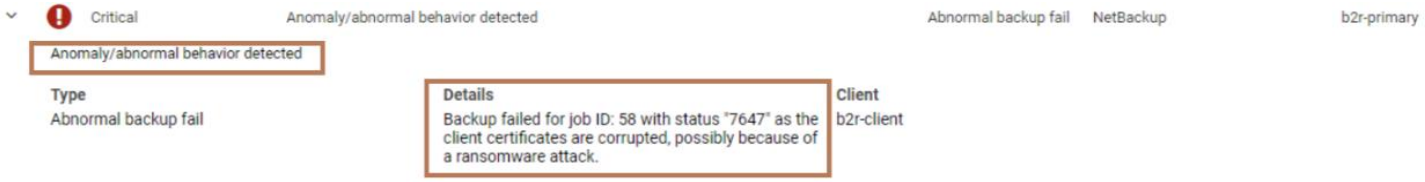
Impact of attacks on NetBackup by the given ransomware families

- 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:

- Veritas NetBackup **Client Offline** system anomaly detects a change in the health of host certificates that are deployed on the NetBackup client. When the host certificate of a NetBackup client is compromised, a system anomaly is detected, and the Client Offline system anomaly creates a critical audit event that indicates failed communications between the NetBackup services and the impacted client.

The following screenshot shows the data from REDLab:



Threat Alert: Akira

Akira emerged in March 2023 and has since targeted victims across a variety of industries, including critical infrastructure entities, in North America, Europe, and Australia. As of January 2024, the Akira TA has impacted over 250 organizations and accumulated approximately $42 million USD in ransomware proceeds. FBI, CISA, EC3 and NCSC-NL are releasing this joint CSA to disseminate known Akira ransomware IOCs

NetBackup Malware Scan results: Detected

Attack Pattern: The ransomware is designed to encrypt data on infected computers and manipulate filenames by appending the ".akira" extension.

VERITAS

VERITAS

VERITAS REDLab

May 2024

Malware Scan Host Configuration

Script options for automating configuration

A scan host in Veritas NetBackup is a host machine that has the desired malware tool configured. One or more scan hosts can be configured within a scan pool; this is helpful when many backups need to be scanned simultaneously. Once the scan pool is configured, malware scan jobs can be launched on-demand, during a recovery operation or automatically when anomalies are detected.

Scan host configuration steps can now be automated using the netbackup-scanhost-config utility. This utility installs and configures all prerequisites needed on a scan host to enable malware scanning with NetBackup.

GitHub Repository: https://github.com/VeritasOS/netbackup-scanhost-config

- **Description:**

  - This utility is supported on the following scan host operating systems only - RHEL (Red Hat Enterprise Linux) (8.x, 9.x), and Windows Server 2016 and above.
  - Additionally, this utility can be used to install NetBackup Malware Scanner on the scan host.
  - The following OS components are installed or configured by the utility on the scan hosts:
    This requires internet connectivity.
    i. Linux scan hosts:
       - Prerequisites installed:
         libnsl, NFS client, SMB client.
       - Configuration: Non-root user creation.

    ii. Windows scan hosts:
       - Prerequisites installed: OpenSSH, NFS-Client, VC Runtime
       - Configurations: Non-administrator user creation.

VERITAS

- **Scripts to configure a scan host:**

Script	Supported scan host platforms
Ansible	Linux, Windows
Shell	Linux
PowerShell	Windows

- **Steps to configure a scan host:**

You can refer to the following steps for configuring a scan host using Ansible, Additionally, you can refer to the GitHub repository for steps on how to use Shell and PowerShell to configure the scan host.

Refer to the following ReadMe files for detailed steps:

1. Ansible: https://github.com/VeritasOS/netbackup-scanhost-config/blob/main/ansible/ReadMe.md
2. Shell: https://github.com/VeritasOS/netbackup-scanhost-config/blob/main/shell/ReadMe.md
3. PowerShell: https://github.com/VeritasOS/netbackup-scanhost-config/blob/main/powershell/readme.md

For more information on Malware Scanning, see the NetBackup™ Security and Encryption Guide.

VERITAS

VERITAS REDLab

May 2024

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)
- 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

VERITAS