

Popular Backup Solution are Easily Disabled by Recent HILDACRYPT Ransomware

By AcronisThreatResearchUnit

Published: 2019-10-24 · Archived: 2026-04-05 22:37:43 UTC

Acronis

Acronis True Image

Backup and cybersecurity software you can trust

We recently analyzed a new ransomware strain named HILDACRYPT. As we explained, this ransomware specifically targets backup and anti-virus solutions from vendors including Veeam, Symantec, Veritas, Carbonite, Sophos, MBAM, McAfee, and ESET. While HILDACRYPT also targets Acronis solutions, our AI-based anti-malware defense that is integrated into Acronis Cyber Backup and Acronis True Image can detect this ransomware and stop the threat.

We decided to check a couple of backup solutions in the list to see what happens if there is a HILDACRYPT infection on the machine.

Our specialists installed the newest trial versions of **Veeam Backup and Replication** and **Veritas BackupExec**, and ran the HILDACRYPT ransomware sample we recently [reviewed in our blog](#).

Unfortunately for users of these products, the results are mostly not positive.

Veeam Backup and Replication

When hit with the HILDACRYPT ransomware, two Veeam services were stopped: vPower NFS Service and Data Mover Service.

According to Veeam, the vPower NFS Service enables the following features:

- Recovery verification
- Instant VM Recovery
- Staged restore
- Universal Application-Item Recovery (U-AIR)
- Multi-OS file-level restore

The Data Mover Service obtains job instructions and communicates with the source-side counterpart to begin data collection. While copying, the source-side Veeam Data Mover performs additional data processing (filtering out zero data blocks, blocks of swap files and blocks of excluded VM guest OS files), compresses and deduplicates VM data blocks, and moves them to the target-side Data Mover Service.

Since those tasks were stopped, we can conclude that any kind of restoration is unlikely to be successful after this attack. And if data is corrupted or encrypted, a machine or server won't get data back in easy or timely manner.

Veritas BackupExec

This test resulted in the worst-case scenario: ALL services were stopped by HILDACRYPT. After that, the bad guys can encrypt or delete the backups and do whatever they want with the data.

Hildacrypt closing down Veritas

Conclusion

HILDACRYPT may be the newest example, but Acronis has warned users and companies for a long time that modern ransomware strains are targeting backup software, files, and agents. For true protection of valuable data, modern solutions must have the ability to protect themselves from these attacks.

Acronis invested a lot of research and technology into countering this threat, which is why the integrated Acronis Active Protection technology has been proven in [independent testing](#) to give our solutions a high level of self-defense.

Unfortunately, many of our competitors' products do not deliver the same level of protection...which you ought to keep in mind when choosing a solution to safeguard your valuable data.

Source: <https://www.acronis.com/en-eu/blog/posts/popular-backup-solutions-easily-disabled-recent-hildacrypt-ransomware/>