Ransom.Win32.WHITERABBIT.YACAET - Threat Encyclopedia | Trend Micro (US)

By Analysis by: Bren Matthew Ebriega

Archived: 2026-04-05 13:01:32 UTC

This Ransomware arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

It drops files as ransom note. It avoids encrypting files with the following file extensions.

Step 1

Trend Micro Predictive Machine Learning detects and blocks malware at the first sign of its existence, before it executes on your system. When enabled, your Trend Micro product detects this malware under the following machine learning name:

- Troj.Win32.TRX.XXPE50FFF052

Step 2

Before doing any scans, Windows 7, Windows 8, Windows 8.1, and Windows 10 users must disable *System Restore* to allow full scanning of their computers.

Step 3

Note that not all files, folders, and registry keys and entries are installed on your computer during this malware's/spyware's/grayware's execution. This may be due to incomplete installation or other operating system conditions. If you do not find the same files/folders/registry information, please proceed to the next step.

Step 4

Search and delete these files

[Learn More]

There may be some files that are hidden. Please make sure you check the *Search Hidden Files and Folders* checkbox in the "More advanced options" option to include all hidden files and folders in the search result.

- {Malware Directory}\{Filename from argument}
- {Encrypted Directory}\{Filename}.scrypt.txt

Step 5

Scan your computer with your Trend Micro product to delete files detected as Ransom.Win32.WHITERABBIT.YACAET. If the detected files have already been cleaned, deleted, or quarantined by your Trend Micro product, no further step is required. You may opt to simply delete the quarantined files. Please check the following Trend Micro Support pages for more information:

- Home and Home Office Support
- Business Support

Step 6

Restore encrypted files from backup.

Did this description help? Tell us how we did.
