





Ransom.Win32.WHITERABBIT.YACAET

 trendmicro.com/vinfo/us/threat-encyclopedia/malware/Ransom.Win32.WHITERABBIT.YACAET

Analysis by: Bren Matthew Ebriega

-  Threat Type: Ransomware
-  Destructiveness: No
-  Encrypted: Yes
-  In the wild: Yes

OVERVIEW

Infection Channel: Downloaded from the Internet

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.

TECHNICAL DETAILS

Arrival Details

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.

Installation

This Ransomware drops the following files:

{Malware Directory}\{Filename from argument} → If -I was used.

It adds the following processes:

```
cmd /c choice /t 9 /d y & attrib -h {Malware Filepath}\{Malware Filename} & del  
{Malware Filepath}\{Malware Filename}
```

It adds the following mutexes to ensure that only one of its copies runs at any one time:

```
Global\{GUID}
```

Process Termination

This Ransomware terminates the following services if found on the affected system:

- msexchange*
- msex-change*
- vss
- sql
- svc\$
- memtas
- mepocs
- sophos
- veeam
- backup
- gxvss
- gxblr
- gxfwd
- gxcvd
- gxcimgr
- defwatch
- ccevtmgr
- ccsetmgr
- savroam
- rtvscan
- qbfcservice
- qbidpservice
- intuit.quickbooks.fcs
- qbcfmonitorservice
- yoobackup
- yooit
- zhudongfangyu
- stc _ raw _ agent
- vsnapvss
- veeamtransportsvc
- veeamdeploymentservice
- veeamnfssvc

- pdvfsservice
- backupexecvssprovider
- backupexeca-gentaccelerator
- backupexecagentbrowser
- backupexecdivecimediasevice
- backupexecjobengine
- backupexecmanagementservice
- backupexecrpcservice
- acrsch2svc
- acronisagent
- casad2dwebsvc
- caarcupdatesvc
- vmwp
- back
- xchange
- ackup
- acronis
- enterprise
- acrsch
- antivirus
- bedbg
- dcagent
- epsecurity
- epupdate
- eraser
- esgshkernel
- fa_scheduler
- iisadmin
- imap4
- mbam
- endpoint
- afee
- mcshield
- task
- mfemms
- mfevtp
- mms
- msdts
- exchange
- ntrt
- pdvf
- pop3

- report
- resvc
- sacsvr
- savadmin
- sams
- sdrsvc
- sepmaster
- monitor
- smcinst
- smcservice
- smtp
- snac
- swi_
- ccsf
- truekey
- tmlisten
- ui0detect
- w3s
- wrsvc
- netmsmq
- ekrn
- ehhttpsvrn

It terminates the following processes if found running in the affected system's memory:

- *sqlserver*
- agntsvc
- avp
- backup
- calc
- cntaosmgr
- dbeng
- dbeng50
- dbsnmp
- ekrn
- encsvc
- eshasrv
- excel
- firefox
- firefoxconfig
- infopath
- isqlplussvc

- kavf
- klnagent
- mbamtray
- mfefire
- msaccess
- msdtc
- mspub
- mydesktop
- mydesktopqos
- mydesktopservice
- mysql*
- notepad
- ntrtscan
- ocautoupds
- ocomm
- ocssd
- onenote
- oracle
- outlook
- pccntmon
- powerpnt
- sofos
- sqbcoreservice
- sqbcoreser-vice
- sql*
- steam
- synctime
- tbirdconfig
- thebat
- thunderbird
- tmlisten
- veeam
- virtual
- visio
- vmcomp
- vmcompute
- vmms
- vmsp
- vmwp
- wbengine
- winword
- word

- wordpad
- xchange
- xfssvccon
- zoolz

Other Details

This Ransomware does the following:

- It requires to be executed with the password/passphrase in order to proceed with its malicious routine:
KissMe
- It will encrypt files found in the following set of drives in the affected system:
 - Fixed Drives
 - Removable Drives
 - Network Drives and Resources

It accepts the following parameters:

- -p {password/passphrase}
- -f {file to encrypt}
- -l {logfile}
- -t {day}-{month}-{year} {hour}:{minute} → Use 24 Hour Format and 2 Digits

Ransomware Routine

This Ransomware avoids encrypting files with the following strings in their file name:

- *\.desktop.ini
- *\.thumbs.db

It avoids encrypting files with the following strings in their file path:

- c:\filesource*
- c:\windows*
- c:\programdata*
- %User Temp%*
- *:\sysvol*
- *:\netlogon*
- *:\windows*
- *:\programfiles*
- *:\program files (x86)*
- *:\program files (x64)*

SOLUTION

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:

Step 6

Restore encrypted files from backup.

Did this description help? Tell us how we did.