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} \rightarrow If -I was used.

It adds the following processes:

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

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
- backupexecdivecimediaservice
- 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
- ehttpsrvn

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)*

(Note: %User Temp% is the current user's Temp folder, which is usually C:\Documents and Settings\{user name}\Local Settings\Temp on Windows 2000(32-bit), XP, and Server 2003(32-bit), or C:\Users\{user name}\AppData\Local\Temp on Windows Vista, 7, 8, 8.1, 2008(64-bit), 2012(64-bit) and 10(64-bit).)

It appends the following extension to the file name of the encrypted files:

.scrypt

It drops the following file(s) as ransom note:

{Encrypted Directory}\{Filename}.scrypt.txt HELLO {Company Name} If you are reading this message, means that: - your network infrastructures have been compromised, - critical data has leaked, - files are encrypted

83

The best and only thing you can do is to contact us to settle the matter before any losses occurs.

1. THE FOLLOWING IS STRICTLY FORBIDDEN

1.1 DELETION THIS NOTE.

Each note carries the encryption key needed to decrypt the data, don't lose it

1.2 EDITING FILES OR HDD.

Renaming, copying or moving any files could DAMAGE the cypher and decryption will be impossible.

1.3 USING THIRD-PARTY SOFTWARE.

Trying to recover with any software can also break the cipher and file recovery will become a problem.

1.4 SHUTDOWN OR RESTART THE PC. Boot and recovery errors can also damage the cipher. Sorry about that, but doing so is entirely at your own risk.

1.5 HIRING THE FBI AND OTHERS

Cooperating with the FBI|CIA and so on and involving their officers in negotiations will end our communication with you and we will share all the leaked data for free.

It avoids encrypting files with the following file extensions:

- *.scrypt.txt
- *.scrypt
- *.exe
- *.dll
- *.lnk
- *.iso
- *.msi
- *.Sys
- *.inf

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 <u>disable System Restore</u> 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.