Ransom:Win32/DefrayCrypt.A

Article URL
malware.php?mal_id=186651732559d837491376d2.48661001

Author
SecurityHome.eu

Published: 07 October 2017

Aliases :

There are no other names known for **Ransom:Win32/DefrayCrypt.A**

.

Explanation :

Installation

This threat injects its code into common process, including the following Adobe-related processes:

* AcroBroker.exe
* AcroExt.exe
* AcroRd32.exe

We have seen it spread from tech scam spam emails in an Office attachment. Payload

Encrypts your files

This ransomware searches for and encrypts files in all directories except for the following:

* avast
* avg
* eset
* kaspersky
* windows

In all other folders, it encrypts files with the following extensions:

* .001
* .3d
* .3ds
* .7z
* .7zip
* .abr
* .accdb
* .afi
* .AI
* .ai
* .arw
* .asm
* .BESR
* .BIN
* .bkf
* .c
* .c4d
* .cab
* .cbm
* .cbu

* .CDR
* .class
* .cls
* .cpp
* .cr2
* .crw
* .cs
* .csh
* .csv
* .DAA
* .dat
* .db
* .dbx
* .dcr
* .dgn
* .djvu
* .DMG
* .dng
* .doc
* .docm
* .docx
* .DRW
* .dwfx
* .dwg
* .dxf
* .fla

* .fpx
* .gdb
* .gho
* .ghs
* .hdd
* .html
* .ISO
* .iso

* .ISZ
* .iv2i
* .java
* .key
* .lcf
* .matlab
* .max
* .mdb
* .MDF
* .mdi
* .mrbak
* .mrimg
* .mrw
* .nef
* .NRG
* .odg
* .ofx
* .orf

* .ova
* .ovf
* .pbd
* .PBF
* .pcd
* .pdf
* .php
* .pps
* .ppsx

* .ppt
* .pptx
* .pqi
* .prn
* .psb
* .psd
* .pst
* .ptx
* .pvm
* .pzl
* .qfx
* .qif
* .r00
* .raf
* .rar
* .raw
* .reg

* .rw2
* .s3db
* .skp
* .spf
* .spi
* .sql
* .SQLITE
* .SQLITE2
* .SQLITE3
* .SQLITEDB
* .sqlite-journal
* .stl
* .sup
* .SVG
* .swift
* .tib
* .txf
* .u3d
* .UIF
* .v2i
* .vcd
* .vcf
* .vdi
* .vhd
* .vmdk
* .vmem

* .vmwarevm
* .vmx
* .vsdx
* .wallet
* .win
* .WMF
* .xls
* .xlsm
* .xlsx
* .zip

Unlike many other types of ransomware, after the files are encrypted this ransomware doesn't rename the newly encrypted file.

Instead, it uses the same name - although the binary is different and the file can not be opened.

For example, if file.png is encrypted by this ransomware, the file will still be called file.png.

The ransomware creates notes in every directory where it encrypts files. We have observed it drop these ransom notes with the following file names:

* FILES.txt
* HELP.txt

The note contains the following text: Don't panic, read this and contact some from IT department. Your computer has been infected with a virus known as ransomware. It instructs you to contact someone from your IT department.

Deletes backup copies of files

This malware deletes local backup copies. It may attempt to delete or corrupt other backup-related processes, including processes for the following:

* Acronis TIB Mounter
* AomeiBR
* Bvckup2

* Comodo Backup
* Dropbox
* Genie9
* Google Drive
* Macrium Reflect
* Nedrive

Note: This list is not exhaustive and it may attempt to delete or corrupt other processes not listed here.

Connects to a remote host

This malware communicates with a command and control (C2) server. We have seen it connect to URLs with the subdomain 000webhostapp.com, such as:

* defrayable-listings.000webhostapp.com
* kinaesthetic-electr.000webhostapp.com

Analysis by Carmen Liang

Last update 07 October 2017