cuckoo

Analysis report summary
2023/08/19 16:30

Summary - *8b6bc16fd137c09a08b02bbe1bb7d670.bin*

File info

name:	8b6bc16fd137c09a08b02bbe1bb7d670.bin
type:	PE32 executable (GUI) Intel 80386, for MS Windows
size:	619008 bytes

Checksums

SHA1	`c69a0f6c6f809c01db92ca658fcf1b643391a2b7`
MD5	`8b6bc16fd137c09a08b02bbe1bb7d670`

Detected signatures

- Queries for the computername 9 events
- Command line console output was observed 4 events
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate
- Checks amount of memory in system, this can be used to detect virtual machines that have a lo
1 event
- One or more processes crashed 1 event
- One or more potentially interesting buffers were extracted, these generally contain injected cod
- Allocates read-write-execute memory (usually to unpack itself) 5 events
- Queries the disk size which could be used to detect virtual machine with small fixed size or dyn
- Creates (office) documents on the filesystem 8 events

Name	Data
file	`c:\Acrobat3\Reader\LICENSE.PDF`
file	`c:\Users\ahmed\documents\lurvodovdhv`
file	`c:\Users\ahmed\documents\qorvgpzeuzz`
file	`c:\Acrobat3\Reader\HELP\READER.PDF`
file	`c:\Users\ahmed\documents\gtmavsqqols`
file	`c:\Users\ahmed\documents\oucubcfmcv.`
file	`c:\Acrobat3\Reader\ACROBAT.PDF`
file	`c:\Users\ahmed\documents\jnbulrxxpb.`

- Creates a shortcut to an executable file 6 events

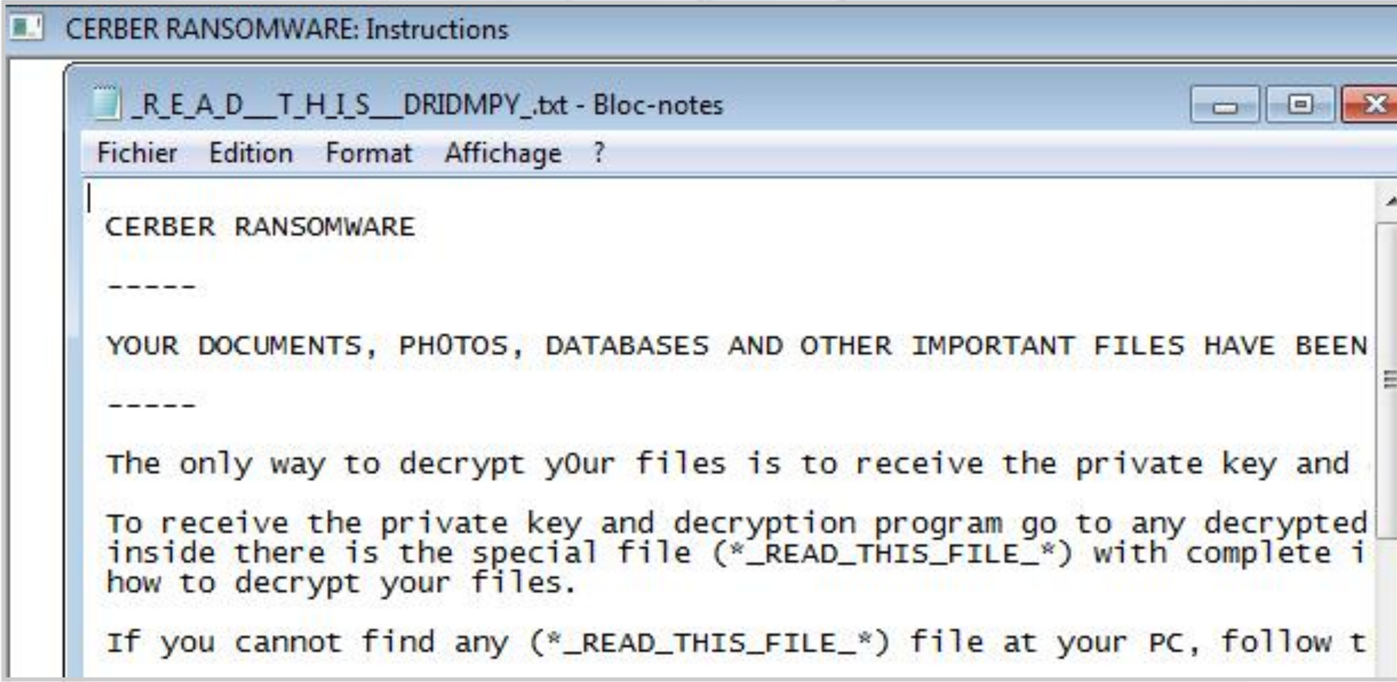
- Creates a suspicious process 2 events

cmdline	`C:\Windows\System32\cmd.exe`
cmdline	`"C:\Windows\System32\mshta.exe" "C:\Users\ahmed\Desktop\_R_E`

- Drops an executable to the user AppData folder 1 event

- Executes one or more WMI queries 2 events
- A process created a hidden window 4 events
- Moves the original executable to a new location 1 event
- Checks for the Locally Unique Identifier on the system for a suspicious privilege 1 event
- Potentially malicious URLs were found in the process memory dump 550 events
- Terminates another process 4 events
- Uses Windows utilities for basic Windows functionality 6 events
- Operates on local firewall's policies and settings 4 events
- Attempts to detect Cuckoo Sandbox through the presence of a file 1 event
- Disables proxy possibly for traffic interception 1 event
- Found URLs in memory pointing to an IP address rather than a domain (potentially indicative of
events
- Found URLs related to Tor in process memory dump (e.g. onion services, Tor2Web, and Ransom
- Writes a potential ransom message to disk 10 events

Screenshots (4/7)


CERBER RANSOMWARE: Instructions
_R_E_A_D__T_H_I_S__DRIDMPY_.txt - Bloc-notes
Fichier Edition Format Affichage ?

CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN

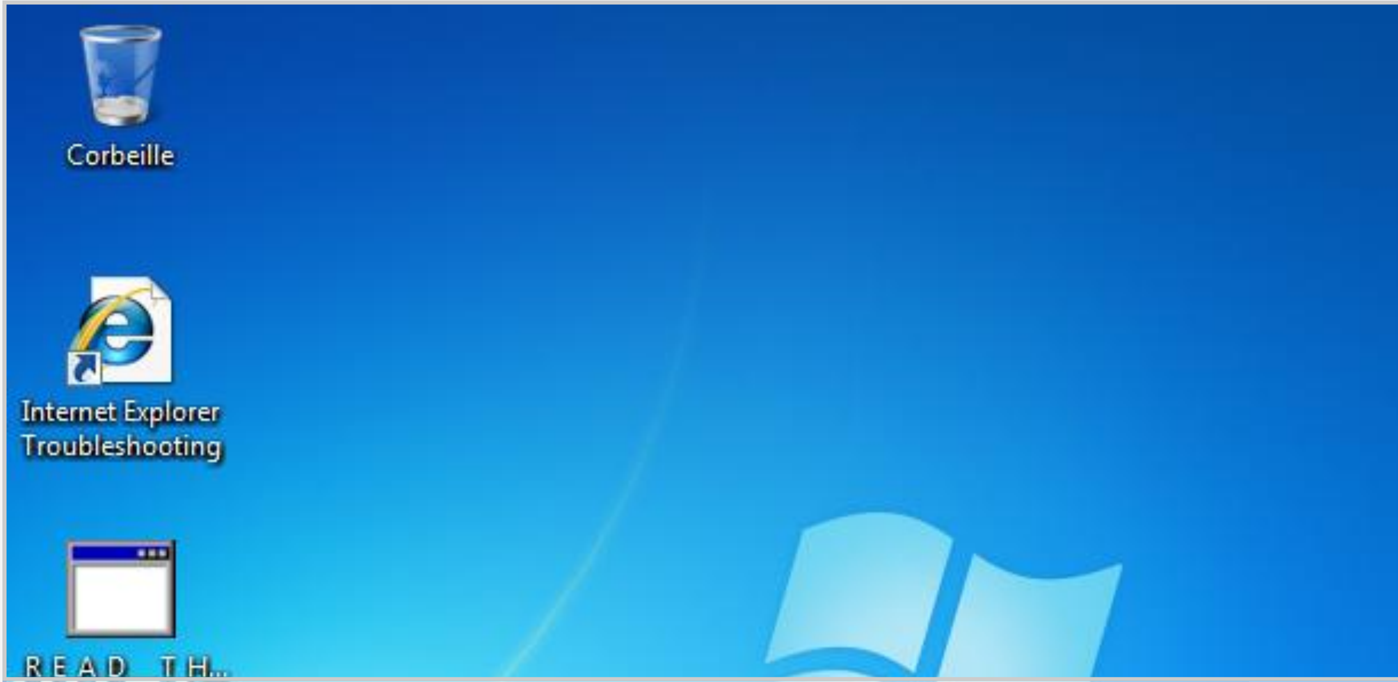
The only way to decrypt yOur files is to receive the private key and

To receive the private key and decryption program go to any decrypted inside there is the special file (*_READ_THIS_FILE_*) with complete i how to decrypt your files.

If you cannot find any (*_READ_THIS_FILE_*) file at your PC, follow t

0006.jpg

0003.jpg



0004.jpg

0001.jpg

Process memory dump

URLs found in process memory

```
http://www.iec.ch
```

http://purl.org/rss/1.0/modules/content/
http://wellformedweb.org/CommentAPI/
http://purl.org/rss/1.0/modules/syndication/
http://www.microsoft.com/schemas/rss/core/2005
http://purl.org/dc/elements/1.1/
http://www.microsoft.com/schemas/rss/core/2005/internal
http://localizability/practices/XMLConfiguration.asp
http://purl.org/atom/ns
http://purl.org/rss/1.0/
http://purl.org/dc/terms/
http://localizability/practices/XML.asp
http://www.microsoft.com/schemas/rss/monitoring/2007
http://purl.org/rss/1.0/modules/slash/