Download Sample

Download PCAP

Download PCAPNG

Feedback

Report Files Registry Network Processes Mutex Misc

General

Target
7906dc47_by_Libranalysis.exe

Filesize
22KB

Completed
21-05-2021 17:17

Score

10/10

MD5
7906dc475a8ae55ffb5af7fd3ac8f

SHA1
e7304e2436dc0eddddba229f1ec7

SHA256
1814a6a6749684cdacd792374e0b

ransomware

Analysis

MAX TIME KERNEL
149s

MAX TIME NETWORK
106s

PLATFORM
windows10_x64

RESOURCE
win10v20210408

SUBMITTED
21-05-2021 17:15

Malware Config

Extracted

Path	C:\Users\Admin\Desktop\readme.txt

E-mail

Ransom Note

```
 Any attempts to restore your files with the third party software will be fatal
for your files!

===============================================================
=====================================
 To receive the private key and decryption program follow the instructions
below:

 1. Download "Tor Browser" from https://www.torproject.org/ and install it.

 2. In the "Tor Browser" open your personal page here:


 http://6260bea096ec44d022eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj


 Note! This page is available via "Tor Browser" only.

===============================================================
=====================================
 Also you can use temporary addresses on your personal page without using
"Tor Browser":


 http://6260bea096ec44d022eltalkfzj.jobsbig.cam/eltalkfzj

 http://6260bea096ec44d022eltalkfzj.boxgas.icu/eltalkfzj

 http://6260bea096ec44d022eltalkfzj.sixsees.club/eltalkfzj

 http://6260bea096ec44d022eltalkfzj.nowuser.casa/eltalkfzj


 Note! These are temporary addresses! They will be available for a limited
amount of time!
```

Filter: none

Defense Evasion **Discovery**

Process spawned unexpected child process	cmd.exe cmd.exe cmd.exe cmd.exe cmd.exe cm
Suspicious use of NtCreateProcessExOtherParentProcess	WerFault.exe
Modifies extensions of user files	sihost.exe
Checks computer location settings	cmd.exe
Suspicious use of SetThreadContext	7906dc47_by_Libranalysis.exe
Drops file in Windows directory	MicrosoftEdge.exe
Program crash	WerFault.exe
Modifies Internet Explorer settings	MicrosoftEdge.exe browser_broker.exe MicrosoftEdg
Modifies registry class	taskhostw.exe MicrosoftEdge.exe MicrosoftEdgeCP.e

Suspicious use of UnmapMainImage Explorer.EXE ▸

Suspicious use of WriteProcessMemory sihost.exe svchost.exe cmd.exe taskhostw.exe cm ▸

▾ Processes

55

C:\Windows\Explorer.EXE PID:2996

```
C:\Windows\Explorer.EXE
```

C:\Users\Admin\AppData\Local\Temp\7906dc47_by_Libranalysis.exe PID:636

```
"C:\Users\Admin\AppData\Local\Temp\7906dc47_by_Libranalysis.exe"
```

C:\Windows\System32\RuntimeBroker.exe

PID:3436

```
C:\Windows\System32\RuntimeBroker.exe -Embedding
```

C:\Windows\System32\cmd.exe

PID:196

```
cmd.exe /c "%SystemRoot%\system32\wbem\wmic proce
ss call create "cmd /c computerdefaults.exe""
```

C:\Windows\system32\wbem\WMIC.exe

PID:4152

```
C:\Windows\system32\wbem\wmic  process call cr
```

C:\Windows\system32\wbem\WMIC.exe PID:404

```
C:\Windows\system32\wbem\wmic  process call cr
eate "cmd /c computerdefaults.exe"
```

c:\windows\svstem32\svchost.exe PID:2324