Browse / Malware sample

MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Entry

Conti

Vendor detections: **8**

Intelligence 8 | IOCs | YARA | File information | Comments 1 | Actions

SHA256 hash:	1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367
SHA3-384 hash:	5220ad49838d42d162e1266c030c27d1351f4e1cce96f12c25914758598e99ac83a4d4ef4e1ffa5986a4ec57fb838961
SHA1 hash:	e7304e2436dc0eddddba229f1ec7145055030151
MD5 hash:	7906dc475a8ae55ffb5af7fd3ac8f10a
humanhash:	oregon-cat-twelve-oregon
File name:	7906dc47_by_Libranalysis
Download:	download sample
Signature	Conti Alert
File size:	23'040 bytes
First seen:	2021-05-21 17:14:13 UTC
Last seen:	*Never*
File type:	exe
MIME type:	application/x-dosexec
ssdeep	384:otLvArTA5n2Kc/vURgbHs19l897hkuzetFS/z1ANkp2RD0CwMiOQkSd:odvOM5UNMRS7W2AiEd08D
Threatray	1 similar samples on MalwareBazaar
TLSH	77A2CF67B2E96DC6CD88247E3D87AD1815322D41F7021FAE1C4C3B7C095F12899629EB
Reporter	@Libranalysis
Tags:	conti

@Libranalysis

Uploaded as part of the sample sharing project

Intelligence

File Origin

# of uploads:	1
# of downloads:	185
Origin country:	US
Mail intelligence	No data

Vendor Threat Intelligence

ANY.RUN +

ClamAV **Detected** −

Detection(s):	SecuriteInfo.com.Variant.Mikey.122820.25534.26838.UNOFFICIAL Alert

Dr. Web vxCube Malware

Result

Verdict: Malware

Maliciousness:

Behaviour

- Changing a file
- Reading critical registry keys
- Creating a file
- Launching a process
- Creating a window
- Running batch commands
- Deleting a recently created file
- Replacing files
- Sending a UDP request
- DNS request
- Sending an HTTP GET request
- Creating a file in the mass storage device
- Stealing user critical data
- Enabling autorun with the shell\open\command registry branches
- Forced shutdown of a system process
- Encrypting user's files
- Unauthorized injection to a system process
- Unauthorized injection to a browser process

InQuest MALICIOUS

Result

Verdict: MALICIOUS

Details

Windows PE Executable	Found a Windows Portable Executable (PE) binary. Depending on context, the presence of a binary is suspicious or malicious.

Joe Sandbox Conti

Result

Threat name:	Conti Alert
Detection:	malicious
Classification:	rans.evad
Score:	100 / 100
Link:	https://www.joesandbox.com/analysis/787481

Signature

Contains functionality to create processes via WMI

Creates a thread in another existing process (thread injection)

Creates processes via WMI

Deletes shadow drive data (may be related to ransomware)

Found ransom note / readme

Found Tor onion address

Maps a DLL or memory area into another process

Modifies existing user documents (likely ransomware behavior)

Modifies the context of a thread in another process (thread injection)

Multi AV Scanner detection for submitted file

Sets debug register (to hijack the execution of another thread)

Sigma detected: Copying Sensitive Files with Credential Data

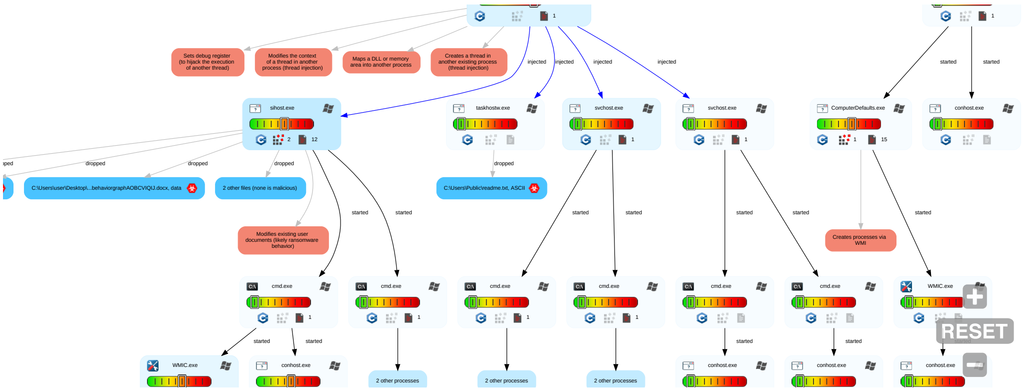
Sigma detected: Shadow Copies Deletion Using Operating Systems Utilities

Sigma detected: Suspicious Svchost Process

Yara detected Conti ransomware

Behaviour

Behavior Graph: Download SVG


Sets debug register (to hijack the execution of another thread)
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Creates a thread in another existing process (thread injection)
injected
injected
injected
injected
started
started
sihost.exe
2
12
taskhostw.exe
svchost.exe
1
svchost.exe
1
ComputerDefaults.exe
1
15
conhost.exe
dropped
dropped
dropped
dropped
C:\Users\user\Desktop\...behaviorgraphAOBCVIQIJ.docx, data
2 other files (none is malicious)
C:\Users\Public\readme.txt, ASCII
Modifies existing user documents (likely ransomware behavior)
Creates processes via WMI
started
started
started
started
started
started
started
cmd.exe
cmd.exe
cmd.exe
cmd.exe
cmd.exe
cmd.exe
WMIC.exe
started
started
started
started
started
WMIC.exe
conhost.exe
2 other processes
2 other processes
2 other processes
conhost.exe
conhost.exe
conhost.exe
RESET

CERT.PL MWDB

ReversingLabs TitaniumCloud **Win64.Trojan.Mikey** −

Threat name:	Win64.Trojan.Mikey Alert
Status:	**Malicious**
First seen:	2021-05-21 17:15:13 UTC
AV detection:	14 of 44 (31.82%)
Threat level:	□□□□□ 5/5

Spamhaus Hash Blocklist **Suspicious file** −

Detection(s):	**Suspicious file**
Link:	https://www.spamhaus.org/query/hash/dakknjtus2cm3lgxsi3u4c5ddn56j73psz27h7iv2vb27o2uantq._file

Threatray **unknown** +

Hatching Triage **Malicious** −

Result

Malware family:	n/a
Score:	□□□□□□□□□□ 10/10
Tags:	**ransomware**
Link:	https://tria.ge/reports/210521-f7lr19wnc6/

Behaviour

Modifies Internet Explorer settings

Modifies registry class

Opens file in notepad (likely ransom note)

Suspicious behavior: EnumeratesProcesses

Suspicious behavior: GetForegroundWindowSpam

Suspicious behavior: MapViewOfSection

Suspicious use of AdjustPrivilegeToken

Suspicious use of FindShellTrayWindow

Suspicious use of SendNotifyMessage

Suspicious use of SetWindowsHookEx

Suspicious use of UnmapMainImage

Suspicious use of WriteProcessMemory

Program crash

Drops file in Windows directory

Suspicious use of SetThreadContext

Checks computer location settings

Modifies extensions of user files

Process spawned unexpected child process

Suspicious use of NtCreateProcessExOtherParentProcess

VirusTotal **42.86%**

AV coverage: **42.86%**

AV detections: 30 / 70

Link: https://www.virustotal.com/gui/file/1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367/detection/f-1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367-1621609927

YOROI YOMI **Cryptor**

Threat name: Cryptor

Score: **1.00**

Link: https://yomi.yoroi.company/submissions/1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367

File information

The table below shows additional information about this malware sample such as delivery method and external references.

☹ No further information available

Comments

Login required

You need to login to in order to write a comment. Login with [your Twitter account](#).

Karlo Licudine commented on 2021-05-21 18:29:18 UTC

```
============================================================
MBC behaviors list (github.com/accidentalrebel/mbcscan):
============================================================
0) [C0026.002] Data Micro-objective::XOR::Encode Data
```