Recorded Future® Triage

Submit Reports

Overview overview 7 | Static static 3 | 015a36adea...2f.exe windows7-x64 7 | 015a36adea...2f.exe windows10-2004-x64

Report | Analysis Logs

Download Sample
Download PCAP
Download PCAPNG
Feedback
Print to PDF

Analysis

max time kernel
122s

max time network
125s

platform
windows7_x64

resource
win7-20240221-en

resource tags

ARCH:X64
ARCH:X86
IMAGE:WIN7-20240221-EN
LOCALE:EN-US
OS:WINDOWS7-X64
SYSTEM

submitted
26-02-2024 04:51

Sharing

Copy URL
Twitter
E-mail

General

Target
015a36adeafc759d8034813bff44559ef28060351dd0e8750b87fdf12802e82f.exe

Size
2.3MB

MD5
f14b54c6e41545c8ba51629183431d1d

SHA1
758aa4668d2206d3a80308ecd2fecae459fed07e

SHA256
015a36adeafc759d8034813bff44559ef28060351dd0e8750b87fdf12802e82f

SHA512
d25744c0a1185205641d3f0199bea923d4224e43ea91f371782424339c4d56bd92efe41de3c3f026bf72f5d1e6d324aff3a1d737fade6ae56d2aa3632f899fee

SSDEEP
49152:anGlmUlx7X/pQ2P6p6rVzCOKPec313JYbcBKUd+IAWgLqGWQy:aGlfXha29COKWc31ZkcBuIA/Li

Score
7/10

Malware Config

Signatures

Discovery

Loads dropped DLL • 8 IoCs

Enumerates physical storage devices • 1 TTPs
Attempts to interact with connected storage/optical drive(s).

Suspicious use of WriteProcessMemory • 22 IoCs

Processes

C:\Users\Admin\AppData\Local\Temp\015a36adeafc759d8034813bff44559ef28060351dd0e8750b87fdf12802e82f.exe — PID:3008

PID:2972

C:\Windows\SysWOW64\rundll32.exe PID:2600

```
"C:\Windows\system32\rundll32.exe"
Shell32.dll,Control_RunDLL "C:\User
s\Admin\AppData\Local\Temp\_d8c4M1.
CPL",
```

C:\Windows\system32\RunDll32.exe PID:3004

```
C:\Windows\system32\RunDll32.exe
Shell32.dll,Control_RunDLL "C:\Us
ers\Admin\AppData\Local\Temp\_d8c
4M1.CPL",
```

C:\Windows\SysWOW64\rundll32.exe PID:2576

```
"C:\Windows\SysWOW64\rundll32.e
xe" "C:\Windows\SysWOW64\shell3
2.dll",#44 "C:\Users\Admin\AppD
ata\Local\Temp\_d8c4M1.CPL",
```

Network

MITRE ATT&CK Enterprise v15

Replay Monitor

Downloads

C:\Users\Admin\AppData\Local\Temp_d8c4M1.CPL

Filesize	1.8MB
MD5	8eef672e83482bb034938cc84e9...
SHA1	6c600d6b953febf4197e7a008e65...
SHA256	069c2a3d601547af6d67cbda2b62...
SHA512	257e9d8c6e193d7eaae80d596190...

Download Submit

\Users\Admin\AppData\Local\Temp_d8c4M1.cpl

Filesize	2.0MB
MD5	4516fffb265c3011e2750a255b382...
SHA1	cd74ae4c5424e4f529e29bbd22c4...
SHA256	3dddf9d138c67c29b932605e99bc...
SHA512	3c9a4fda5d7a52b660a05d2a82f9f...

Download Submit

\Users\Admin\AppData\Local\Temp_d8c4M1.cpl

Filesize	433KB
MD5	fbc59e3025014f4e1e6d328fd9f41...
SHA1	d14910e64fbb7c07a2c212a534847...
SHA256	675f0ee2bb065775ecdf6b149d7d...
SHA512	9952bdc97236ca51dd89699b1fbc...

Download Submit

\Users\Admin\AppData\Local\Temp_d8c4M1.cpl

Filesize	192KB
MD5	c4bee1b891e726ebb017aa824c12a...
SHA1	d7caf50c47160f27591bc44a7b3c4...
SHA256	a0cc4361eaa6e3fb9ecb48294fda...
SHA512	5e103acc7e7c903ce76456cc7530...

Download Submit

memory/2576-30-0×0000000002910000-0×000...
Filesize 1.0MB
Download

memory/2576-29-0×0000000002910000-0×000...
Filesize 1.0MB
Download

memory/2576-27-0×0000000002910000-0×000...
Filesize 1.0MB
Download

memory/2576-26-0×00000000027E0000-0×00...
Filesize 1.2MB
Download

memory/2576-22-0×0000000000130000-0×000...
Filesize 24KB
Download

memory/2600-9-0×0000000000170000-0×0000...
Filesize 24KB
Download

memory/2600-17-0×0000000002790000-0×000...
Filesize 1.0MB
Download

memory/2600-16-0×0000000002790000-0×000...
Filesize 1.0MB
Download

memory/2600-15-0×0000000002790000-0×000...
Filesize 1.0MB
Download

memory/2600-13-0×0000000002790000-0×000...
Filesize 1.0MB
Download

memory/2600-12-0×0000000002660000-0×00...
Filesize 1.2MB
Download

memory/2600-8-0×0000000010000000-0×000...
Filesize 2.0MB
Download