KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_16426ff24dfb.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 36 anti-VM checks (mixed)

Analysis Overview

Score: 8/10

Threat level: Likely malicious

Malicious Activity Summary

- T1497.001
- T1571
- Process Injection: Dynamic-link Library Injection
- System Information Discovery
- Native API
- Shared Modules
- Access Token Manipulation
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion
- Process Injection
- File and Directory Discovery
- Application Layer Protocol: Web Protocols

Hashes

SHA-256:	16426ff24dfb2d568d41366471199d62a8e98fb57c5a62e23efd612cd2adc018
SHA-1:	96394a0a2d12d52ccef98d6c568b735a1020d25b
MD5:	a122d3856d069fcf34009dc5187a2425
Size:	225,831 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x12288
Sections:	8

Name	Virtual Size	Entropy

.text	0x20277	6.44
.rdata	0xE354	5.21
.data	0x1CC0	2.12
.pdata	0x19E0	5.31
.fptable	0x100	0.0
_RDATA	0x1F4	4.22
.rsrc	0x494	2.74
.reloc	0x6B8	5.05

Imports

KERNEL32.dll

AddVectoredExceptionHandler
CloseHandle
CopyFileW
CreateDirectoryW
CreateFileW
CreateMutexW
CreateProcessW
DeleteCriticalSection
EncodePointer
EnterCriticalSection

ADVAPI32.dll

GetTokenInformation
OpenProcessToken

Strings (200 found)

```
!This program cannot be run in DOS mode.$
.text
`.rdata
@.data
.pdata
@.fptable
_RDATA
@.rsrc
@.reloc
VWSH
L$8A
D$7H
T$xH
L$l1
T$HH
D$8H
L$HH
D$8H
D$pH
L$XH
L$XH
L$XH
D$8H
D$8H
```

```
T$HH
D$8H
T$HH
D$ \
D$8H
D$P\
D$8H
T$HH
D$
D$PH
D$pH
D$@H
H;D$
H;D$
$!{O
AWAVAUATVWUSH
L$pA
)D$`H
L$`A
D$`H
L$hH
T$pH1
T$0H3
D$ H3L$xH
L$8H
T$(E1
```

... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
`217.195.153.81:50000`	network

Indicators of Compromise (5)

IPv4 addresses (1)

`217.195.153.81`

Domains (4)

`api.msn.com`
`assets.msn.com`
`www.bing.com`
`arc.msn.com`

MITRE ATT&CK (12)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1571			detonation-evidence
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1082	System Information Discovery	Discovery	
T1106	Native API	Execution	

T1129	Shared Modules	Execution	
T1134	Access Token Manipulation	Privilege Escalation	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	
T1055	Process Injection		pt_trace
T1083	File and Directory Discovery		pt_trace
T1071.001	Application Layer Protocol: Web	Command and Control	behavioral_inference

Per-Process ATT&CK Attribution (3)

Which process attributed which technique, from the Intel-PT per-CR3 demux (each syscall resolved under its own process address space).

Proces				
NVDisplay.Cont	1192	1833	T1055, T1083	
jsc.exe	4528	8	T1057	
svchost.exe	756	33	T1083	

Dynamic Detonation

Coverage: ran

Behavior: malicious-behavior

Threat score: 85/100 (high)

Factors: c2, beaconing, attack_techniques

C2 beaconing: 1

Network Connections (9)

Destination	Domain	Proto
`10.0.2.3:80`		`tcp`
`10.0.2.3:443`		`tcp`
`10.0.2.3:53`		`udp`
`217.195.153.81:50000`		`tcp`
`224.0.0.251:5353`		`udp`
`224.0.0.252:5355`		`udp`
`10.0.2.255:137`		`udp`
`255.255.255.255:67`		`udp`
`10.0.2.255:138`		`udp`

TLS Handshake Failures (cert-pinning) (50)

```
assets.msn.com  (tlsstate: deadline exceeded)
login.live.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
login.live.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
```

```
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
```

Behavioral Timeline (100)

1. [conn] pid 0: udp 224.0.0.251:5353
2. [conn] pid 0: udp 224.0.0.252:5355
3. [conn] pid 0: udp 255.255.255.255:67
4. [conn] pid 0: udp 224.0.0.251:5353
5. [conn] pid 0: udp 224.0.0.252:5355
6. [conn] pid 0: udp 224.0.0.252:5355
7. [conn] pid 0: udp 10.0.2.255:137
8. [conn] pid 0: udp 10.0.2.3:53
9. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
10. [conn] pid 0: tcp 10.0.2.3:80
11. [conn] pid 0: udp 10.0.2.3:53
12. [dns] pid 0: DNS 1 login.live.com -> 10.0.2.3
13. [conn] pid 0: tcp 10.0.2.3:443
14. [conn] pid 0: udp 10.0.2.3:53
15. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
16. [conn] pid 0: tcp 10.0.2.3:80
17. [conn] pid 0: tcp 10.0.2.3:80
18. [conn] pid 0: tcp 10.0.2.3:80
19. [conn] pid 0: tcp 10.0.2.3:443
20. [conn] pid 0: tcp 10.0.2.3:80
21. [conn] pid 0: tcp 10.0.2.3:80
22. [conn] pid 0: tcp 10.0.2.3:443
23. [conn] pid 0: tcp 10.0.2.3:80
24. [conn] pid 0: tcp 10.0.2.3:80
25. [conn] pid 0: tcp 10.0.2.3:80

...and 75 more events

Packet capture: available (full PCAP)

Spawned Processes (50)

```
System
Registry
lsass.exe - C:\Windows\system32\lsass.exe
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
winlogon.exe - winlogon.exe
wininit.exe - wininit.exe
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
smss.exe - \SystemRoot\System32\smss.exe
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
msedge.exe
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:ShellFeedsUI.AppXnj65k2d1a1rnztt2t2nng5ctm
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.
```

```
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\urlhaus_1642
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
jsc.exe - "C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe"
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c855 /state1:0x41c64e6d
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\System32\svchost.exe -k NetSvcs -p -s iphlpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
```

...and 20 more