KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_e87d14fd4696.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 41 anti-VM checks (mixed)

Analysis Overview

Score: 4/10

Threat level: Suspicious

Malicious Activity Summary

- T1497.001
- T1105
- 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
- Application Layer Protocol: Web Protocols
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	e87d14fd46969a5a2341482f1e1082f00a84520b9d6fe7138807584c83a25269
SHA-1:	695fe5d40398a4f75c5125cffeb5bb1ab2117040
MD5:	1bb0a4abcc83dd82f0c7da52ce5d9e8a
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	0x480	2.72
.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)

`assets.msn.com`

`www.bing.com`

`config.edge.skype.com`

`edge-consumer-static.azureedge.net`

MITRE ATT&CK (13)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1105			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
T1071.001	Application Layer Protocol: Web	Command and Control	behavioral_inference
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Per-Process ATT&CK Attribution (4)

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

Proces			
NVDisplay.Cont	1272	1082	T1055
msedge.exe	2220	6	T1057
0x141027000		6	T1083
svchost.exe	760	24	T1083

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 45/100 (medium)

Factors: c2, attack_techniques

Network Connections (9)

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

TLS Handshake Failures (cert-pinning) (50)

```
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)
assets.msn.com  (tlsstate: deadline exceeded)
edge.microsoft.com  (remote error: tls: unknown certificate)
edge.microsoft.com  (remote error: tls: unknown certificate)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (remote error: tls: unknown certificate)
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)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (tlsstate: deadline exceeded)
```

Behavioral Timeline (100)

1. [conn] pid 0: udp 255.255.255.255:67
2. [conn] pid 0: udp 224.0.0.251:5353
3. [conn] pid 0: udp 224.0.0.252:5355
4. [conn] pid 0: udp 10.0.2.255:137
5. [conn] pid 0: udp 10.0.2.3:53
6. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
7. [conn] pid 0: tcp 10.0.2.3:80
8. [conn] pid 0: udp 224.0.0.252:5355
9. [conn] pid 0: tcp 10.0.2.3:80
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 assets.msn.com -> 10.0.2.3
13. [conn] pid 0: tcp 10.0.2.3:443
14. [conn] pid 0: tcp 10.0.2.3:443
15. [conn] pid 0: udp 10.0.2.3:53
16. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
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 10.0.2.3:80
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 10.0.2.3:80
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)

Persistence (2)

```
[Startup folder] urlhaus_e87d14fd4696.exe.local.bat -> /ProgramData/Microsoft/Windows/Start Menu/Programs/StartUp/ur
[Startup folder] malray.bat -> /ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/malray.bat
```

Spawned Processes (50)

```
svchost.exe - C:\Windows\system32\svchost.exe -k NetworkService -p -s Dnscache
System
Registry
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
smss.exe - \SystemRoot\System32\smss.exe
BdeUISrv.exe - C:\Windows\System32\BdeUISrv.exe -Embedding
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
jsc.exe - "C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe"
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s LicenseManager
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
slui.exe - "C:\Windows\System32\SLUI.exe" RuleId=31e71c49-8da7-4a2f-ad92-45d98a1c79ba;Action=AutoActivate;AppId=55c9
slui.exe - "C:\Windows\System32\SLUI.exe" RuleId=31e71c49-8da7-4a2f-ad92-45d98a1c79ba;Action=AutoActivate;AppId=55c9
```

SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A

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

svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc

msedge.exe

svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://www.msftconnect

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=networ

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --gpu-preferences=SAA

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storag

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --v

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --v

taskhostw.exe - taskhostw.exe SyncFromCloud

mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start

cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.

...and 20 more