KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_d38299b943c1.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 40 anti-VM checks (mixed)

Analysis Overview

Score: 5/10

Threat level: Suspicious

Malicious Activity Summary

- T1497.001
- T1071.001
- 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
- File and Directory Discovery
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	d38299b943c1817179a82bcde7bca8e613781c8fc00689c8abf29282b2c02309
SHA-1:	610c72729712f693d7990e717bdb7b1cd9548b6c
MD5:	901e3a08ef749329668b94cb09691d06
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	0x474	2.68
.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 (14)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			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
T1083	File and Directory Discovery		pt_trace
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Per-Process ATT&CK Attribution (5)

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

Proces				
NVDisplay.Cont	1236	908	T1055, T1083	
svchost.exe	3352	253	T1057, T1134	
0x153b82000		175	T1057	
svchost.exe	1556	202	T1134	
svchost.exe	3992	198	T1057, T1083	

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 50/100 (medium)

Factors: c2, attack_techniques

Network Connections (9)

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

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 224.0.0.252:5355`
5. `[conn] pid 0: udp 10.0.2.255:137`
6. `[conn] pid 0: udp 10.0.2.3:53`
7. `[dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3`
8. `[conn] pid 0: tcp 10.0.2.3:80`

9. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
10. [conn] pid 0: tcp 10.0.2.3:80
11. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
12. [conn] pid 0: tcp 10.0.2.3:80
13. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
14. [conn] pid 0: udp 10.0.2.3:53
15. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
16. [conn] pid 0: tcp 10.0.2.3:443
17. [conn] pid 0: tcp 10.0.2.3:443
18. [conn] pid 0: udp 10.0.2.3:53
19. [dns] pid 0: DNS 1 www.bing.com -> 10.0.2.3
20. [conn] pid 0: tcp 10.0.2.3:443
21. [conn] pid 0: tcp 10.0.2.3:443
22. [conn] pid 0: tcp 10.0.2.3:443
23. [conn] pid 0: tcp 10.0.2.3:80
24. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
25. [conn] pid 0: tcp 217.195.153.81:50000

...and 75 more events

Packet capture: available (full PCAP)

Persistence (2)

[Startup folder] urlhaus_d38299b943c1.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)

```
System
Registry
services.exe - C:\Windows\system32\services.exe
winlogon.exe - winlogon.exe
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
wininit.exe - wininit.exe
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
smss.exe - \SystemRoot\System32\smss.exe
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
msedge.exe
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
taskhostw.exe
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=gpu-process --gpu-preferences=SAA
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=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
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
netsh.exe - netsh  advfirewall set allprofiles state off
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
BdeUISrv.exe - C:\Windows\System32\BdeUISrv.exe -Embedding
jsc.exe - "C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe"
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.
```

...and 20 more