KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_aeee9e8262ae.exe

Verdict: SUSPICIOUS

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

Analysis Overview

Score: 4/10

Threat level: Suspicious

Malicious Activity Summary

- T1497.001
- T1105
- 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:	aeee9e8262aea170816e1af225dbab94ff607cd32e78ab76d41b8ec2c5a6e6d6
SHA-1:	d70250eaf001392087652da5419220049921ca8f
MD5:	93dfe7280fc32b16336d6c981421049a
Size:	243,239 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	0x4917	4.65
.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

MITRE ATT&CK (12)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1105			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 (1)

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

				Proces
NVDisplay.Cont	1180	486	T1055, T1083	

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 35/100 (medium)

Factors: dropped_exe, attack_techniques

Network Connections (6)

Destination	Domain	Proto
224.0.0.252:5355		udp
10.0.2.3:80		tcp
10.0.2.3:53		udp
10.0.2.255:137		udp
255.255.255.255:67		udp
224.0.0.251:5353		udp

Behavioral Timeline (60)

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: tcp 10.0.2.3:80
15. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
16. [conn] pid 0: tcp 10.0.2.3:80
17. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
18. [conn] pid 0: tcp 10.0.2.3:80
19. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
20. [conn] pid 0: udp 10.0.2.3:53
21. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
22. [conn] pid 0: tcp 10.0.2.3:80
23. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
24. [conn] pid 0: tcp 10.0.2.3:80
25. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt

...and 35 more events

Packet capture: available (full PCAP)

Persistence (1)

```
[Startup folder] malray.bat -> /ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/malray.bat
```

Spawned Processes (50)

```
System
Registry
svchost.exe - C:\Windows\system32\svchost.exe -k AzureAttestService -s AzureAttestService
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c855 /state1:0x41c64e6d
fontdrvhost.ex - "fontdrvhost.exe"
smss.exe - \SystemRoot\System32\smss.exe
```

```
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv 7HnBpo4/tEKjJpkFxVZKQA.0
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
```

...and 20 more