KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_2e76a50f38c1.exe

Verdict: MALICIOUS

Verdict: suspicious; 117 anti-VM checks (mixed)

Analysis Overview

Score: 6/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- Input Capture: Keylogging
- Credentials from Password Stores: Credentials from Web Browsers
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	2e76a50f38c136fba5f74d91e141869bf8cc926af5d416c3bf47cad884110f8d
SHA-1:	05b2f5d7c5806b14e7f067cf77d661b24ea46d70
MD5:	f1952aef992c8328d815b30894cfe0f6
Size:	245,248 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x3D1EE
Sections:	3

Name	Virtual Size	Entropy
.text	0x3B1F4	5.01
.rsrc	0x71A	3.86
.reloc	0xC	0.1

Imports

mscoree.dll

_CorExeMain

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
H>H}>
hSw/
=!t@K
com.apple.Safari
ixKZ-
~[b8
wCLG
Unable to resolve HTTP prox
*J(z
*J(z
*J(z
*BrR
 1SPS*
iX*B
jX(N
Zlo~
Zlo~
jX(N
?Y>3
pra#
jX(N
ca(F
Z q1
pr6/
pr6/
pr6/
pr$1
prJ2
pr83
pr83
pr83
pr83
pr56
iY(@
jYl#
@[l(
jYl#
@[l(
nXi
nXi
YjX
jYl#
@[l(
jYl#
@[l(
```

XY=Z

... and 150 more

Malware Config

Indicators of Compromise (14)

URLs (3)

`http://ip-api.com/line/?fields=hosting`

`https://account.dyn.com/`

`http://ip-api.com/line/`

Domains (11)

`ftp.vilimorin.com`

`vilimorin.com`

`ip-api.com`

`account.dyn.com`

`privateinternetaccess.com`

`paltalk.com`

`discord.com`

`assets.msn.com`

`www.bing.com`

`config.edge.skype.com`

`edge-consumer-static.azureedge.net`

MITRE ATT&CK (6)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1056.001	Input Capture: Keylogging	Credential Access	
T1555.003	Credentials from Password Stores	Credential Access	
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 65/100 (medium)

Factors: c2, evasion, attack_techniques

Network Connections (8)

Destination	Domain	Proto
`10.0.2.3:80`		`tcp`
`10.0.2.3:443`		`tcp`
`224.0.0.252:5355`		`udp`
`10.0.2.3:53`		`udp`
`10.0.2.255:138`		`udp`
`255.255.255.255:67`		`udp`

224.0.0.251:5353		udp
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)
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)
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)
```

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 10.0.2.255:137
 7. [conn] pid 0: udp 224.0.0.252:5355
 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. [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: udp 10.0.2.3:53
17. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
18. [conn] pid 0: tcp 10.0.2.3:443
19. [conn] pid 0: tcp 10.0.2.3:443
20. [conn] pid 0: udp 10.0.2.3:53
21. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
22. [conn] pid 0: tcp 10.0.2.3:80
23. [http] pid 0: GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab
24. [conn] pid 0: tcp 10.0.2.3:80
25. [http] pid 0: GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab
```

...and 75 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
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c055 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s LanmanServer
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv FpsU6GdEz0GnbF05YaKyeg.0
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
smss.exe - \SystemRoot\System32\smss.exe
slui.exe - "C:\Windows\System32\SLUI.exe" RuleId=31e71c49-8da7-4a2f-ad92-45d98a1c79ba;Action=AutoActivate;AppId=55c9
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome
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
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
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=storag
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --gpu-preferences=SAA
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
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
UserOOBEBroker - C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
BdeUISrv.exe - C:\Windows\System32\BdeUISrv.exe -Embedding
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.

...and 20 more