KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_4180269c675c.exe

Verdict: MALICIOUS

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

Analysis Overview

Score: 7/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1105
- Input Capture: Keylogging
- Application Layer Protocol: Web Protocols
- Credentials from Password Stores: Credentials from Web Browsers
- Process Injection
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	4180269c675c26e85d20a22f06587a5a45e6f4af5ee4a60fb73dc51317ce50e7
SHA-1:	b97b882b6a04a61fd479cb745bc2c10c6c6f63a9
MD5:	c761146981540c657a8fd4b761ab98b1
Size:	240,128 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x3BF4E
Sections:	3

Name	Virtual Size	Entropy
.text	0x39F54	5.01
.rsrc	0x546	3.99
.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(U
*J(U
*J(U
 1SPS*
iX*B
jX(B
ZloY
ZloY
jX(B
?Y>3
prW
pr'!
pr/#
jX(B
prG)
ca(*
Z q1
pr&-
pr&-
pr&-
pr&/
prZ/
pr>0
pr^0
iY($
nXi
jYl#
@[l(
jYl#
@[l(
YjX
nXi
jYl#
@[l(
jYl#
@[l(
 @[(
```

`KDBM(*`

... and 150 more

Malware Config

Indicators of Compromise (20)

URLs (1)

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

IPv4 addresses (5)

`2.5.29.10`

`2.5.29.14`

`2.5.29.15`

`2.5.29.19`

`2.5.29.37`

Domains (14)

`mail.outlook-office365.com`

`outlook-office365.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`

`icrosoft.net`

`oft.net`

`switch.system.io`

`switch.system.net`

MITRE ATT&CK (7)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1105			detonation-evidence
T1056.001	Input Capture: Keylogging	Credential Access	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1555.003	Credentials from Password Stores	Credential Access	
T1055	Process Injection		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
explorer.exe	4300	132	T1055	

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 69/100 (medium)

Factors: c2, evasion, attack_techniques

Network Connections (8)

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

Memory-Recovered IOCs (runtime deobfuscation) (13)

Decoded from guest memory at the hypervisor - recovered from obfuscation static analysis cannot unpack.

```
[domain] discord.com
[domain] icrosoft.net
[domain] mail.outlook-office365.com
[domain] oft.net
[domain] outlook-office365.com
[domain] privateinternetaccess.com
[domain] switch.system.io
[domain] switch.system.net
[ip] 2.5.29.10
[ip] 2.5.29.14
[ip] 2.5.29.15
[ip] 2.5.29.19
[ip] 2.5.29.37
```

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 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 10.0.2.3:53
5. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
6. [conn] pid 0: tcp 10.0.2.3:80
7. [conn] pid 0: udp 10.0.2.255:137
8. [conn] pid 0: tcp 10.0.2.3:80
9. [conn] pid 0: tcp 10.0.2.3:80
10. [conn] pid 0: udp 10.0.2.3:53
11. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
12. [conn] pid 0: tcp 10.0.2.3:443
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 10.0.2.3:80
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 (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 RPCSS -p
fontdrvhost.ex - "fontdrvhost.exe"
smss.exe - \SystemRoot\System32\smss.exe
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
slui.exe - "C:\Windows\System32\SLUI.exe" RuleId=31e71c49-8da7-4a2f-ad92-45d98a1c79ba;Action=AutoActivate;AppId=55c9
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s LicenseManager
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
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
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=edge_s
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity
UserOOBEBroker - C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://www.msftconnect
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC

```
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=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
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
SecurityHealth
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
```

...and 20 more