

Analysis Report: urlhaus_b1ec921ab8b8.exe

Verdict: **LIKELY-MALICIOUS**

Verdict: likely-malicious; 177 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Likely malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- Process Injection
- Process Injection: Dynamic-link Library Injection
- Input Capture: Keylogging
- Process Discovery
- Indicator Removal: File Deletion
- System Information Discovery
- Shared Modules
- Access Token Manipulation
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion
- File and Directory Discovery
- Scheduled Task/Job: Scheduled Task
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	b1ec921ab8b8c04be4f13b9ad814e8e3f2d6c046891c74211143330b5492dbd5
SHA-1:	7cd4be79f2ef243fbde63352ca59d5b9848dc417
MD5:	041f5888750ae8f3f6ca0a8e8b9215b6
Size:	655,952 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x76C0

Name	Virtual Size	Entropy
.text	0x1A1B1	6.55
.rdata	0xCF46	5.1
.data	0x1AEA8	1.94
.pdata	0x14A0	5.12
.fptable	0x100	0.0
.rsrc	0x73660	7.99
.reloc	0x664	4.89

Imports

KERNEL32.dll

- TerminateProcess
- CreateThread
- GetCurrentThreadId
- OpenThread
- FlushInstructionCache
- GetTickCount
- VirtualAlloc
- VirtualProtect
- VirtualFree
- GetModuleHandleA

USER32.dll

- DispatchMessageW
- GetSystemMetrics
- GetCursorPos
- wsprintfA
- MsgWaitForMultipleObjectsEx
- PeekMessageW
- TranslateMessage
- MessageBoxW
- wsprintfW
- GetAsyncKeyState

ADVAPI32.dll

- RegCloseKey
- GetTokenInformation
- OpenProcessToken
- RegQueryInfoKeyW
- RegOpenKeyExW
- GetUserNameW

COMCTL32.dll

- InitCommonControlsEx

SHLWAPI.dll

- PathFileExistsW
- StrCmpIW

UxTheme.dll

- IsAppThemed
- IsThemeActive

USERENV.dll

GetUserProfileDirectoryW

ole32.dll

CoInitializeEx

CoUninitialize

VERSION.dll

GetFileVersionInfoSizeW

Strings (200 found)

"py *
Qqra4
)f<#
|@kRich
.text
` .rdata
@.data
.pdata
@.fptable
.rsrc
@.reloc
L\$ L
SVWATAUAVAWH
D\$80le3
D\$<2.dlf
D\$@1
D\$HH
\\$ M
\\$LE2
D\$`H
D\$tH
D\$23
d\$3L
L\$LD
|\$03
d\$3H
|\$1E3
D\$`H
D\$tH
|\$03
tyD
|\$03
|\$1H
A_A^A]A_^[
\\$0H
t\$8H
|17ss
I*Ai
ssss|ls
|\$ f
|\$ fA
|ls|l3sH
D\$8H
D\$(H
\\$ A

"r?L
\\\$`H
t\$hH
|\$pH
|l7ss|ls
... and 150 more

Malware Config

Indicators of Compromise (48)

URLs (10)

https://telegram.me/m1duus
https://www.pinterest.com/m1duus
https://steamcommunity.com/profiles/76561198657426610
http://crl.comodo.net/AAACertificateServices.crl0
http://www.microsoft.com0
http://www.quovadis.bm0
https://aware-cr1.com/
https://aware-cr1.com/api/beacon
https://aware-cr1.com:443/api/beacon
https://ocsp.quovadisoffshore.com0

IPv4 addresses (16)

1.3.132.0
1.3.36.3
1.9.16.1
1.9.16.2
2.23.43.1
2.5.29.1
2.5.29.10
2.5.29.14
2.5.29.15
2.5.29.17
2.5.29.19
2.5.29.31
2.5.29.32
2.5.29.35
2.5.29.37
41.3.6.1

Domains (22)

telegram.me
www.pinterest.com
steamcommunity.com
aware-cr1.com
assets.msn.com
www.bing.com
config.edge.skype.com
edge-consumer-static.azureedge.net
crl.comodo.net
www.microsoft.com0
www.quovadis.bm0
ocsp.quovadisoffshore.com0

access.nextlsoft.com
are-cr1.com
ate.com
e-cr1.com
ipv6-literal.net
izenpe.com
ndowsupdate.com
ssl.com
stugwarepanelv2.com
www.stugwarepanelv2.com

MITRE ATT&CK (16)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1055	Process Injection	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1056.001	Input Capture: Keylogging	Credential Access	
T1057	Process Discovery	Discovery	
T1070.004	Indicator Removal: File Deletion	Defense Evasion	
T1082	System Information Discovery	Discovery	
T1129	Shared Modules	Execution	
T1134	Access Token Manipulation	Privilege Escalation	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	
T1083	File and Directory Discovery		pt_trace
T1053.005	Scheduled Task/Job: Scheduled Ta	Persistence	behavioral_inference
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).

				Process
msedge.exe	5512	155	T1057, T1083	
RuntimeBroker.	6040	115	T1057, T1083	
0x147121000		326	T1083	
0x124d7d000		17	T1083	
0x124d83000		13	T1083	

Dynamic Detonation

Coverage: ran
Behavior: malicious-behavior
Threat score: 70/100 (high)
Factors: c2, attack_techniques

Network Connections (8)

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

Memory-Recovered IOCs (runtime deobfuscation) (38)

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

[url] http://crl.comodo.net/AAACertificateServices.cr10

[url] http://www.microsoft.com0

[url] http://www.quovadis.bm0

[url] https://aware-cr1.com/

[url] https://aware-cr1.com/api/beacon

[url] https://aware-cr1.com:443/api/beacon

[url] https://ocsp.quovadisoffshore.com0

[domain] access.nextlsoft.com

[domain] are-cr1.com

[domain] ate.com

[domain] aware-cr1.com

[domain] crl.comodo.net

[domain] e-cr1.com

[domain] ipv6-literal.net

[domain] izenpe.com

[domain] ndowsupdate.com

[domain] ocsp.quovadisoffshore.com0

[domain] ssl.com

[domain] stugwarepanelv2.com

[domain] www.microsoft.com0

[domain] www.quovadis.bm0

[domain] www.stugwarepanelv2.com

[ip] 1.3.132.0

[ip] 1.3.36.3

[ip] 1.9.16.1

...and 13 more

TLS Handshake Failures (cert-pinning) (50)

www.bing.com (tlsstate: deadline exceeded)

assets.msn.com (tlsstate: deadline exceeded)

assets.msn.com (tlsstate: deadline exceeded)

www.bing.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)

www.bing.com (tlsstate: deadline exceeded)

www.bing.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 224.0.0.252:5355
7. [conn] pid 0: udp 224.0.0.252:5355
8. [conn] pid 0: udp 10.0.2.255:137
9. [conn] pid 0: udp 10.0.2.3:53
10. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
11. [conn] pid 0: tcp 10.0.2.3:80
12. [conn] pid 0: tcp 10.0.2.3:80
13. [conn] pid 0: tcp 10.0.2.3:80
14. [conn] pid 0: udp 10.0.2.3:53
15. [dns] pid 0: DNS 1 aware-cr1.com -> 10.0.2.3
16. [conn] pid 0: tcp 10.0.2.3:443
17. [conn] pid 0: udp 10.0.2.3:53
18. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
19. [conn] pid 0: tcp 10.0.2.3:80
20. [conn] pid 0: tcp 10.0.2.3:80
21. [conn] pid 0: udp 10.0.2.3:53
22. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
23. [conn] pid 0: tcp 10.0.2.3:443
24. [conn] pid 0: tcp 10.0.2.3:443
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
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe"
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.AppXnn6fnh4raxtmg45ba8k2f4yk
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
urlhaus_b1ec92 - svchost.exe
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler --user-data-dir=C:\Program Files (x86)\Microsoft\Edge\User Data\Default
```

msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --gpu-preferences=SA
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=networ
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
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=utility --utility-sub-type=entity
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1\JOH\AppData\Local\Temp\~st0000
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
fontdrvhost.exe - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
lsass.exe - C:\Windows\system32\lsass.exe
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
NVIDIA.Container - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContainer
...and 20 more

Report ID: owu3zrl4ViCOskHmQR_mKI0ggFCMliFDFuoyU59V5_I

Generated by KVMX - kvmx.ai