KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_e2b6dbb5b5c4.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 745 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Suspicious

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
- Scheduled Task/Job: Scheduled Task
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	e2b6dbb5b5c44863df8e9e79a6c0d0c4d8fe7bfca346335fbfcd4dc6ca5f9010
SHA-1:	ef72cfef1a1e57d55376ffe629fa7275238c1951
MD5:	a518660aec0ba76afbe4ac9d9443132f
Size:	434,688 bytes

Packer Detection

No packer detected.

PE Information

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

Sections: 7

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	0x3FFDC	7.45
.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)

```
sb 4t
wRich
.text
`.rdata
@.data
.pdata
@.fptable
.rsrc
@.reloc
L$ L
SVWATAUAVAWH
D$8ole3
D$<2.dlf
D$@l
D$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$8H
|l7ss
|lsDi
I*Ai
ssss
|$ f
|$ fA
|l3s
D$8H
D$(H
\$ A
"r?L
```

\$`H

t$hH

|$pH

ssss|l3s

r4E3

... and 150 more

Malware Config

Indicators of Compromise (46)

URLs (9)

- http://crl.comodo.net/AAACertificateServices.crl0
- http://vexdico.s
- http://vexdico.shop:8539/
- http://vexdico.shop:8539/files
- http://vexdico.shop:8539/files-89
- http://www.microsoft.com0
- http://www.quovadis.bm0
- https://aware-cr1.com/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 (21)

- aware-cr1.com
- vexdico.shop
- assets.msn.com
- www.bing.com
- config.edge.skype.com
- edge-consumer-static.azureedge.net
- crl.comodo.net
- vexdico.s
- www.microsoft.com0
- www.quovadis.bm0
- ocsp.quovadisoffshore.com0
- access.nextlsoft.com
- e-cr1.com

ipv6-literal.net
izenpe.com
l.aware-cr1.com
ndowsupdate.com
o.shop
ssl.com
stugwarepanelv2.com
www.stugwarepanelv2.com

MITRE ATT&CK (15)

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	
T1053.005	Scheduled Task/Job: Scheduled Ta	Persistence	behavioral_inference
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 69/100 (medium)

Factors: c2, evasion, attack_techniques

Network Connections (9)

Destination	Domain	Proto
224.0.0.251:5353		udp
10.0.2.3:80		tcp
10.0.2.3:443		tcp
10.0.2.3:53		udp
224.0.0.252:5355		udp
10.0.2.255:138		udp
10.0.2.255:137		udp
255.255.255.255:67		udp
10.0.2.3:8539		tcp

Memory-Recovered IOCs (runtime deobfuscation) (42)

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

```
[url] http://crl.comodo.net/AAACertificateServices.crl0
[url] http://vexdico.s
[url] http://vexdico.shop:8539/
[url] http://vexdico.shop:8539/files
[url] http://vexdico.shop:8539/files-89
[url] http://www.microsoft.com0
[url] http://www.quovadis.bm0
[url] https://aware-cr1.com/api/beacon
[url] https://ocsp.quovadisoffshore.com0
[domain] access.nextlsoft.com
[domain] aware-cr1.com
[domain] crl.comodo.net
[domain] e-cr1.com
[domain] ipv6-literal.net
[domain] izenpe.com
[domain] l.aware-cr1.com
[domain] ndowsupdate.com
[domain] o.shop
[domain] ocsp.quovadisoffshore.com0
[domain] ssl.com
[domain] stugwarepanelv2.com
[domain] vexdico.s
[domain] vexdico.shop
[domain] www.microsoft.com0
[domain] www.quovadis.bm0
```

...and 17 more

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 10.0.2.3:53
8. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
9. [conn] pid 0: tcp 10.0.2.3:80
10. [conn] pid 0: udp 224.0.0.252:5355
11. [conn] pid 0: tcp 10.0.2.3:80
12. [conn] pid 0: tcp 10.0.2.3:80
13. [conn] pid 0: udp 10.0.2.3:53
14. [dns] pid 0: DNS 1 aware-cr1.com -> 10.0.2.3
15. [conn] pid 0: tcp 10.0.2.3:443
16. [conn] pid 0: udp 10.0.2.3:53
17. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
18. [conn] pid 0: tcp 10.0.2.3:80
19. [conn] pid 0: tcp 10.0.2.3:80
20. [conn] pid 0: udp 10.0.2.3:53
21. [dns] pid 0: DNS 1 vexdico.shop -> 10.0.2.3
22. [conn] pid 0: tcp 10.0.2.3:8539
23. [conn] pid 0: udp 10.0.2.3:53
24. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
25. [conn] pid 0: tcp 10.0.2.3:443

...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 netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
smss.exe - \SystemRoot\System32\smss.exe
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
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=utility --utility-sub-type=entity
urlhaus_e2b6db - svchost.exe
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
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
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
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.
taskhostw.exe - taskhostw.exe SyncFromCloud
```

```
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
```

...and 20 more