# KVMX

Evidence-First Malware Analysis

## Analysis Report: urlhaus_660966e3a75d.exe

### Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 102 anti-VM checks (mixed)

## Analysis Overview

# Score: 7/10

**Threat level: Likely malicious**

**Malicious Activity Summary**

- Decrypted C2 recovered (1 HTTPS request(s)) - TLS-MITM at the hypervisor
- 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:** | 660966e3a75d5243ba66ef04e8aea4d66bfb325a4f3959c6d15b476351ad8d41 |
| **SHA-1:** | c42165cbd0bd0ba1d01e8d5222871e5976f22c52 |
| **MD5:** | bf8bdad0876ea167c165929e0aaa17e2 |
| **Size:** | 1,474,800 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 | 0x13AEE8 | 7.88 |
| .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)

```
Rich
.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$8H
sssss
I*Ai
|ls|l3s
|$ f
|$ fA
|lsH
D$8H
D$(H
\$ A
"r?L
\$`H
t$hH
```

`|$pH`

`|l7ss|l3s`

`r4E3`

`TCDA`

`D$`H`

*... and 150 more*

## Malware Config

### C2 / Network (5)

| Endpoint | Source |
|---|---|
| `api.msn.com` | decrypted_c2 |
| `assets.msn.com` | decrypted_c2 |
| `fs.microsoft.com` | decrypted_c2 |
| `realniggacheats.cc` | decrypted_c2 |
| `www.bing.com` | decrypted_c2 |

## Indicators of Compromise (13)

### URLs (3)

`https://telegram.me/s11yme`

`https://dev.epicgames.com/community/api/user_profiles/profile.json`

`https://steamcommunity.com/profiles/76561198652917381`

### Domains (10)

`telegram.me`

`dev.epicgames.com`

`steamcommunity.com`

`api.msn.com`

`assets.msn.com`

`www.bing.com`

`realniggacheats.cc`

`aware-cr1.com`

`config.edge.skype.com`

`edge-consumer-static.azureedge.net`

## 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:** 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 |
| 224.0.0.252:5355 | | udp |
| 255.255.255.255:67 | | udp |
| 10.0.2.255:137 | | udp |
| 10.0.2.255:138 | | udp |
| 224.0.0.251:5353 | | udp |

### Decrypted C2 (TLS-MITM) (1)

```
HEAD /fs/windows/config.json  [status=501 sni=fs.microsoft.com]
```

### 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)
config.edge.skype.com  (remote error: tls: unknown certificate)
www.bing.com  (remote error: tls: unknown certificate)
assets.msn.com  (tlsstate: deadline exceeded)
edge.microsoft.com  (remote error: tls: unknown certificate)
www.bing.com  (remote error: tls: unknown certificate)
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 10.0.2.255:137
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 aware-cr1.com -> 10.0.2.3
18. [conn] pid 0: tcp 10.0.2.3:443
19. [conn] pid 0: udp 10.0.2.3:53
20. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
21. [conn] pid 0: tcp 10.0.2.3:80
22. [http] pid 0: GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
23. [conn] pid 0: tcp 10.0.2.3:80
24. [http] pid 0: GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
25. [conn] pid 0: udp 10.0.2.3:53

*...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
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
Registry
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s LicenseManager
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
mobsync.exe - C:\Windows\System32\mobsync.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
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0001
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
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --gpu-preferences=SAA
taskhostw.exe - taskhostw.exe $(Arg0)
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storag
BdeUISrv.exe - C:\Windows\System32\BdeUISrv.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=networ
urlhaus_660966 - svchost.exe
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
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0001
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0001
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
SecurityHealth

```
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0001
schtasks.exe
```

*...and 20 more*