# KVMX

Evidence-First Malware Analysis

## Analysis Report: urlhaus_4b0d8aaa3f52.exe

### Verdict: SUSPICIOUS

Verdict: suspicious; 62 anti-VM checks (mixed)

### Analysis Overview

# Score: 4/10

### Threat level: Suspicious

**Malicious Activity Summary**

- T1027.002
- T1497.001
- T1071.001
- T1105
- Obfuscated Files or Information
- Boot or Logon Autostart Execution: Registry Run Keys

### Hashes

| | |
|---|---|
| **SHA-256:** | 4b0d8aaa3f52f48c5c59d368bf925b4456f39162b16dba03dc328678c6208a7b |
| **SHA-1:** | b09195b0e8fb7122c7cfbc9f3dadee8b1a329e2a |
| **MD5:** | 8f42c066a13d5e5d023c96607d310414 |
| **Size:** | 286,208 bytes |

### Packer Detection

| | |
|---|---|
| **Packer:** | Unknown packer (high entropy in .text) |
| **Confidence:** | medium |

### PE Information

| | |
|---|---|
| **Architecture:** | 32-bit |
| **Type:** | Executable |
| **Entry Point:** | 0x26E0 |
| **Sections:** | 1 |

| Name | Virtual Size | Entropy |
|---|---|---|
| .text | 0x44E00 | 7.99 |

### Strings (200 found)

```
MZER
```

```
!This program cannot be run in DOS mode.
Rich
.text
;JPu
uiPt
k0g_
=bP5S
D$_
9,c$
5u?h
 d^=
?5\Y
-4ZG
6>{ @
oO)f
m^5A
rJ1PB
KX9:
h|po
5Wu?
f J|"A;
"+*Qs
mK0U
`p2#
"4T{k
C6][:
b?v>q
zH%o
0KsA
VA!8
QmXs
k31'Cb[
aP{@K
;lFD
V~eu
PI!!`Y*
!P1C
:(@=?
Scq+
#+;$
,f?;
LL9(
0+d}
vM\:
^%c`
OU#R
(;0%
tI1,
m'-jL
```

*... and 150 more*

## Malware Config

## Indicators of Compromise (17)

### URLs (6)

- `http://www.bshuhd.com/yy2f/`
- `http://www.avspd.cc/scpn/`
- `http://www.deikos.xyz/isb9/`
- `http://www.springcityrealty.click/y25g/`
- `http://www.zzwksw.com/jbpt/`
- `http://www.en-en-neuropan.com/9fn3/`

### Domains (10)

- `www.bshuhd.com`
- `www.avspd.cc`
- `www.deikos.xyz`
- `www.springcityrealty.click`
- `www.zzwksw.com`
- `www.en-en-neuropan.com`
- `assets.msn.com`
- `www.bing.com`
- `config.edge.skype.com`
- `edge-consumer-static.azureedge.net`

### File paths (1)

- `x:\}`

## MITRE ATT&CK (6)

| Technique | Name | Tactic | Source |
|---|---|---|---|
| T1027.002 | | | detonation-evidence |
| T1497.001 | | | detonation-evidence |
| T1071.001 | | | detonation-evidence |
| T1105 | | | detonation-evidence |
| T1027 | Obfuscated Files or Information | Defense Evasion | |
| T1547.001 | Boot or Logon Autostart Executio | Persistence | behavioral_inference |

## Dynamic Detonation

**Coverage:** ran

**Behavior:** suspicious

**Threat score:** 40/100 (medium)

**Factors:** c2, attack_techniques

### Network Connections (8)

| Destination | Domain | Proto |
|---|---|---|
| `10.0.2.3:80` | | `tcp` |
| `10.0.2.3:53` | | `udp` |
| `10.0.2.3:443` | | `tcp` |
| `224.0.0.252:5355` | | `udp` |
| `10.0.2.255:137` | | `udp` |
| `224.0.0.251:5353` | | `udp` |
| `10.0.2.255:138` | | `udp` |
| `255.255.255.255:67` | | `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)
functional.events.data.microsoft.com  (remote error: tls: unknown certificate)
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: tcp 10.0.2.3:80
11. [conn] pid 0: udp 10.0.2.3:53
12. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
13. [conn] pid 0: tcp 10.0.2.3:443
14. [conn] pid 0: tcp 10.0.2.3:443
15. [conn] pid 0: udp 10.0.2.3:53
16. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
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
smss.exe
winlogon.exe - winlogon.exe
wininit.exe - wininit.exe
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
smss.exe - \SystemRoot\System32\smss.exe
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
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" --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=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=utility --utility-sub-type=networ
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
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv R+K5+6kxHUW9R9biL103Uw.0
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
services.exe - C:\Windows\system32\services.exe
svchost.exe - C:\Windows\system32\svchost.exe -k NetworkService -p -s Dnscache
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
```

*...and 20 more*