# KVMX

Evidence-First Malware Analysis

## Analysis Report: urlhaus_dc5ced17f0c8.exe

### Verdict: SUSPICIOUS

Verdict: suspicious; 42 anti-VM checks (mixed)

## Analysis Overview

# Score: 3/10

### Threat level: Suspicious

**Malicious Activity Summary**

- T1027.002
- T1497.001
- Obfuscated Files or Information
- Process Injection
- File and Directory Discovery

## Hashes

| | |
|---|---|
| **SHA-256:** | dc5ced17f0c85fef8a1fa466796a84fb83592eb7c8a86302d9b0cc9e5837c140 |
| **SHA-1:** | 0b93ef56795109dce8b398912f0d1e10905bfb23 |
| **MD5:** | 077bb61e9d3cc382319c34388faf2065 |
| **Size:** | 286,720 bytes |

## Packer Detection

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

## PE Information

| | |
|---|---|
| **Architecture:** | 32-bit |
| **Type:** | Executable |
| **Entry Point:** | 0x26B0 |
| **Sections:** | 1 |

| Name | Virtual Size | Entropy |
|---|---|---|
| .text | 0x45000 | 8.0 |

## Strings (200 found)

```
MZER
!This program cannot be run in DOS mode.
```

```
Rich
.text
d4+U
Pt;Q
5>8{
Jt;H
Jt;H
WI"@
|W;$
$@o\
ttW~
?|PDiXb
sMY>
yI0M
wNF.
LCZ%
KD_<v
9"R+
v'3K
ML;%K
2R~3
^Y2n
XvzV
;2qr
P4@])u
LE?^y
oV2[,
<hNB1
)1p_H
bUkhim0
v^'b
J,*I
(zJ>
$@m6
gtM.\
[(d:
lO1K
T1Re~od
Ialg
Tv]P
%Do>
SU@0
zs1,
i,%js
W0;6
F(8$
!5'1
1i?F
```

*... and 150 more*

## MITRE ATT&CK (5)

| Technique | Name | Tactic | Source |
|---|---|---|---|
| T1027.002 | | | detonation-evidence |

| | | | |
|---|---|---|---|
| T1497.001 | | | detonation-evidence |
| T1027 | Obfuscated Files or Information | Defense Evasion | |
| T1055 | Process Injection | | pt_trace |
| T1083 | File and Directory Discovery | | pt_trace |

## Per-Process ATT&CK Attribution (4)

*Which process attributed which technique, from the Intel-PT per-CR3 demux (each syscall resolved under its own process address space).*

| Proces | | | | |
|---|---|---|---|---|
| NVDisplay.Cont | 1180 | 874 | T1055, T1083 | |
| 0x173231000 | | 37 | T1055 | |
| svchost.exe | 1256 | 20 | T1057 | |
| svchost.exe | 752 | 15 | T1083 | |

## Dynamic Detonation

**Coverage:** ran

**Behavior:** suspicious

**Threat score:** 30/100 (medium)

**Factors:** dropped_exe, attack_techniques

### Network Connections (6)

| Destination | Domain | Proto |
|---|---|---|
| `10.0.2.3:80` | | `tcp` |
| `10.0.2.3:53` | | `udp` |
| `255.255.255.255:67` | | `udp` |
| `224.0.0.252:5355` | | `udp` |
| `224.0.0.251:5353` | | `udp` |
| `10.0.2.255:137` | | `udp` |

### Behavioral Timeline (60)

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 224.0.0.252:5355`
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. `[http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt`
11. `[conn] pid 0: tcp 10.0.2.3:80`
12. `[http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt`
13. `[conn] pid 0: tcp 10.0.2.3:80`
14. `[http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt`
15. `[conn] pid 0: tcp 10.0.2.3:80`
16. `[http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt`
17. `[conn] pid 0: tcp 10.0.2.3:80`
18. `[http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt`
19. `[conn] pid 0: tcp 10.0.2.3:80`
20. `[http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt`

```
21. [conn] pid 0: udp 10.0.2.3:53
22. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
23. [conn] pid 0: tcp 10.0.2.3:80
24. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
25. [conn] pid 0: tcp 10.0.2.3:80
```

*...and 35 more events*

**Packet capture:** available (full PCAP)

### Spawned Processes (50)

```
System
Registry
services.exe - C:\Windows\system32\services.exe
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2d055 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
lsass.exe - C:\Windows\system32\lsass.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
smss.exe - \SystemRoot\System32\smss.exe 00000080 00000084
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv k1zQ7MefCUe82cLFOTyZ4A.0
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Winmgmt
```

*...and 20 more*