# KVMX

Evidence-First Malware Analysis

## Analysis Report: 24de9e8109b96df4.bin

### Verdict: MALICIOUS

Verdict: suspicious; 60 anti-VM checks (mixed)

### Analysis Overview

# Score: 3/10

### Threat level: Malicious

**Malicious Activity Summary**

- Family: Formbook
- T1027.002
- T1497.001
- T1027

### Hashes

| | |
|---|---|
| **SHA-256:** | 24de9e8109b96df449fcbf9722bccc8dc22c2b666854e53f3974233bd4fb9e35 |
| **SHA-1:** | 870236e97a76f7ce35ec0600a78807358d524525 |
| **MD5:** | 87bbaac098c22beb0c40621967a1573e |
| **Size:** | 283,136 bytes |

### Packer Detection

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

### PE Information

| | |
|---|---|
| **Architecture:** | 32-bit |
| **Type:** | Executable |
| **Entry Point:** | 0x2690 |
| **Sections:** | 1 |

| Name | Virtual Size | Entropy |
|---|---|---|
| .text | 0x44200 | 8.0 |

### Strings (200 found)

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

```
.text
Bv5X
;H9}<
;H9}
;B9u9
Bv5P
;QlsP
;A1u9
RFT]
X]q?g'ra
" VU
4t]SK
1:;D.
`tKH
LzBEb"7g
LtvpR
JqnWy
3Q+b
c6>h
(I>3UTd=
 80t
 :j:
#?f<*Y
3Nu|
r']%Lnw
3LkN}&dBS]'
N)Wxn
V2#^
K|%/
`|Sj)
wpp]
w$]SO*
}\qm
tQ<,
31&jg
7\RX*
~0eL
T04a<
aMit
bbFO
 'h:
-<pJR
1\*0
o1-}
6B(N
*b%i
LXle
```

*... and 150 more*

## Malware Config

**Family:** Formbook

## MITRE ATT&CK (3)

| Technique | Name | Tactic | Source |
|---|---|---|---|
| T1027.002 | | | detonation-evidence |
| T1497.001 | | | detonation-evidence |
| T1027 | | | static-analyzer |

## Dynamic Detonation

**Coverage:** ran

**Behavior:** suspicious

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

**Factors:** dropped_exe

### Network Connections (6)

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

### Behavioral Timeline (54)

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 29 more events*

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

**Spawned Processes (10)**

```
System
Registry
smss.exe - \SystemRoot\System32\smss.exe
taskhostw.exe
svchost.exe
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
smss.exe
winlogon.exe - winlogon.exe
wininit.exe - wininit.exe
slui.exe
```

Report ID: JCWdCen0fAjP7JjA9O42_9F5fnAkcl7A8F678Br7jhc
Generated by KVMX - kvmx.ai