# KVMX

Evidence-First Malware Analysis

## Analysis Report: urlhaus_1ebf64ceb8ec.exe

### Verdict: MALICIOUS

Verdict: suspicious; 40 anti-VM checks (mixed)

### Analysis Overview

# Score: 3/10

### Threat level: Malicious

**Malicious Activity Summary**

- T1027.002
- T1497.001
- Obfuscated Files or Information
- Process Injection
- Input Capture: Keylogging
- Application Layer Protocol: Web Protocols
- Ingress Tool Transfer
- Data Encrypted for Impact
- Service Stop
- Resource Hijacking
- Credentials from Password Stores: Credentials from Web Browsers

### Hashes

| | |
|---|---|
| **SHA-256:** | 1ebf64ceb8ec5601ead8cd44c4a3b22a7e9b5a8a4432ea70e96e2837495b19a9 |
| **SHA-1:** | 812a04bdcfda4c78ce5c21eb84ba82feb9d50a8d |
| **MD5:** | afd6ecf0fc85d3fe1d30f616e4774ff8 |
| **Size:** | 2,554,368 bytes |

### Packer Detection

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

### PE Information

| | |
|---|---|
| **Architecture:** | 32-bit |
| **Type:** | Executable |
| **Entry Point:** | 0x270E4E |
| **Sections:** | 3 |

| Name | Virtual Size | Entropy |
|---|---|---|

| | | |
|---|---|---|
| .text | 0x26EE54 | 7.72 |
| .rsrc | 0x5CE | 4.14 |
| .reloc | 0xC | 0.08 |

## Imports

**mscoree.dll**

_CorExeMain

## Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
p*rF
*F~&
*.~?
*Z(;
*2~9
*Z(;
*n~B
*. @B
*V(W
*.(g
&*^~
*R(-
*.su
prra
*^~&
&*.~&
*.s
*.("
*.($
*.(%
*.sh
&*.sv
+*.s
+*2r^
*z~e
*2~G
*6(@
*.s[
_h*J
&*B~0
*F()
*.(,
&*V(-
*.s:
prfH
*R(S
,3(+
-8s>
```

```
,p(H
-Ls>
-Asb
16sb
,}rR
-csb
-csb
,;~B
```
*... and 150 more*

## Indicators of Compromise (21)

### URLs (7)

```
https://t.me/example
https://pastebin.com/raw/ebwkm4hs
https://ipwhois.app/json/
http://ip-api.com/json/?fields=status,country,regionName,city,lat,lon,isp,query
https://ipinfo.io/json
https://geolocation-db.com/json/
https://api.my-ip.io/ip.json
```

### IPv4 addresses (2)

```
8.8.8.8
1.1.1.1
```

### Domains (12)

```
t.me
pastebin.com
roblox.com
ipwhois.app
ip-api.com
ipinfo.io
geolocation-db.com
api.my-ip.io
my-ip.io
mail.ru
eb.pw
upr.gq
```

## MITRE ATT&CK (11)

| Technique | Name | Tactic | Source |
|---|---|---|---|
| T1027.002 | | | detonation-evidence |
| T1497.001 | | | detonation-evidence |
| T1027 | Obfuscated Files or Information | Defense Evasion | |
| T1055 | Process Injection | Defense Evasion | |
| T1056.001 | Input Capture: Keylogging | Credential Access | |
| T1071.001 | Application Layer Protocol: Web | Command and Control | |
| T1105 | Ingress Tool Transfer | Command and Control | |
| T1486 | Data Encrypted for Impact | Impact | |
| T1489 | Service Stop | Impact | |
| T1496 | Resource Hijacking | Impact | |
| T1555.003 | Credentials from Password Stores | Credential Access | |

## Dynamic Detonation

**Coverage:** ran

**Behavior:** suspicious

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

**Factors:** dropped_exe

### Network Connections (6)

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

### Behavioral Timeline (58)

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 33 more events*

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

### Spawned Processes (50)

```
System
Registry
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
dwm.exe - "dwm.exe"
smss.exe - \SystemRoot\System32\smss.exe
fontdrvhost.ex - "fontdrvhost.exe"
```

```
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv L3V3x8t5wEenv92EVudpYQ.0
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
NVDisplay.Cont - "C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContain
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k NetworkService -p -s Dnscache
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
```

*...and 20 more*