KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_155d1dce8e17.exe

Verdict: MALICIOUS

Verdict: suspicious; 81 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- T1571
- Process Injection
- Input Capture: Keylogging
- Web Service
- Data Encrypted for Impact
- Service Stop
- Credentials from Password Stores: Credentials from Web Browsers
- Scheduled Task/Job: Scheduled Task
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	155d1dce8e17b107b531b80b648f1a3fcbcbed764d76a39b0b3972d9424dd2f7
SHA-1:	ff5db489782f10217946f75450803f6c835108c5
MD5:	0268fde13e99c555ed4a4c6ef193b9ea
Size:	3,425,280 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x3379EE
Sections:	3

Name	Virtual Size	Entropy

.text	0x3359F4	5.84
.rsrc	0xE540	7.35
.reloc	0xC	0.1

Imports

mscoree.dll

_CorExeMain

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
njlO
s]yx
mt8*
j{Um7
AA0V0y
h`4bE
3O);
7i(}
y'E}
>F9U+
?;eK
@, p
xBZB
Xy6/>
Z58b
'\e(8iY
https://github.com/LimerBoy/StormKitty
as."0
0|3Zw
y{DR5
 N#5
@SxB
QVv}
l=nS
C'A34
}tl
p+*l
ek#:Y
L[a2/A?
{#q!
3/f3o3K-11=G-N7VJtozOWRr=(tNZBfK+bS7Fy
t@IU
;&KF!M!h8^iT:<)a?~mXeN*~o?gN[v@rQ=B
yfI{@2
" :)OAN
^B09SH
W%UL
sT.A
```

```
)O%q
%-V
pO r
}A+5
@(,,
o+3*[
|}|y|u|q|m|i|e|a|]|Y|U|Q|M|I|E|A|>|<|:|8|6|4|2|0|.|,|*|(|&|$|"|
 )UU
```

... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
62.60.226.185:6002	network

Indicators of Compromise (10)

URLs (1)

`http://ipinfo.io/ip`

IPv4 addresses (1)

`62.60.226.185`

Domains (8)

`vk.com`
`ok.ru`
`battle.net`
`ipinfo.io`
`assets.msn.com`
`www.bing.com`
`config.edge.skype.com`
`edge-consumer-static.azureedge.net`

MITRE ATT&CK (12)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1571			detonation-evidence
T1055	Process Injection	Defense Evasion	
T1056.001	Input Capture: Keylogging	Credential Access	
T1102	Web Service	Command and Control	
T1486	Data Encrypted for Impact	Impact	
T1489	Service Stop	Impact	
T1555.003	Credentials from Password Stores	Credential Access	
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: suspicious

Threat score: 69/100 (medium)

Factors: c2, evasion, attack_techniques

Network Connections (9)

Destination	Domain	Proto
10.0.2.3:443		tcp
10.0.2.3:80		tcp
10.0.2.3:53		udp
255.255.255.255:67		udp
62.60.226.185:6002		tcp
10.0.2.255:137		udp
224.0.0.252:5355		udp
224.0.0.251:5353		udp
10.0.2.255:138		udp

TLS Handshake Failures (cert-pinning) (50)

```
www.bing.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)
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)
```

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 10.0.2.255:137
5. [conn] pid 0: udp 10.0.2.3:53
6. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
7. [conn] pid 0: tcp 10.0.2.3:80
8. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
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: udp 10.0.2.3:53

14. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
15. [conn] pid 0: tcp 10.0.2.3:443
16. [conn] pid 0: tcp 10.0.2.3:443
17. [conn] pid 0: udp 10.0.2.3:53
18. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
19. [conn] pid 0: tcp 10.0.2.3:80
20. [http] pid 0: GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab
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/disallowedcertstl.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: 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
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
fontdrvhost.ex - "fontdrvhost.exe"
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv +KukEf1oT0+WpSqYqWSlTQ.0
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\Users\Matt.JOHNS-PC\AppData\Local\Temp\tmp8627.tmp.bat""
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
schtasks.exe - schtasks /create /f /sc onlogon /rl highest /tn "Wihnup" /tr '"C:\Users\Matt.JOHNS-PC\AppData\Local\
Wihnup.exe - "C:\Users\Matt.JOHNS-PC\AppData\Local\Temp\Wihnup.exe"
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
identity_helpe - "C:\Program Files (x86)\Microsoft\Edge\Application\146.0.3856.109\identity_helper.exe" --type=utili
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
UserOOBEBroker - C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
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=renderer --pdf-upsell-enabled --v
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=utility --utility-sub-type=networ
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_s
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp

...and 20 more