KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_e64e855c04b0.exe

Verdict: MALICIOUS

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

Analysis Overview

Score: 4/10

Threat level: Malicious

Malicious Activity Summary

- T1027.002
- T1497.001
- T1105
- Obfuscated Files or Information
- Input Capture: Keylogging
- Application Layer Protocol: Web Protocols
- Credentials from Password Stores: Credentials from Web Browsers
- Process Injection
- File and Directory Discovery
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	e64e855c04b00a3e61fe91eee9999817d273a2c4f9fef5cb9f2d3e6e3ff4fb56
SHA-1:	969b0ee6c555222c5831c4f84b6e346e93819e31
MD5:	be3f5461bd6614268faac9e7d68cd746
Size:	320,000 bytes

Packer Detection

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

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x4F5CE
Sections:	3

Name	Virtual Size	Entropy
.text	0x4D5D4	7.3

.rsrc	0x71C	3.85
.reloc	0xC	0.1

Imports

mscoree.dll

_CorExeMain

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rsrc
.reloc
 KDBM(?
?_d
 vT2
f_`X
f`aX
_b`*
prVR
prVR
XjXo
jaU
JjY(
k?e=
vlmX
JjY(
p?!"
JjY(
ZjXs
jY<U
rr;V
rr_V
rr?W
BSJB
v4.0.30319
#Strings
#GUID
#Blob
- 3
*#3
0#3
-%9%
n'~'
UDbD
UY9%
kY9%
EZRZ
_`9%
Jlgl
I=!V
I=!V
```

I=!V

I=!V

I=!V

I=!V

I=!V

I=!V

I=!V

... and 150 more

Indicators of Compromise (9)

URLs (2)

`http://ip-api.com/line/?fields=hosting`

`https://account.dyn.com/`

Domains (7)

`ftp.anmarinee.it.com`

`anmarinee.it.com`

`ip-api.com`

`account.dyn.com`

`privateinternetaccess.com`

`paltalk.com`

`discord.com`

MITRE ATT&CK (10)

Technique	Name	Tactic	Source
T1027.002			detonation-evidence
T1497.001			detonation-evidence
T1105			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
T1056.001	Input Capture: Keylogging	Credential Access	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1555.003	Credentials from Password Stores	Credential Access	
T1055	Process Injection		pt_trace
T1083	File and Directory Discovery		pt_trace
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

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	1192	1111	T1055, T1083	
spoolsv.exe	2512	11	T1055	
svchost.exe	1304	22	T1057	
svchost.exe	756	14	T1083	

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 35/100 (medium)

Factors: dropped_exe, attack_techniques

Network Connections (6)

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

Behavioral Timeline (59)

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

...and 34 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
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
Registry
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
autochk.exe
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c855 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi

NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
services.exe - C:\Windows\system32\services.exe
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
smss.exe - \SystemRoot\System32\smss.exe 00000080 00000084
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv E5IyUg4hFEWt+MV6P8CBIg.0
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
dbInstaller.ex
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
XtuService.exe - C:\Windows\SysWOW64\XtuService.exe
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache

...and 20 more