KVMX

Evidence-First Malware Analysis

Analysis Report: dc31e710277e.bin

Verdict: MALICIOUS

dc31e710277e.bin is a 32-bit executable with 4 sections. Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Application Layer Protocol: Web Protocols

Hashes

SHA-256:	dc31e710277eac1b125de6f4626765a2684d992147691a33964e368e5f269cba
SHA-1:	ec0efbe8fd2fa5300164e9e4eded0d40da549c60
MD5:	b6e148ee1a2a3b460dd2a0adbf1dd39c
Size:	86,016 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x1449E
Sections:	4

Name	Virtual Size	Entropy
.text	0x124A4	6.62
.sdata	0x138	1.43
.rsrc	0x2058	5.9
.reloc	0xC	0.1

Imports

mscoree.dll

_CorExeMain

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.sdata
.rsrc
@.reloc
lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c5
PADPADP
lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c5
PADPADP1:
dlrarhsiva.exe
l=lY
GF#o
 @U*
;\<<P
QX0M
\5h"d
)n(u
`>p{
m=W8s
G21;
_)+]
+jh=v
Tz<L
#yHY
(T#,
\G6r
*R!Y
2zyg
lYrYo
v$L(Z#
Mc%o
>(43
g`<C
#&wpz
a5!z
FGs^:-w
.k(r
z&i'7
a#ZPan
185W
LFf>N
4WX0`
f>OLTH
G4v'
\*a7
ssS4
p"j.
'D>B
B70t
;0N33
```

... and 150 more

Indicators of Compromise (3)

IPv4 addresses (2)

`4.0.0.0`

`1.0.0.0`

Domains (1)

`iii.fff.fff.iii.cc`

MITRE ATT&CK (1)

Technique	Name	Tactic	Source
T1071.001	Application Layer Protocol: Web	Command and Control	