KVMX

Evidence-First Malware Analysis

Analysis Report: 61e6a93f4304.bin

Verdict: MALICIOUS

61e6a93f4304.bin is a 32-bit executable with 3 sections. Packer detected: Unknown packer (high entropy in .text). Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Obfuscated Files or Information
- Application Layer Protocol: Web Protocols
- Dynamic Resolution

Hashes

SHA-256:	61e6a93f43049712b5f2d949fd233fa8015fe4bef01b9e1285d3d87b12f894f2
SHA-1:	1b5f0ac48e06edc4ed8243be61d71077f770f2b4
MD5:	600e0dbaefc03f7bf50abb0def3fb465
Size:	329,216 bytes

Packer Detection

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

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x3CFEE
Sections:	3

Name	Virtual Size	Entropy
.text	0x3AFF4	7.66
.rsrc	0x151C8	2.94
.reloc	0xC	0.1

Imports

mscoree.dll

_CorExeMain

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
*B(*
PAs5
lXsc
lXsc
DU//
!.:u
zzZtk
!XkK0
#/5"J
%.0+
A.J+
i@sc
PAs5
Ylsc
lYsc
I@sc
d[}-
 A(4
 A(4
 A(4
 A(4
HB(4
 A(4
YZY#
ZX(q
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
PADPADP
lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c5
hSystem.Drawing.Bitmap, System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d
QSystem.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
System.Drawing.Bitmap
Data
IHDR
gAMA
 cHRM
IDATx^
bo`/1
*FZ#
Je;d
lFd!JOO
J%3%Bcaaa
AYZM@?
rf5#
/ljj
```

... and 150 more

Indicators of Compromise (5)

IPv4 addresses (3)

`4.0.0.0`

`9.7.6.3`

`8.7.6.2`

Domains (2)

`hn48hn-.in`

`inhhdndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddndddn`

MITRE ATT&CK (3)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1568	Dynamic Resolution	Command and Control	