KVMX

Evidence-First Malware Analysis

Analysis Report: a885b1f5377c.bin

Verdict: MALICIOUS

a885b1f5377c.bin is a 32-bit executable with 3 sections. Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Input Capture: Keylogging
- Application Layer Protocol: Web Protocols
- Credentials from Password Stores: Credentials from Web Browsers

Hashes

SHA-256:	a885b1f5377c2a1cead4e2d7261fab6199f83610ffdd35d20c653d52279d4683
SHA-1:	f7721d590770e2076e64f148a4ba1241404996b8
MD5:	f52fbb02ac0666cae74fc389b1844e98
Size:	307,712 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x4C52E
Sections:	3

Name	Virtual Size	Entropy
.text	0x4A534	5.85
.rsrc	0x686	3.84
.reloc	0xC	0.1

Imports

mscoree.dll

_CorExeMain

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
!`hi
 p~og~am,cazno
 bq r
n un POS,mope.
.tqxt
`.~sro
@:rexoc
?Thus |
osray umnn{t
e ~un,{n,DO_
{de:
`:rs~u
^.rqloo
6BeVB
v@.0:3B?19
#_tru
#YaID
#Nlon
duxe>
UO\Y_RI^Q_RQST_RTMBLQ
P^OG^Ee__C[NTgNUQ
vm~uq__
Patm
co~lin
T{taxB
es`ra
sfqrrqv
_trqa
NytqsT
fe~re
mqth{v
QndUn
inUnv{}e
olpF{xe
rcqFixw
t{zatuondilq
Fule
gFuleZsmq
l|Nw
FixeN
osre
sd{utune
Co|yP~
g~es
tize
tPelqgs
```

... and 150 more

Indicators of Compromise (13)

IPv4 addresses (12)

```
11.11.11.11
1.17.11.11
11.11.17.11
1.11.11.11
11.31.11.11
12.11.11.11
11.01.15.11
11.15.11.11
2.11.51.11
21.11.11.11
1.01.10.11
1.0.0.0
```

Domains (1)

```
neraninkrenineреninere.in
```

MITRE ATT&CK (3)

Technique	Name	Tactic	Source
T1056.001	Input Capture: Keylogging	Credential Access	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1555.003	Credentials from Password Stores	Credential Access	