KVMX

Evidence-First Malware Analysis

Analysis Report: db0d72bc7d10.bin

Verdict: MALICIOUS

db0d72bc7d10.bin is a 32-bit executable with 5 sections. Packer detected: Unknown packer (high entropy in .rdata). Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection
- Application Layer Protocol: Web Protocols
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion

Hashes

SHA-256:	db0d72bc7d10209f7fa354ec100d57abbb9fe2e57ce72789f5f88257c5d3ebd1
SHA-1:	2cdb5fdeee4e9c7bd2e5f744150521963487eb71
MD5:	48d8f7bbb500af66baa765279ce58045
Size:	2,795,520 bytes

Packer Detection

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

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x3AA3
Sections:	5

Name	Virtual Size	Entropy
.text	0xF7FD	6.72
.rdata	0x27DEA8	8.0
.data	0x405D88	1.1
.tls	0x9	0.0

.rsrc	0x163C0	5.75

Imports

KERNEL32.dll

lstrlenA
CommConfigDialogA
HeapAlloc
SetEnvironmentVariableW
FlushViewOfFile
GetTickCount
GetCommConfig
GetPrivateProfileStringW
GetWindowsDirectoryA
GetMailslotInfo

USER32.dll

GetClipCursor

Strings (200 found)

```
!This program cannot be run in DOS mode.
hRich
.text
`.rdata
@.data
.tls
.rsrc
D$0u#j
D$XPj
D$<P
D$PP
D$LPj
l$ )D$
L$$M
8_^]
u?j0
D$DPj
_^[3
h@fi
T$\P
5LSi
ugh4gA
h@fi
h@fi
uFhDgA
h@fi
ualP
h@fi
B,)0
B0)0
V _]
][^Y
?PQS
```

```
N [^
;0v=f
9r8v
9B8s
9C8s
|$ +
|$ +
9G8s
wP+L$
_^][
hdgA
hdgA
hTgA
hTgA
hdgA
Y_^[
5,Vi
```
... and 150 more

Indicators of Compromise (1)

Domains (1)

```
zaa.co
```

MITRE ATT&CK (6)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1129	Shared Modules	Execution	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	