KVMX

Evidence-First Malware Analysis

Analysis Report: wc.bin

Verdict: MALICIOUS

wc.bin is a 32-bit executable with 4 sections. Packer detected: Unknown packer (high entropy in .rsrc). Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Family: ransomware-like
- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection
- Application Layer Protocol: Web Protocols
- Shared Modules
- Deobfuscate/Decode Files or Information
- Data Encrypted for Impact

Hashes

SHA-256:	be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
SHA-1:	120ed9279d85cbfa56e5b7779ffa7162074f7a29
MD5:	5c7fb0927db37372da25f270708103a2
Size:	229,376 bytes

Packer Detection

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

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x6F9A
Sections:	4

Name	Virtual Size	Entropy
.text	0x6190	6.11
.rdata	0x5D06	6.55
.data	0x16AC	4.1

.rsrc	0x27B94	7.99

Imports

KERNEL32.dll

- GetFileSizeEx
- CreateFileA
- InitializeCriticalSection
- DeleteCriticalSection
- GetFileSize
- LeaveCriticalSection
- EnterCriticalSection
- SizeofResource
- LockResource
- LoadResource

USER32.dll

- wsprintfA

ADVAPI32.dll

- CryptDecrypt
- CryptDestroyKey
- CryptReleaseContext
- CryptImportKey
- CryptAcquireContextA

WS2_32.dll

- WSAStartup
- inet_addr
- WSACleanup

MSVCRT.dll

- _controlfp
- __set_app_type
- __p__fmode
- _adjust_fdiv
- __setusermatherr
- _initterm
- __getmainargs
- _acmdln
- exit
- _XcptFilter

Strings (200 found)

```
!This program cannot be run in DOS mode.
Gl^AH1^
Gm^2Gl^
Gl^EAj^
Gl^Rich
.text
`.rdata
@.data
.rsrc
X_^[
X_^[
QPPh
```

```
tXVP
w>WV
X_^]
SjJ3
X[_^
VWj@
SVWj@
>MZt
t'j<j
U$VW
@4+G4t
Yt<V
Yt1V
t29N
t&QW
QSVW
X_^[
K8IV
(f9A
q89p8t
vVSW
V,YYj
V,YYj
tY9V
CC;F
tk9^
t,W3
V,YYG;~
G@F;
vGSW
F,9E
N(9F4
W4VW
;O,u
W4VW
W4VW
9W0t$
W4VW
```

... and 150 more

Malware Config

Family: ransomware-like

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	
T1140	Deobfuscate/Decode Files or Info	Defense Evasion	
T1486	Data Encrypted for Impact	Impact	

Report ID: hVBcHD1upMayfz0eA6nygYwLkArvlnSTJKOpejAJwwQ
Generated by KVMX - kvmx.ai