KVMX

Evidence-First Malware Analysis

Analysis Report: 258f82166d20.bin

Verdict: MALICIOUS

258f82166d20.bin is a 32-bit executable with 3 sections. Packer detected: UPX. Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection
- Shared Modules

Hashes

SHA-256:	258f82166d20c68497a66d82349fc81899fde8fe8c1cc66e59f739a9ea2c95a9
SHA-1:	bed8e439f28a1a0d3876366cbd76a43cdccf60fa
MD5:	5ae700c1dffb00cef492844a4db6cd69
Size:	6,176 bytes

Packer Detection

Packer:	UPX
Confidence:	high

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x71F0
Sections:	3

Name	Virtual Size	Entropy
UPX0	0x5000	0.0
UPX1	0x2000	7.64
UPX2	0x1000	2.64

Imports

KERNEL32.DLL

LoadLibraryA

GetProcAddress

ExitProcess

ADVAPI32.DLL

RegCloseKey

CRTDLL.DLL

atoi

WININET.DLL

InternetGetConnectedState

WS2_32.DLL

send

Strings (105 found)

```
!This program cannot be run in DOS mode.
*|7?
UPX0
UPX1
UPX2
1.22
UPX!
t ;t
t:VU
]^M[
t(x1%Sr
fj]He
j2h<
|hCH
%,1@
=W}$h>
 94(
u<|(1
N%,U
203;
,G"0;0
|@-vr
Xaor
|R[L
Gvx/[G
)db5
]5QD
MIw~f#n#F
?"u#j"
<0E}r
msblast.exe
I ju
 wan
to say LOVE YOU SAN!!
bill
gates&h
d%you make
possiQ
?1[{
one-Wd
```

```
 fix2r]oftireU
H`KG
C2$C
$C2$
0_n#l
"LLb
~'?bB
41Qk
wNtwsupd
.com
```
... and 55 more

MITRE ATT&CK (3)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1129	Shared Modules	Execution	