KVMX

Evidence-First Malware Analysis

Analysis Report: 322eb96fc331.bin

Verdict: MALICIOUS

322eb96fc331.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
- Application Layer Protocol: Web Protocols
- Shared Modules

Hashes

SHA-256:	322eb96fc33119d8ed21b45f1cd57670f74fb42fd8888275ca4879dce1c1511c
SHA-1:	ab03e674b407aecf29c907b39717dec004843b13
MD5:	ea534626d73f9eb0e134de9885054892
Size:	128,512 bytes

Packer Detection

Packer:	UPX
Confidence:	high

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x52360
Sections:	3

Name	Virtual Size	Entropy
UPX0	0x33000	0.0
UPX1	0x1F000	7.92
.rsrc	0x1000	3.3

Imports

KERNEL32.DLL

LoadLibraryA

GetProcAddress

ExitProcess

advapi32.dll

RegCloseKey

comctl32.dll

ImageList_Add

gdi32.dll

SaveDC

ole32.dll

IsEqualGUID

oleaut32.dll

VariantClear

user32.dll

GetDC

Strings (200 found)

```
This program must be run under Win32
UPX0
UPX1
.rsrc
$Info: This file is packed with the UPX executable packer http://upx.tsx.org $
$Id: UPX 1.06 Copyright (C) 1996-2001 the UPX Team. All Rights Reserved. $
UPX!
Boolean
alse
True
Integer
X'Word
String
TObject
m95m
IUnknown
rfaced
 hd`2
PLH
,(S/
u:hD
iZ]_
w^#u
C2w;;tis{
`d^+
.x?~
Q+D-
?ZYY
yeiVX4
S;*\
;57S
3}sL
,|<|
D-3<>|
Tk-I
```

```
Uh~%
l"J1d
y$ S
>#s"
cAqM
}oR~
gmjl
Z; |S
A$Yr
0mic
m'Ey
PRQ[
ZXEfm
t/ix*
uDJt
```
... and 150 more

Indicators of Compromise (2)

URLs (1)

```
http://upx.tsx.org
```

Domains (1)

```
upx.tsx.org
```

MITRE ATT&CK (4)

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	