KVMX

Evidence-First Malware Analysis

Analysis Report: 7a84dd83f4f0.bin

Verdict: MALICIOUS

7a84dd83f4f0.bin is a 32-bit executable with 3 sections. Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Obfuscated Files or Information
- Process Injection
- Input Capture: Keylogging
- Application Layer Protocol: Web Protocols
- Ingress Tool Transfer

Hashes

SHA-256:	7a84dd83f4f00cf0723b76a6a56587bdce6d57bd8024cc9c55565a442806cf69
SHA-1:	a0f4f3a1c5e159b6e2dadaa6615c5e4eb762479f
MD5:	29a37b6532a7acefa7580b826f23f6dd
Size:	32,256 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x954E
Sections:	3

Name	Virtual Size	Entropy
.text	0x7554	5.65
.rsrc	0x240	4.97
.reloc	0xC	0.08

Imports

mscoree.dll

_CorExeMain

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
(%(0
"%(0
"%(0
"%(0
"%(0
"%(0
(%(0
%%(0
(%(0
,`+j
J%(0
,os)
,Os)
"%(0
J%(0
F%(0
;,ar
"%(0
<%(0
3%(0
3%(0
3%(0
.%(0
.%(0
.%(0
"%(0
(%(0
"%(0
"%(0
"%(0
"%(0
"%(0
"%(0
"%(0
"%(0
"%(0
"%(0
"%(0
",?~
"%(0
"%(0
"%(0
"%(0
f%(0
"%(0
 %(0
"%(0
```

... and 150 more

MITRE ATT&CK (5)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1055	Process Injection	Defense Evasion	
T1056.001	Input Capture: Keylogging	Credential Access	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1105	Ingress Tool Transfer	Command and Control	