Basic properties

MD5	9e24b19629a3e35a0fb202a853ce9441
SHA-1	105eecad92634b3d0c2078b67b0fbf4739866562
SHA-256	4eb840617883bf6ed7366242ffee811ad5ea3d5bfd2a589a96d6ee9530690d28
Vhash	115056655d15555048z7f1z27z13z20b1z61z51z96z3
Authentihash	708478d1155b3196cc3c76929a9562a2c398d449afb4a6b9f163e714578f1256
Imphash	0cb4bffd5eba4f2971db3a4369110453
Rich PE header has…	176bd1dfbd8cf2d488bc85a2409b0923
SSDEEP	3072:0Qe2jBmrBnHQrXsjdJ00AegurE3KdQhlMCJoLmOI2I5ctseO:0hiBmNnRdxJgurEadc…
TLSH	T1BB148D177690C07BC177163021AB97719AB9B8316A68DC47F7848E6D6E603D0FB3A3…
File type	Win32 DLL executable windows win32 pe pedll
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (48.8%) | Win64 Executable (generic) (16.4…
File size	190.30 KB (194872 bytes)

History

Creation Time	2014-11-15 04:32:28 UTC
First Submission	2015-12-08 12:36:17 UTC
Last Submission	2022-01-20 15:42:36 UTC
Last Analysis	2022-01-20 15:42:36 UTC

Names

4eb840617883bf6ed7366242ffee811ad5ea3d5bfd2a589a96d6ee9530690d28_unpacked

Signature info

Signature Verification

⚠ A certificate was explicitly revoked by its issuer.

+ Certum Level III CA
+ Certum

X509 Certificates

+ Certum Level III CA
+ Open Source Developer, meicun ge

Portable Executable Info

Compiler Products

id: 150, version: 20413 count=5
[ASM] VS2008 SP1 build 30729 count=22
[C] VS2008 SP1 build 30729 count=134
[C++] VS2008 SP1 build 30729 count=53
[IMP] VS2005 build 50727 count=23
[---] Unmarked objects count=183
id: 138, version: 30729 count=12
[EXP] VS2008 SP1 build 30729 count=1
[LNK] VS2008 SP1 build 30729 count=1

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timest…	2014-11-15 04:32:28 UTC
Entry Point	76430
Contained Sections…	5

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	138030	138240	6.62	3a597617a880eb64a0bdffc5fca6a109	708758.69
.rdata	143360	33227	33280	5.31	54d5ab6610d94bad42949	1005225.25
.data	180224	76128	22280	9728	1.62	70a3e009e4b8cb52c4a25abaccda58d	4634.25

.reloc	204800	9604	9728	5.26	fb67b9e7a8713e45a036afe1c347903c	341006.19

Imports

- imagehlp.dll
- IPHLPAPI.DLL
- WININET.dll
- SHELL32.dll
- KERNEL32.dll
- NETAPI32.dll
- ADVAPI32.dll
- PSAPI.DLL
- SHLWAPI.dll
- WS2_32.dll

Exports

install
installthread
uninstall

Contained Resources By Type

RT_MANIFEST	1

Contained Resources By Language

ENGLISH US	1

Contained Resources

SHA-256	File Type	Type	Language	Entropy	Chi2
[illegible]	[illegible]	[illegible]	[illegible]	4.8	3958.65

filetype	Data
entropy	7.264765739440918
offset	191488
md5	9947ff8ac44c1d51984e1857aa379fe6
size	3384