VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: IDMan.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 2f21b70b732e0d9c691a1bbec763dd7298454f7f
MD5: c65cbc38df2132ac20d333b2cf8a7707
First Seen Date: 2017-01-02 08:07:17 UTC
Number of Clients Seen: 5
Last Analysis Date: 2017-01-02 08:07:17 UTC
Human Expert Analysis Date: 2017-05-22 18:00:30 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2017-01-02 08:07:17 UTC	Clean
Static Analysis Overall Verdict	2017-01-02 08:07:17 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2017-01-02 08:07:17 UTC	No Threat Found
Human Expert Analysis Overall Verdict	2017-05-22 18:00:30 UTC	Clean
File Certificate Validation		Not Applicable

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Clean
Timestamp value suspicious	Clean
Header Checksum is zero!	Clean
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Anti-vm present	Suspicious
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean
TLS callback functions array detected	Clean

Packer detection on signature database

- Armadillo v1.71
- Microsoft Visual C++ v5.0/v6.0 (MFC)
- Microsoft Visual C++

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Creates a child process	
Writes to address space of another process	
Uses a function clandestinely	
Copies itself to startup	
Modifies Windows Service Keys	
Reads memory of another process	
Modifies Windows policies	
Opens a file in a system directory	

Behavioral Information

OpenMutex

Local\MSCTF.Asm.MutexDefault1

QueryFilePath

C:\IDMan.exe
C:\Windows\SysWOW64\regsvr32.exe
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\system32\Connect.dll
C:\Windows\system32\RICHED20.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Windows\system32\propsys.dll
C:\Windows\system32\EhStorShell.dll

LowerChar

.exe
program
file

ReadRegisteryKey

Content Type
Extension
MaxConnectionsNumber
Disable
DataFilePath
Plane1
Plane2
Plane3
Plane4
Plane5
Plane6
Plane7
Plane8

Plane9
Plane10
Plane11
Plane12
Plane13
Plane14
Plane15
Plane16
isUseWinDialUp
mAttempts
mRedialTime
bUseAltKey
bUseControlKey
AppDataIDMFolder
CommonAppDataIDMFolder
LanguageID
scansk
<NULL>
FileName
DateAdded
Queue
Size
Status
Timeleft
TransferRate
LastTry
Description
SaveTo
Referer
Order
ToolbarStyle
LargeButtons
ExceptionServers
Visiblity
AFD
LocalPathW
LocalPath
maxID
evDownloadComplete
evDownloadFailed
evQueueStarted
evQueueFinished
Personal
Address
bUse
iedownl1_v
iedownlAll_v
iedownlFLV_v
iedownl10FLV_v
iedownl1_str
iedownlAll_str
iedownlFLV_str
iedownl10FLV_str
found
DownloadUI
EnableDriver
AdvancedIntegration
FSSettingsChecked
ExceptionProxyServers
ProxyServer
AutoConfigURL
lastintres
mzcc_vers
PendingFileRenameOperations
NeedChAfRb
NeedSnRpAfRb
NoExplorer
path
version
sls_maxSpeed
sls_bTOOst
sls_bShChb
sls_bRemIndEx
bRISF
rshext
CreateUriCacheSize
EnablePunycode
FrameTabWindow

FrameMerging
SessionMerging
AdminTabProcs
TabProcGrowth
DisableSecuritySettingsCheck
SystemSetupInProgress
SpecialFoldersCacheSize
FName
LName
Email
Serial
Extensions
TempPath
FindApps
idmvers
ffdownlFLV_v
ffdownl10FLV_v
LstCheck
LaunchOnStart
IDMan
RememberLastSave
MonitorUrlClipboard
UseHttpProxy
UseFtpProxy
FtpPasive
MData
Model
Therad
FLV
MP3
MP4
M4V
F4V
M4A
MPG
MPEG
AVI
WMV
WMA
WAV
ASF
RM
OGG
OGV
MOV
3GP
QT
WEBM
TS
MKV
AAC
radxcnt
drTbInfo
TrayIcon
isLimitEnabled
m_MBytes
m_hours
showLimitExceededWarning
isStartEnabled
isStopEnabled
isStartDilay
isForceTurnOff
isHangUpModem
isTurnOffComputer
isExitIDMWhenDone
startDaysOfWeek
startTime
startDay
stopTime
startImmediately
StImmMsg
sortOrder
nDESC7
nDESC8
LastCheckQU
Version
ShowDropTarget
bExPnEd

PanelExceptionServers
windowPlacementV6
EnableLUA
RunIEMonitor
vCOUFP
SPChecked
TipStartUp
TipFilePos

CreateRegisteryKey

Software\DownloadManager\
Software\DownloadManager\MCN
Software\DownloadManager\IDMBI
IEXPLORE
Firefox
chrome
OPERA
Safari
Mozilla
SpecialKeys
Software\DownloadManager\menuExt
Software\DownloadManager\Passwords
Software\DownloadManager\ListSettings
Software\DownloadManager\FoldersTree
Software\DownloadManager\maxID
Compressed
Documents
Music
Programs
Video
IDMan.CIDMLinkTransmitter
CLSID
CLSID\{AC746233-E9D3-49CD-862F-068F7B7CCCA4}
LocalServer32
AppID\{AC746233-E9D3-49CD-862F-068F7B7CCCA4}
SOFTWARE\Classes\AppID\{AC746233-E9D3-49CD-862F-068F7B7CCCA4}
Software\DownloadManager\ProxyPac
Software\Microsoft\Internet Explorer\MenuExt\
Download with IDM
Download all links with IDM
Software\Microsoft\Internet Explorer\Low Rights
Software\Microsoft\Internet Explorer\Low Rights\ElevationPolicy
Software\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{E0DACC63-037F-46EE-AC02-E4C7B0FBFEB4}
Software\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{1902485B-CE75-42C1-BA2D-57E660793D9A}
Software\Microsoft\Internet Explorer\Low Rights\DragDrop
Software\Microsoft\Internet Explorer\Low Rights\DragDrop\{19129CDA-AFC0-4330-99BC-C5A834F89006}
Software\Microsoft\Windows\CurrentVersion\Internet Settings
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
{0055C089-8582-441B-A0BF-17B458C2A3A8}
Software\Google
Software\Google\Chrome
Software\Google\Chrome\Extensions
ngpampappnmepgilojfohadhhmbhlaek
http\
https\
ftp\
Software\Mozilla
Software\Classes\CLSID\{D5B91409-A8CA-4973-9A0B-59F713D25671}
Software\Microsoft\Windows\CurrentVersion\Run
Software\Classes\CLSID\{6DDF00DB-1234-46EC-8356-27E7B2051192}
Software\DownloadManager\DwnlPanel
minsize
Software\DownloadManager\ConfigTime
Software\DownloadManager\Scheduler
Software\DownloadManager\Queue

CreateFile

C:\
C:\Windows\Fonts\staticcache.dat
C:\Windows\system32\rsaenh.dll
C:\Users\win7\AppData\Local\Temp\\~DF47F9A5E26656AAB0.TMP

C:\Users\win7\AppData\Roaming\IDM\urlexclist.dat
C:\Users\win7\AppData\Roaming\IDM\defextmap.dat
C:\defexclist.txt
C:\Users\win7\AppData\Roaming\IDM\cnlurllist.dat
C:\Windows\system32\IDManTypeInfo.tlb
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db
C:\Users\desktop.ini
C:\Users
C:\Users\win7
C:\Users\win7\Downloads\desktop.ini
\\.\IDMWFP
C:\IDMGCExt.crx
\\.\IDMTDI
\??\C:\Windows\SysWOW64\ieframe.dll
C:\Windows
C:\Windows\System32
C:\Windows\System32\regsvr32.exe
C:\IDMan.exe
C:\IDMIntegrator64.exe
C:\Users\win7\AppData\Roaming\IDM\Grabber\projects.dat
C:\Users\win7\AppData\Roaming\IDM\Grabber\projects2.dat
C:\Users\win7\AppData\Roaming\IDM\\Scheduler\q_1.dt
C:\Users\win7\AppData\Roaming\IDM\\Scheduler\s_1.dt
C:\Users\win7\AppData\Roaming\IDM\\Scheduler\q_2.dt
C:\Users\win7\AppData\Roaming\IDM\\Scheduler\s_2.dt
\??\C:\Windows\system32\EhStorShell.dll
\??\C:\Windows\system32\ntshrui.dll
\\.\PIPE\srvsvc
C:\Program Files\Internet Explorer\iexplore.exe
C:\tips.txt

OpenRegisteryKey

SOFTWARE\Microsoft\OLEAUT
Software\Microsoft\Windows\CurrentVersion\Setup
Software\Microsoft\Windows\CurrentVersion
system\CurrentControlSet\control\NetworkProvider\HwOrder
SOFTWARE\Classes
.386
.a
.ai
.aif
.aifc
.aiff
.ani
.ans
.application
.appref-ms
.aps
.art
.asa
.asc
.ascx
.asf
.asm
.asmx
.asp
.aspx
.asx
.au
.avi
.bas
.bat
.bcp
.bin
.bkf
.blg
.bmp
.bsc
.c
.cab
.camp
.cat
.cc

.cda
.cdmp
.cdx
.cer
.cgm
.chk
.chm
.cls
.cmd
.cod
.com
.compositefont
.contact
.cpl
.cpp
.crd
.crds
.crl
.crt
.cs
.csa
.csproj
.css
.csv
.cur
.cxx
.dat
.db
.dbg
.dbs
.dct
.def
.der
.desklink
.diagcab
.diagcfg
.diagpkg
.dib
.dic
.diz
.dll
.dl_
.doc
.docx
.dos
.dot
.drv
.dsn
.dsp
.dsw
.dwfx
.easmx
.edrwx
.emf
.eprtx
.eps
.etp
.evt
.evtx
.exe
.exp
.ext
.ex_
.eyb
.faq
.fif
.fky
.fnd
.fnt
.fon
.gadget
.ghi
.gif
.gmmp
.group
.grp
.gz
.h

.H1C
.H1D
.H1F
.H1H
.H1K
.H1Q
.H1S
.H1T
.H1V
.H1W
.hdp
.hhc
.hlp
.hpp
.hqx
.hta
.htc
.htm
.html
.htt
.htw
.htx
.hxx
.i
.ibq
.icc
.icl
.icm
.ico
.ics
.idl
.idq
.ilk
.imc
.img
.inc
.inf
.ini
.inl
.inv
.inx
.in_
.iso
.IVF
.jav
.java
.jbf
.jfif
.jnt
.Job
.jod
.jpe
.jpeg
.jpg
.js
.JSE
.jtp
.jtx
.jxr
.kci
.label
.latex
.lgn
.lib
.library-ms
.lnk
.local
.log
.lst
.m14
.m1v
.m3u
.m4a
.mak
.man
.manifest
.mapimail
.mht

.mhtml
.mid
.midi
.mig
.mk
.mlc
.mmf
.mov
.movie
.mp2
.mp2v
.mp3
.mpa
.mpe
.mpeg
.mpg
.mpv2
.msc
.msg
.msi
.msp
.msrcincident
.msstyles
.msu
.mv
.mydocs
.ncb
.nfo
.nls
.nvr
.obj
.ocx
.oc_
.odc
.odh
.odl
.odt
.osdx
.otf
.p10
.p12
.p7b
.p7c
.p7m
.p7r
.p7s
.partial
.pbk
.pch
.pdb
.pds
.perfmoncfg
.pfm
.pfx
.php3
.pic
.pif
.pko
.pl
.plg
.pma
.pmc
.pml
.pmr
.pnf
.png
.pot
.pps
.ppt
.prc
.prf
.printerExport
.ps
.ps1
.ps1xml
.psc1
.psd
.psd1

.psm1
.py
.pyc
.pyo
.pyw
.qds
.rat
.rc
.rc2
.rct
.RDP
.reg
.res
.resmoncfg
.rgs
.rle
.rll
.rmi
.rpc
.rsp
.rtf
.rul
.s
.sbr
.sc2
.scc
.scd
.scf
.sch
.scp
.scr
.sct
.search-ms
.searchConnector-ms
.sed
.sfcache
.shtm
.shtml
.sit
.slupkg-ms
.snd
.sol
.sor
.spc
.sql
.srf
.sr_
.sst
.stl
.stm
.svg
.swf
.sym
.sys
.sy_
.tab
.tar
.tdl
.text
.tgz
.theme
.themepack
.tif
.tiff
.tlb
.tlh
.tli
.trg
.tsp
.tsv
.ttc
.ttf
.txt
.udf
.UDL
.udt
.URL
.user

.usr
.VBE
.vbproj
.vbs
.vbx
.vcf
.vcproj
.viw
.vspscc
.vsscc
.vssscc
.vxd
.wab
.wav
.wax
.wbcat
.wcx
.wdp
.webpnp
.website
.wll
.wlt
.wm
.wma
.wmf
.wmp
.wmv
.wmx
.wmz
.wpl
.wri
.wsc
.WSF
.WSH
.wsz
.wtx
.wvx
.x
.xaml
.xbap
.xht
.xhtml
.xix
.xlb
.xlc
.xls
.xlt
.xml
.xps
.xrm-ms
.xsd
.xsl
.xslt
.z
.z96
.zfsendtotarget
.zip
MIME\Database\Content Type
application/atom+xml
application/fractals
application/hta
application/mac-binhex40
application/opensearchdescription+xml
application/pkcs10
application/pkcs7-mime
application/pkcs7-signature
application/pkix-cert
application/pkix-crl
application/postscript
application/rss+xml
application/vnd.ms-pki.certstore
application/vnd.ms-pki.pko
application/vnd.ms-pki.seccat
application/vnd.ms-pki.stl
application/vnd.ms-xpsdocument
application/x-complus
application/x-compress
application/x-compressed

application/x-gzip
application/x-informationCard
application/x-jtx+xps
application/x-latex
application/x-mix-transfer
application/x-ms-application
application/x-ms-license
application/x-ms-xbap
application/x-mswebsite
application/x-pkcs12
application/x-pkcs7-certificates
application/x-pkcs7-certreqresp
application/x-stuffit
application/x-tar
application/x-troff-man
application/x-x509-ca-cert
application/x-zip-compressed
application/xaml+xml
application/xhtml+xml
application/xml
audio/mp3
audio/x-ms-wma
image/bmp
image/gif
image/jpeg
image/pjpeg
image/png
image/svg+xml
image/tiff
image/vnd.ms-dds
image/vnd.ms-photo
image/x-emf
image/x-icon
image/x-jg
image/x-png
image/x-wmf
message/rfc822
model/vnd.dwfx+xps
model/vnd.easmx+xps
model/vnd.edrwx+xps
model/vnd.eprtx+xps
pkcs10
pkcs7-mime
pkcs7-signature
pkix-cert
pkix-crl
text/css
text/html
text/plain
text/scriptlet
text/x-component
text/x-ms-contact
text/x-scriptlet
text/x-vcard
text/xml
video/mpeg
video/x-mpeg
video/x-ms-asf
video/x-msvideo
vnd.ms-pki.certstore
vnd.ms-pki.pko
vnd.ms-pki.seccat
vnd.ms-pki.stl
x-pkcs12
x-pkcs7-certificates
x-pkcs7-certreqresp
x-x509-ca-cert
Software\DownloadManager\
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
Tahoma
SpecialKeys
Software\Classes\CLSID\{7B8E9164-324D-4A2E-A46D-0165FB2000EC}
Software\Classes\CLSID\{5ED60779-4DE2-4E07-B862-974CA4FF2E9C}
Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
Software\Microsoft\Internet Explorer\MenuExt\
Firefox

firefox
Opera
seamonkey
orca
Software\Microsoft\Internet Explorer
Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
SOFTWARE\Internet Download Manager
SYSTEM\CurrentControlSet\Services\IDMWFP
Software\Mozilla\Mozilla Firefox
Software\mozilla.org\Mozilla Firefox
SOFTWARE\mozilla.org\Mozilla
SOFTWARE\Netscape\Netscape
SOFTWARE\Netscape\Netscape 6
SOFTWARE\Netscape\Netscape Browser
SOFTWARE\Mozilla\Netscape Navigator
SOFTWARE\Mozilla\SeaMonkey
Software\Flock\Flock
Software\Opera Software
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
SOFTWARE\Google\Chrome\Extensions\ngpampappnmepgilojfohadhhmbhlaek
SOFTWARE\Google\Chrome\Extensions\jmolcgpienlcieaajfkkdamlngancncm
SOFTWARE\Google\Chrome\Extensions\jeaohhlajejodfjadcponpnjgkiikocn
Software\Google\Chrome\Extensions
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome
Software\Mozilla\Aurora
Software\Mozilla\Mozilla Firefox ESR
Software\Mozilla\Waterfox
Software\Mozilla\Firefox\Extensions
SYSTEM\CurrentControlSet\Control\Session Manager
Software\Classes\PROTOCOLS\Name-Space Handler\
{0055C089-8582-441B-A0BF-17B458C2A3A8}
Software\Mozilla
SOFTWARE\FullCircle\TalkBack
SYSTEM\CurrentControlSet\Services\IDMTDI
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
Software\Microsoft\Internet Explorer\Main\FeatureControl
FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap
FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915
FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001
Software\Policies
Software
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Software\Microsoft\Internet Explorer\Main
Software\Policies\Microsoft\Internet Explorer\Main
FEATURE_INITIALIZE_URLACTION_SHELLEXECUTE_TO_ALLOW_KB936610
Software\Policies\Microsoft\Internet Explorer
Microsoft\Internet Explorer\Security
System\Setup
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
FEATURE_LOCALMACHINE_LOCKDOWN
FEATURE_ZONES_DEFAULT_DRIVE_INTRANET_KB941000
FEATURE_PROTOCOL_LOCKDOWN
Software\Classes\CLSID\{6DDF00DB-1234-46EC-8356-27E7B2051192}
minsize
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
System
Marlett
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EE5B8E34-973C-4FBE-AC83-99F064009FC7}
CLSID\{CDC95B92-E27C-4745-A8C5-64A52A78855D}\InProcServer32

CreateMutex

<NULL>
RasPbFile
Tonec_Internet_Download_Manager_MTX
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Local\IDMEventMonitor

CreateProcess

"C:\Windows\System32\regsvr32.exe" /s "C:\IDMShellExt64.dll"
"C:\Program Files\Internet Explorer\iexplore.exe" http://www.internetdownloadmanager.com/welcome.html?v=627b2
"C:\Windows\System32\regsvr32.exe" /s "C:\IDMIECC64.dll"
"C:\Windows\System32\regsvr32.exe" /s "C:\IDMGetAll64.dll"
"C:\Windows\System32\regsvr32.exe" /s "C:\downlWithIDM64.dll"

LoadLibrary

API-MS-Win-Core-LocalRegistry-L1-1-0.dll
C:\IDMIECC64.dll
shell32
ADVAPI32.dll
comctl32.dll
ole32.dll
C:\idmvs.dll
UxTheme.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL
Connect.dll
RASAPI32
shlwapi.dll
RichEd32.Dll
CRYPTBASE.dll
C:\Windows\system32\asycfilt.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
IDMGetAll.dll
IDMIECC.dll
downlWithIDM.dll
idmfsa.dll
propsys.dll
ntmarta.dll
SHELL32.dll
imageres.dll
PSAPI.DLL
Kernel32.DLL
WS2_32
C:\Windows\SysWOW64\ieframe.dll
kernel32.dll
Secur32.dll
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
OLEAUT32.dll
C:\Windows\system32\sfc.dll
COMCTL32.DLL
IMM32.dll
WindowsCodecs.dll
C:\Windows\system32\EhStorShell.dll
C:\Windows\system32\ntshrui.dll
srvcli.dll
cscapi.dll
slc.dll
c:\windows\system32\imageres.dll
SspiCli.dll

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2017-05-22 15:34:24 UTC
Analysis End Date: 2017-05-22 18:00:30 UTC
File Upload Date: 2017-01-02 08:07:44 UTC
Human Expert Analyst Feedback: None

Verdict: Clean

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x58524761 [Thu Dec 15 07:33:53 2016 UTC]
Entry Point	0x5dfe4f (.text)
File Size	4001848
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	Tonec Inc., Copyright \xa9 1999 - 2016
Internal Name	Internet Download Manager
File Version	6, 27, 2, 2
Company Name	Tonec Inc.
Private Build	
Legal Trademarks	Internet Download Manager
Comments	http://www.internetdownloadmanager.com
Product Name	Internet Download Manager (IDM)
Special Build	
Product Version	6, 27, 2, 2
File Description	Internet Download Manager (IDM)
Original Filename	IDMan.exe
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	dd96595220be02458955469df663c8e7f02e608b18b5e7a89567d90c2012cc88

File Paths

FILE PATH ON CLIENT	SEEN COUNT
2f21b70b732e0d9c691a1bbec763dd7298454f7f	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2260ba	0x227000	6.620550	-
.rdata	0x228000	0x902c6	0x91000	4.591242	-
.data	0x2b9000	0x36808	0x31000	5.463836	-
.rsrc	0x2f0000	0xe7000	0xe7000	5.924575	-