VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: ZAMShellExt64.dll
File Type: PE32+ executable (DLL) (GUI) x86-64, for MS Windows
SHA1: 0e7e15015d2dcbff1e02e16bece30f1525e3163d
MD5: 9e637cb9353c62c8019d20bd1a9491ff
First Seen Date: 2017-01-20 13:30:07 UTC
Number of Clients Seen: 8
Last Analysis Date: 2017-01-20 13:30:07 UTC
Human Expert Analysis Date: 2017-01-20 17:58:00 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-01-20 13:30:07 UTC	Clean	
Static Analysis Overall Verdict	2017-01-20 13:30:07 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2017-01-20 13:30:07 UTC	No Threat Found	
Human Expert Analysis Overall Verdict	2017-01-20 17:58:00 UTC	Clean	
File Certificate Validation		Certificate and Vendor name are Valid	

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	Suspicious	
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	

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS
Has no visible windows

Behavioral Information

QueryFilePath

C:\DLL_Loader.exe

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2017-01-20 15:42:45 UTC
Analysis End Date: 2017-01-20 17:58:00 UTC
File Upload Date: 2017-01-20 13:31:41 UTC
Human Expert Analyst Feedback: None
Verdict: Clean

Additional File Information

Vendor Validation - Verified ✔

[+] Zemana Ltd.

Status	Valid ✔

Certificate Validation - Success ✔

[+] Zemana Ltd.

Status	NoError ✔
Start Date	2014-12-16 00:00:00+00:00
End Date	2017-12-20 12:00:00+00:00
Sha256	ca93a53867810f5e45c6eab5330a7910651872bdd88e8a71fb19dc17c717da71
Serial	0210230FD364B469091B8A4440145E18
Subject Name	Zemana Ltd.
Subject Key Identifier	b2 6c 79 56 d1 06 d8 35 f3 8e b7 5b 1f 63 f5 fc 1f d5 a4 90
Subject Organization	Zemana Ltd.
Subject Locality	Edirne
Subject Country	TR
Issuer Name	DigiCert High Assurance Code Signing CA-1
Issuer Key Identifier	97 48 03 eb 15 08 6b b9 b2 58 23 cc 94 2e f1 c6 65 d2 64 8e
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	http://crl3.digicert.com/ha-cs-2011a.crl,http://crl4.digicert.com/ha-cs-2011a.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] DigiCert High Assurance Code Signing CA-1

Status	NoError ✔
Start Date	2011-02-11 12:00:00+00:00
End Date	2026-02-10 12:00:00+00:00
Sha256	81e137d4348615d2a93388ef9befe004dac1aff661f3e490727b383d3bbb1d2e
Serial	02C4D1E58A4A680C568DA3047E7E4D5F
Subject Name	DigiCert High Assurance Code Signing CA-1
Subject Key Identifier	97 48 03 eb 15 08 6b b9 b2 58 23 cc 94 2e f1 c6 65 d2 64 8e
Subject Organization	DigiCert Inc
Subject Country	US
Subject Organizational Unit	www.digicert.com
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl,http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] DigiCert High Assurance EV Root CA

Status	NoError ✔
Start Date	2006-11-10 00:00:00+00:00
End Date	2031-11-10 00:00:00+00:00
Sha256	ed960860d0e06c89fa3ff7723437b6812c6d7e1ad370c7885b1251d2e1c2a938
Serial	02AC5C266A0B409B8F0B79F2AE462577
Subject Name	DigiCert High Assurance EV Root CA
Subject Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Subject Organization	DigiCert Inc
Subject Country	US
Subject Organizational Unit	www.digicert.com
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	undefined
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

[+] Symantec Time Stamping Services CA - G2

Status	NoError ✔
Start Date	2012-12-21 00:00:00+00:00
End Date	2020-12-30 23:59:59+00:00
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Name	Symantec Time Stamping Services CA - G2
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Subject Organization	Symantec Corporation
Subject Country	US
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

[+] Thawte Timestamping CA

Status	NoError ✔
Start Date	1997-01-01 00:00:00+00:00
End Date	2020-12-31 23:59:59+00:00
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Name	Thawte Timestamping CA
Subject Key Identifier	undefined
Subject Organization	Thawte
Subject Locality	Durbanville
Subject State	Western Cape
Subject Country	ZA
Subject Organizational Unit	Thawte Certification
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x57ECFDD8 [Thu Sep 29 11:41:12 2016 UTC]
Entry Point	0x1800034d4 (.text)
File Size	152944
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Legal Copyright	Copyright \xa9 2007 - 2015 Zemana Ltd.
Internal Name	ZemanaShell
File Version	1.0
Company Name	Zemana Ltd.
Legal Trademarks	
Product Name	Zemana AntiMalware
Product Version	2.0
File Description	Zemana AntiMalware
Original Filename	ZemanaShell
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	7
Sha256	646d42b24f09b27206c03ca3d73a9148478ea8b1554af50f3696883f9cdcf4c0

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x13220	0x13400	6.426514	-
.rdata	0x15000	0xb058	0xb200	4.956179	-
.data	0x21000	0x1ef0	0xc00	2.463496	-
.pdata	0x23000	0x13d4	0x1400	5.007366	-
.gfids	0x25000	0xc0	0x200	1.530467	-
.rsrc	0x26000	0x2780	0x2800	5.823270	-
.reloc	0x29000	0x674	0x800	4.898535	-

PE Imports

KERNEL32.dll

- CreateProcessW
- WideCharToMultiByte
- CloseHandle
- FlushFileBuffers
- SetFilePointerEx
- GetConsoleMode
- GetConsoleCP
- WriteFile
- HeapReAlloc
- HeapSize
- GetLastError
- GetVersionExW
- GetModuleFileNameW
- GetShortPathNameW
- ExpandEnvironmentStringsW
- FreeLibrary
- lstrlenW
- GetProcessHeap
- GetProcAddress
- HeapAlloc
- LoadLibraryW
- WriteConsoleW
- HeapFree
- SetStdHandle
- FreeEnvironmentStringsW
- GetEnvironmentStringsW
- GetCommandLineW
- RtlCaptureContext

- RtlLookupFunctionEntry
- RtlVirtualUnwind
- UnhandledExceptionFilter
- SetUnhandledExceptionFilter
- GetCurrentProcess
- TerminateProcess
- IsProcessorFeaturePresent
- QueryPerformanceCounter
- GetCurrentProcessId
- GetCurrentThreadId
- GetSystemTimeAsFileTime
- InitializeSListHead
- IsDebuggerPresent
- GetStartupInfoW
- GetModuleHandleW
- RtlPcToFileHeader
- EncodePointer
- RaiseException
- RtlUnwindEx
- InterlockedFlushSList
- SetLastError
- EnterCriticalSection
- LeaveCriticalSection
- DeleteCriticalSection
- InitializeCriticalSectionAndSpinCount
- TlsAlloc
- TlsGetValue
- TlsSetValue
- TlsFree
- LoadLibraryExW
- ExitProcess
- GetModuleHandleExW
- GetModuleFileNameA
- MultiByteToWideChar
- GetACP
- GetStdHandle
- GetFileType

- GetStringTypeW
- LCMapStringW
- FindClose
- FindFirstFileExA
- FindNextFileA
- IsValidCodePage
- GetOEMCP
- GetCPInfo
- GetCommandLineA
- CreateFileW

- USER32.dll
  - LoadImageW
  - MessageBoxW
  - SetMenuItemInfoW
  - DrawIconEx
  - InsertMenuW
  - SetMenuInfo
  - GetIconInfo
  - DestroyIcon
  - SetRect
- GDI32.dll
  - CreateDIBSection
  - CreateCompatibleDC
  - GetDIBits
  - DeleteDC
  - DeleteObject
  - SelectObject
- ADVAPI32.dll
  - RegCreateKeyExW
  - RegSetValueExW
  - RegOpenKeyExW
  - RegQueryValueExW
  - RegCloseKey
- SHELL32.dll
  - DragQueryFileW
- ole32.dll

ReleaseStgMedium

StringFromGUID2

SHLWAPI.dll

SHDeleteKeyW

PE Exports

DllCanUnloadNow

DllGetClassObject

DllRegisterServer

DllUnregisterServer

PE Resources

RT_ICON
RT_GROUP_ICON
RT_VERSION
RT_MANIFEST