VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: crashrpt.dll
File Type: PE32+ executable (DLL) (GUI) x86-64, for MS Windows
SHA1: 5ba1fb696a714667d6efd65988add7b20a52e014
MD5: 98ef91ba46db8109d27b0d1447b03d9c
First Seen Date: 2016-05-22 05:04:47 UTC
Number of Clients Seen: 8
Last Analysis Date: 2017-04-10 06:31:28 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-04-10 06:31:28 UTC	Clean	
Static Analysis Overall Verdict	2017-04-10 06:31:28 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2017-04-10 06:31:28 UTC	No Threat Found	
Precise Detectors Overall Verdict	2017-04-10 06:31:28 UTC	No Match	
File Certificate Validation		Vendor not found in Trusted List	

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	Clean	
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	
Operation successfully finished.	

Behavioral Information

QueryFilePath

C:\DLL_Loader.exe

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2017-04-10 06:31:29 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Not Verified ✖

[+] ООО "ИДЕАЛЬНЫЙ СОФТ" - Ideal Soft LLC

Status	Not Valid ✖

[+] ООО "ИДЕАЛЬНЫЙ СОФТ" - Ideal Soft LLC

Status	Valid ✔

Certificate Validation - Success ✔

[+] Thawte Timestamping CA

Status	NoError ✔
Start Date	1997-01-01 00:00:00
End Date	2020-12-31 23:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Name	Thawte Timestamping CA
Subject Key Identifier	null
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Crl link	null
Key Usage	null
Extended Usage	null

[+] Symantec Time Stamping Services CA - G2

Status	NoError ✔
Start Date	2012-12-21 00:00:00
End Date	2020-12-30 23:59:59
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
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
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)"}

[+] StartCom Certification Authority

Status	NoError ✔
Start Date	2006-09-17 19:46:36
End Date	2036-09-17 19:46:36
Sha256	97d91552a5ea090a20b1164933f4afdd2876a1e4585a2d7adf974d3cb2e070f4
Serial	01
Subject Name	StartCom Certification Authority
Subject Key Identifier	4e 0b ef 1a a4 40 5b a5 17 69 87 30 ca 34 68 43 d0 41 ae f2
Issuer Name	StartCom Certification Authority
Issuer Key Identifier	null
Crl link	http://cert.startcom.org/sfsca-crl.crl,http://crl.startcom.org/sfsca-crl.crl
Key Usage	{"Digital Signature","Key Encipherment","Key Agreement","Certificate Signing","Off-line CRL Signing","CRL Signing (ae)"}
Extended Usage	null

[+] ООО ”ИДЕАЛЬНЫЙ СОФТ” - Ideal Soft LLC

Status	NoError ✔
Start Date	2014-09-24 03:43:58
End Date	2016-09-24 16:47:44
Sha256	bde840b087dd253fc149ac059496c9c8edd7138f7247f7cccec6307026214ec7
Serial	103C
Subject Name	ООО ”ИДЕАЛЬНЫЙ СОФТ” - Ideal Soft LLC
Subject Key Identifier	10 3a c0 bd 66 be e9 20 10 83 dc a5 05 ab 0f 64 81 ad c1 24
Issuer Name	StartCom Class 2 Primary Intermediate Object CA
Issuer Key Identifier	d0 4e 0f 40 99 6c b8 4b 19 6f 3b 28 b8 e0 e3 88 07 34 aa b7
Crl link	http://crl.startssl.com/crtc2-crl.crl
Key Usage	{"Digital Signature (80)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

[+] StartCom Class 2 Primary Intermediate Object CA

Status	NoError ✔
Start Date	2007-10-14 22:01:46
End Date	2022-10-14 22:01:46
Sha256	b5e11bf30f0a824e9b45059065118ea1e5d912df5f205bf0a2fcce11dfdd8e2b
Serial	1000F5EBE03943
Subject Name	StartCom Class 2 Primary Intermediate Object CA
Subject Key Identifier	d0 4e 0f 40 99 6c b8 4b 19 6f 3b 28 b8 e0 e3 88 07 34 aa b7
Issuer Name	StartCom Certification Authority
Issuer Key Identifier	4e 0b ef 1a a4 40 5b a5 17 69 87 30 ca 34 68 43 d0 41 ae f2
Crl link	http://crl.startssl.com/sfsca.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x55611EAD [Sun May 24 00:43:25 2015 UTC]
Entry Point	0x180008620 (.text)
File Size	124456
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Legal Copyright	Copyright (C) Idol Software 2014
Internal Name	crashrpt
File Version	2.0.17.0
Company Name	Idol Software
Product Name	Doctor Dump
Product Version	2.0.17.0
File Description	Crash reporting library
Original Filename	crashrpt.exe
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	c0ca65d7406288150322232795 2df11c1ea82c78ea4dbd5e5bd9e88e220be405

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C:\Program Files\MPC-HC\CrashReporter\crashrpt.dll	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x132c6	0x13400	6.370989	-
.rdata	0x15000	0x5c68	0x5e00	4.685627	-
.data	0x1b000	0x39b8	0x1600	2.231481	-
.pdata	0x1f000	0x10d4	0x1200	4.779147	-
.rsrc	0x21000	0x4f0	0x600	4.508777	-
.reloc	0x22000	0x50a	0x600	3.153111	-

PE Imports

- VERSION.dll
  - VerQueryValueW
  - GetFileVersionInfoW
  - GetFileVersionInfoSizeW
- KERNEL32.dll
  - HeapDestroy
  - FlushFileBuffers
  - WriteConsoleW
  - SetStdHandle
  - RemoveVectoredExceptionHandler
  - RaiseException
  - LoadLibraryW
  - GetProcAddress
  - AddVectoredExceptionHandler
  - CloseHandle
  - CreateEventW
  - InitializeCriticalSection
  - DeleteCriticalSection
  - EnterCriticalSection
  - LeaveCriticalSection
  - FindResourceW
  - LoadResource
  - CreateFileW
  - GetLastError
  - WriteFile
  - SizeofResource
  - LockResource
  - DuplicateHandle
  - GetCurrentProcess
  - SetHandleInformation
  - GetCurrentProcessId
  - CreateProcessW
  - WaitForMultipleObjects
  - OutputDebugStringA
  - IsDebuggerPresent
  - GetCurrentThreadId
  - CreateThread

- WaitForSingleObject
- GetExitCodeThread
- ExitProcess
- GetModuleHandleW
- VirtualProtect
- TlsGetValue
- TlsSetValue
- GetModuleFileNameW
- ExpandEnvironmentStringsW
- SetUnhandledExceptionFilter
- SetLastError
- HeapAlloc
- GetProcessHeap
- HeapFree
- TlsAlloc
- TlsFree
- MultiByteToWideChar
- lstrlenA
- FindResourceExW
- GetConsoleMode
- GetConsoleCP
- SetFilePointer
- HeapReAlloc
- HeapSize
- InitializeCriticalSectionAndSpinCount
- EncodePointer
- DecodePointer
- GetFileAttributesW
- FlsSetValue
- GetCommandLineA
- RtlPcToFileHeader
- TerminateProcess
- UnhandledExceptionFilter
- RtlVirtualUnwind
- RtlLookupFunctionEntry
- RtlCaptureContext
- Sleep

- RtlUnwindEx
- GetCPInfo
- GetACP
- GetOEMCP
- IsValidCodePage
- FlsGetValue
- FlsFree
- FlsAlloc
- LCMapStringW
- HeapSetInformation
- GetVersion
- HeapCreate
- SetHandleCount
- GetStdHandle
- GetFileType
- GetStartupInfoW
- GetModuleFileNameA
- FreeEnvironmentStringsW
- WideCharToMultiByte
- GetEnvironmentStringsW
- QueryPerformanceCounter
- GetTickCount
- GetSystemTimeAsFileTime
- GetStringTypeW

USER32.dll

- MessageBoxA
- DisableProcessWindowsGhosting

PE Exports

- AddFileToReport
- AddUserInfoToReport
- GetVersionFromApp
- GetVersionFromFile
- InitCrashRpt
- IsReadyToExit
- RemoveFileFromReport
- RemoveUserInfoFromReport
- SendReport
- SetCustomInfo

PE Resources

RT_VERSION
RT_MANIFEST