VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: tbbmalloc.dll
File Type: PE32+ executable (DLL) (GUI) x86-64, for MS Windows
SHA1: 67fe188474ec06dd5fe8d15504b0f5e8aa25582a
MD5: 189922f0a1750e13fc5b88e03aae1f8b
First Seen Date: 2016-02-01 18:08:18 UTC
Number of Clients Seen: 13
Last Analysis Date: 2017-01-09 19:12:27 UTC
Human Expert Analysis Date: 2017-01-28 10:13:37 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-01-09 19:12:27 UTC	Clean	
Static Analysis Overall Verdict	2017-01-09 19:12:27 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2017-01-09 19:12:27 UTC	No Threat Found	
Human Expert Analysis Overall Verdict	2017-01-28 10:13:37 UTC	Clean	
File Certificate Validation		Certificate Not Valid,Vendor name 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	
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	
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	
Packer detection on signature database	Unknown	
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	

Anti-debug calls

IsDebuggerPresent

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: 2017-01-25 14:19:54 UTC
Analysis End Date: 2017-01-28 10:13:37 UTC
File Upload Date: 2017-01-25 14:14:54 UTC
Human Expert Analyst Feedback: Safe
Verdict: Clean

Additional File Information

Vendor Validation - Verified ✔

[+] Intel(R) Software Products

Status	Valid ✔

Certificate Validation - SignatureOrFileCorrupt ✖

[+] Intel(R) Software Products

Status	NotTimeValid ✖
Start Date	2011-12-12 18:40:34+00:00
End Date	2014-11-26 18:40:34+00:00
Sha256	6d54e6dbd6f5365b9f4df8601e74999478f97463c46ce391d4cf664e543955c3
Serial	1BAAC3A2000100007976
Subject Name	Intel(R) Software Products
Subject Key Identifier	cf 22 c7 ac 0d 12 db 4e 61 98 48 4c dd 31 62 cb 1d 04 9d 92
Issuer Name	Intel External Basic Issuing CA 3A
Issuer Key Identifier	aa 16 66 af b7 3d 56 53 60 ae 0d c2 ed f3 ee 07 cb 51 60 7e
Issuer Organization	Intel Corporation
Issuer Country	US
Crl link	http://www.intel.com/repository/CRL/Intel%20External%20Basic%20Issuing%20CA%203A(1).crl,http://certificates.intel.com/reposit
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] Intel External Basic Issuing CA 3A

Status	NotTimeValid ✖
Start Date	2009-05-15 19:25:13+00:00
End Date	2015-05-15 19:35:13+00:00
Sha256	423bca67d748af940b620d84c5cc25fb555d212e5e49b2bc5b20a81fc9988328
Serial	611E80B7000000000007
Subject Name	Intel External Basic Issuing CA 3A
Subject Key Identifier	aa 16 66 af b7 3d 56 53 60 ae 0d c2 ed f3 ee 07 cb 51 60 7e
Subject Organization	Intel Corporation
Subject Country	US
Issuer Name	Intel External Basic Policy CA
Issuer Key Identifier	1a c6 0c 4a c4 47 6f a8 db ad 2b f0 f4 56 06 a3 ed 37 54 0c
Issuer Organization	Intel Corporation
Issuer Country	US
Crl link	http://www.intel.com/repository/CRL/Intel%20External%20Basic%20Policy%20CA.crl,http://certificates.intel.com/repository/CRL/Int
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

[+] Intel External Basic Policy CA

Status	NotTimeValid ✖
Start Date	2006-02-16 18:01:30+00:00
End Date	2016-02-19 18:01:30+00:00
Sha256	732f4c0b21add69052db88d7810c948fefdc7c51fa781686f43edac7bfd38d42
Serial	05B0FF
Subject Name	Intel External Basic Policy CA
Subject Key Identifier	1a c6 0c 4a c4 47 6f a8 db ad 2b f0 f4 56 06 a3 ed 37 54 0c
Subject Organization	Intel Corporation
Subject Country	US
Issuer Name	null
Issuer Key Identifier	48 e6 68 f9 2b d2 b2 95 d7 47 d8 23 20 10 4f 33 98 90 9f d4
Issuer Organization	Equifax
Issuer Country	US
Issuer Organizational Unit	Equifax Secure Certificate Authority
Crl link	http://crl.geotrust.com/crls/secureca.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] null

Status	NoError ✔
Start Date	1998-08-22 16:41:51+00:00
End Date	2018-08-22 16:41:51+00:00
Sha256	0ed83aaa143fbdb5b03bcbd40d31e84401ec0e52ed3c24bace49243a0601b9aa
Serial	35DEF4CF
Subject Key Identifier	48 e6 68 f9 2b d2 b2 95 d7 47 d8 23 20 10 4f 33 98 90 9f d4
Subject Organization	Equifax
Subject Country	US
Subject Organizational Unit	Equifax Secure Certificate Authority
Issuer Name	null
Issuer Key Identifier	48 e6 68 f9 2b d2 b2 95 d7 47 d8 23 20 10 4f 33 98 90 9f d4
Issuer Organization	Equifax
Issuer Country	US
Issuer Organizational Unit	Equifax Secure Certificate Authority
Crl link	
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] Intel External Basic Policy CA

Status	NotTimeValid ✖
Start Date	2006-02-16 18:01:30+00:00
End Date	2016-02-19 18:01:30+00:00
Sha256	732f4c0b21add69052db88d7810c948fefdc7c51fa781686f43edac7bfd38d42
Serial	05B0FF
Subject Name	Intel External Basic Policy CA
Subject Key Identifier	1a c6 0c 4a c4 47 6f a8 db ad 2b f0 f4 56 06 a3 ed 37 54 0c
Subject Organization	Intel Corporation
Subject Country	US
Issuer Name	null
Issuer Key Identifier	48 e6 68 f9 2b d2 b2 95 d7 47 d8 23 20 10 4f 33 98 90 9f d4
Issuer Organization	Equifax
Issuer Country	US
Issuer Organizational Unit	Equifax Secure Certificate Authority
Crl link	http://crl.geotrust.com/crls/secureca.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] null

Status	NoError ✔
Start Date	1998-08-22 16:41:51+00:00
End Date	2018-08-22 16:41:51+00:00
Sha256	0ed83aaa143fbdb5b03bcbd40d31e84401ec0e52ed3c24bace49243a0601b9aa
Serial	35DEF4CF
Subject Key Identifier	48 e6 68 f9 2b d2 b2 95 d7 47 d8 23 20 10 4f 33 98 90 9f d4
Subject Organization	Equifax
Subject Country	US
Subject Organizational Unit	Equifax Secure Certificate Authority
Issuer Name	null
Issuer Key Identifier	48 e6 68 f9 2b d2 b2 95 d7 47 d8 23 20 10 4f 33 98 90 9f d4
Issuer Organization	Equifax
Issuer Country	US
Issuer Organizational Unit	Equifax Secure Certificate Authority
Crl link	
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x534ED630 [Wed Apr 16 19:12:48 2014 UTC]
Entry Point	0x1800116fc (.text)
File Size	111760
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Legal Copyright	Copyright 2005-2014 Intel Corporation. All Rights Reserved.
File Version	4, 2, 2014, 0416
Company Name	Intel Corporation
Private Build	
Legal Trademarks	
Product Name	Intel(R) Threading Building Blocks for Windows
Special Build	
Product Version	4, 2, 2014, 0416
File Description	Scalable Allocator library
Original Filename	tbbmalloc.dll
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	c42dbdd553f7ae31f2575922756299ab20b8af839e33f8cf4cd44d19ce9e6f64

File Paths

FILE PATH ON CLIENT	SEEN COUNT
00000000-0000-0000-0000-000000000000	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x10d6c	0x10e00	6.166661	-
.rdata	0x12000	0x4127	0x4200	5.071752	-
.data	0x17000	0x24c20	0x2000	3.252123	-
.pdata	0x3c000	0x17c4	0x1800	5.047471	-
.rsrc	0x3e000	0x438	0x600	2.549203	-
.reloc	0x3f000	0x704	0x800	4.050241	-

PE Imports

- MSVCR110.dll
  - _lock
  - _unlock
  - __dllonexit
  - _onexit
  - __clean_type_info_names_internal
  - _initterm_e
  - _initterm
  - _malloc_crt

- free
- _amsg_exit
- __CppXcptFilter
- __crtCapturePreviousContext
- __crtCaptureCurrentContext
- __crtTerminateProcess
- __crtUnhandledException
- __crt_debugger_hook
- memcpy
- __C_specific_handler
- fputs
- getenv
- exit
- ??3@YAXPEAX@Z
- _wcsdup
- _strdup
- fflush
- abort
- memset
- fprintf
- __iob_func
- malloc
- _calloc_crt
- _errno

KERNEL32.dll

- GetCurrentProcessId
- QueryPerformanceCounter
- DecodePointer
- EncodePointer
- IsProcessorFeaturePresent
- IsDebuggerPresent
- TlsFree
- TlsSetValue
- TlsGetValue
- TlsAlloc
- LoadLibraryA
- lstrcpynA

- lstrcmpA
- GetProcAddress
- GetCurrentThreadId
- LeaveCriticalSection
- EnterCriticalSection
- InitializeCriticalSection
- GetLastError
- GetEnvironmentVariableA
- GetModuleHandleExA
- SetErrorMode
- VirtualFree
- VirtualAlloc
- SwitchToThread
- GetSystemTimeAsFileTime

PE Exports

- ?pool_aligned_malloc@rml@@YAPEAXPEAVMemoryPool@1@_K1@Z
- ?pool_aligned_realloc@rml@@YAPEAXPEAVMemoryPool@1@PEAX_K2@Z
- ?pool_create@rml@@YAPEAVMemoryPool@1@_JPEBUMemPoolPolicy@1@@Z
- ?pool_create_v1@rml@@YA?AW4MemPoolError@1@_JPEBUMemPoolPolicy@1@PEAPEAVMemoryPool@1@@Z
- ?pool_destroy@rml@@YA_NPEAVMemoryPool@1@@Z
- ?pool_free@rml@@YA_NPEAVMemoryPool@1@PEAX@Z
- ?pool_malloc@rml@@YAPEAXPEAVMemoryPool@1@_K@Z
- ?pool_realloc@rml@@YAPEAXPEAVMemoryPool@1@PEAX_K@Z
- ?pool_reset@rml@@YA_NPEAVMemoryPool@1@@Z
- safer_scalable_aligned_msize
- safer_scalable_aligned_realloc
- safer_scalable_free
- safer_scalable_msize
- safer_scalable_realloc
- scalable_aligned_free
- scalable_aligned_malloc
- scalable_aligned_realloc
- scalable_allocation_command
- scalable_allocation_mode
- scalable_calloc
- scalable_free
- scalable_malloc
- scalable_msize
- scalable_posix_memalign
- scalable_realloc

PE Resources

RT_VERSION