VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: mbimss.sys
File Type: PE32+ executable (native) x86-64, for MS Windows
SHA1: 425a09d768b86454c38a6a86a7f99e3295aadee4
MD5: 543eaa454b51bb9dcf6f5843b7e84ae5
First Seen Date: 2016-11-20 23:06:00 UTC
Number of Clients Seen: 2
Last Analysis Date: 2016-11-20 23:06:00 UTC
Human Expert Analysis Date: 2016-11-21 02:25:48 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2016-11-20 23:06:00 UTC	Clean
Static Analysis Overall Verdict	2016-11-20 23:06:00 UTC	No Threat Found
Human Expert Analysis Overall Verdict	2016-11-21 02:25:48 UTC	Clean
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

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2016-11-21 01:48:47 UTC
Analysis End Date: 2016-11-21 02:25:48 UTC
File Upload Date: 2016-11-20 23:06:00 UTC
Human Expert Analyst Feedback: None
Verdict: Clean

Additional File Information

Vendor Validation - Not Verified ✖

[+] Intel(R) Deutschland GmbH

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] Intel(R) Deutschland GmbH

Status	NotTimeValid (no effect on chain status)
Start Date	2015-08-19 12:15:01+00:00
End Date	2016-08-18 12:15:01+00:00
Sha256	ba0a14b0a35f9d90832b77f9ce35e3b2e8f7d361b71029a57741b3576a5017c0
Serial	330000B77EFA7F132E60013E4D00020000B77E
Subject Name	Intel(R) Deutschland GmbH
Subject Key Identifier	cf 83 ad d5 e1 cc 01 4a ef ff 6b 2f ca a0 c7 10 b1 1f 7b 24
Subject Organization	Intel Corporation
Subject Locality	Santa Clara
Subject State	CA
Subject Country	US
Issuer Name	Intel External Basic Issuing CA 3B
Issuer Key Identifier	e5 9c 00 ae 43 00 bd 1a 5a 4a b7 89 b6 e7 88 d0 0e 77 2d 22
Issuer Organization	Intel Corporation
Issuer Locality	Santa Clara
Issuer State	CA
Issuer Country	US
Crl link	http://certificates.intel.com/repository/CRL/Intel%20External%20Basic%20Issuing%20CA%203B(2).crl,http://www.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 3B

Status	NoError ✔
Start Date	2013-02-08 22:21:23+00:00
End Date	2018-02-08 22:31:23+00:00
Sha256	bcf5b49ca64c27d23bae8196902a397e0e2dc553785dad02770593bcf3ee865e
Serial	612CFF88000100000010
Subject Name	Intel External Basic Issuing CA 3B
Subject Key Identifier	e5 9c 00 ae 43 00 bd 1a 5a 4a b7 89 b6 e7 88 d0 0e 77 2d 22
Subject Organization	Intel Corporation
Subject Locality	Santa Clara
Subject State	CA
Subject Country	US
Issuer Name	Intel External Basic Policy CA
Issuer Key Identifier	56 3a 6f 17 ab 24 0c e5 b7 31 64 b0 11 ed db ea 23 be 5e bc
Issuer Organization	Intel Corporation
Issuer Country	US
Crl link	http://www.intel.com/repository/CRL/Intel%20External%20Basic%20Policy%20CA(1).crl,http://certificates.intel.com/repository/CRL/
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

[+] Intel External Basic Policy CA

Status	NoError ✔
Start Date	2013-02-01 00:00:00+00:00
End Date	2020-05-30 10:48:38+00:00
Sha256	84aeafbb5c739e54efe3090940de5bfcdb5870ee3981f7cd4b01910b12438411
Serial	79174AA9141736FE15A7CA9F2CFF4588
Subject Name	Intel External Basic Policy CA
Subject Key Identifier	56 3a 6f 17 ab 24 0c e5 b7 31 64 b0 11 ed db ea 23 be 5e bc
Subject Organization	Intel Corporation
Subject Country	US
Issuer Name	AddTrust External CA Root
Issuer Key Identifier	ad bd 98 7a 34 b4 26 f7 fa c4 26 54 ef 03 bd e0 24 cb 54 1a
Issuer Organization	AddTrust AB
Issuer Country	SE
Issuer Organizational Unit	AddTrust External TTP Network
Crl link	http://crl.trust-provider.com/AddTrustExternalCARoot.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Server Authentication (1.3.6.1.5.5.7.3.1)

[+] AddTrust External CA Root

Status	NoError ✔
Start Date	2000-05-30 10:48:38+00:00
End Date	2020-05-30 10:48:38+00:00
Sha256	3e8a4f0fb678d2f162b7e0f490b2ed3fd789e30c6828d0e9bd2ad4d9a27cc39c
Serial	01
Subject Name	AddTrust External CA Root
Subject Key Identifier	ad bd 98 7a 34 b4 26 f7 fa c4 26 54 ef 03 bd e0 24 cb 54 1a
Subject Organization	AddTrust AB
Subject Country	SE
Subject Organizational Unit	AddTrust External TTP Network
Issuer Name	AddTrust External CA Root
Issuer Key Identifier	ad bd 98 7a 34 b4 26 f7 fa c4 26 54 ef 03 bd e0 24 cb 54 1a
Issuer Organization	AddTrust AB
Issuer Country	SE
Issuer Organizational Unit	AddTrust External TTP Network
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] AddTrust External CA Root

Status	RevocationStatusUnknown ✖
Start Date	2013-08-15 20:26:30+00:00
End Date	2023-08-15 20:36:30+00:00
Sha256	c78f2781d613ed457dc2b7fc1605df940b8ef7c561b0d8c47d7ec003e3dadf60
Serial	3300000035D8D5595B0671412B000000000035
Subject Name	AddTrust External CA Root
Subject Key Identifier	ad bd 98 7a 34 b4 26 f7 fa c4 26 54 ef 03 bd e0 24 cb 54 1a
Subject Organization	AddTrust AB
Subject Country	SE
Subject Organizational Unit	AddTrust External TTP Network
Issuer Name	Microsoft Code Verification Root
Issuer Key Identifier	62 fb 0a 21 5b 7f 43 6e 11 da 09 54 50 6b f5 d2 96 71 f1 9e
Issuer Organization	Microsoft Corporation
Issuer Locality	Redmond
Issuer State	Washington
Issuer Country	US
Crl link	http://crl.microsoft.com/pki/crl/products/MicrosoftCodeVerifRoot.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)

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x560BA0A8 [Wed Sep 30 08:43:20 2015 UTC]
Entry Point	0x14840 (.text)
File Size	57872
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Legal Copyright	Copyright (C) 2013 Smith Micro Software, Inc.
Internal Name	mbimss.sys
File Version	1.5.1 built by: WinDDK
Company Name	Smith Micro Software, Inc.
Product Name	MBIM Selective Suspend Enabler
Product Version	1.5.1
File Description	MBIM Selective Suspend Enabler
Original Filename	mbimss.sys
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	dcc300480619086aaa52f187d2c9d9e8bf14ef533909722679b75b00c1da1efe

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x4f98	0x5000	6.216995	-
.rdata	0x6000	0x564	0x600	4.976829	-
.data	0x7000	0x11c0	0x400	0.791345[SUSPICIOUS]	-
.pdata	0x9000	0x318	0x400	3.442168	-
PAGE	0xa000	0x4bc	0x600	5.127222	-
INIT	0xb000	0x3b6	0x400	4.788712	-
.rsrc	0xc000	0x3d8	0x400	3.221734	-
.reloc	0xd000	0x9e	0x200	0.582746[SUSPICIOUS]	-