VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: imc1_ecm62_x64_2.sys
File Type: PE32+ executable (native) x86-64, for MS Windows
SHA1: 63f197846f58af9145add4111204bc227ed2eca8
MD5: a10c1246be71ab4eaa6373370cb2d2f9
First Seen Date: 2016-11-20 23:02:49 UTC
Number of Clients Seen: 4
Last Analysis Date: 2016-11-20 23:02:49 UTC
Human Expert Analysis Date: 2016-11-21 02:25:38 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 23:02:49 UTC	Clean
Static Analysis Overall Verdict	2016-11-20 23:02:49 UTC	No Threat Found
Human Expert Analysis Overall Verdict	2016-11-21 02:25:38 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	Suspicious
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 02:25:38 UTC
File Upload Date: 2016-11-20 23:02:50 UTC
Human Expert Analyst Feedback: None
Verdict: Clean

Additional File Information

Vendor Validation - Not Verified ✖

[+] emsys Embedded Systems GmbH

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] emsys Embedded Systems GmbH

Status	NotTimeValid (no effect on chain status)
Start Date	2014-11-14 00:00:00+00:00
End Date	2016-11-04 23:59:59+00:00
Sha256	0e1d606a4d4858719ce6e1b71d1d9d7c21956631b18831ba3847d8fc5a485e59
Serial	6A7A76142937B8D58B3AD28894F78E9B
Subject Name	emsys Embedded Systems GmbH
Subject Key Identifier	3e b4 34 89 2f 69 07 2b 94 e8 78 ff ad a2 76 c4 a5 31 4c 3e
Subject Organization	emsys Embedded Systems GmbH
Subject Locality	Ilmenau
Subject State	Thuringia
Subject Country	DE
Issuer Name	VeriSign Class 3 Code Signing 2010 CA
Issuer Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Issuer Organization	VeriSign, Inc.
Issuer Country	US
Issuer Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)10
Crl link	http://sf.symcb.com/sf.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] VeriSign Class 3 Code Signing 2010 CA

Status	NoError ✔
Start Date	2010-02-08 00:00:00+00:00
End Date	2020-02-07 23:59:59+00:00
Sha256	0f5cd6ebab15fa367e35893fad2bc49cd1a95449f58e7eb978d72bb0b100d764
Serial	5200E5AA2556FC1A86ED96C9D44B33C7
Subject Name	VeriSign Class 3 Code Signing 2010 CA
Subject Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Subject Organization	VeriSign, Inc.
Subject Country	US
Subject Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)10
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Issuer Organization	VeriSign, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Crl link	http://crl.verisign.com/pca3-g5.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

[+] VeriSign Class 3 Public Primary Certification Authority - G5

Status	NoError ✔
Start Date	2006-11-08 00:00:00+00:00
End Date	2036-07-16 23:59:59+00:00
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Name	VeriSign Class 3 Public Primary Certification Authority - G5
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Subject Organization	VeriSign, Inc.
Subject Country	US
Subject Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	undefined
Issuer Organization	VeriSign, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
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	0x565EBAC9 [Wed Dec 2 09:32:57 2015 UTC]
Entry Point	0x22064 (INIT)
File Size	84312
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Legal Copyright	\xa9 2013-2015
Build Type	release
Internal Name	cdcecm62_x64
File Version	2.39.5.0
Company Name	Intel Mobile Communications GmbH
Product Name	CDC/ECM Driver
Platform	Windows x64
Product Version	2.39.5.0
File Description	Ethernet Driver
Original Filename	cdcecm62_x64.sys
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	7
Sha256	0db9afe5ff84f658c2451068da3572c9477ca34ec0b46e022afc204b0f58d078

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xcb43	0xcc00	6.063029	-
.rdata	0xe000	0x137c	0x1400	4.492840	-
.data	0x10000	0x138	0x200	0.301407[SUSPICIOUS]	-
.pdata	0x11000	0xb7c	0xc00	4.437474	-
INIT	0x12000	0x91e	0xa00	4.974802	-
.rsrc	0x13000	0x450	0x600	2.590541	-
.reloc	0x14000	0x22a	0x400	2.318252	-