xcitium

CLEAN
Xcitium Final Verdict

File Name: ada.exe
File Type: PE32+ executable (GUI) x86-64, for MS Windows
SHA1: af784969780e20ec5aee2de5e08b3c24c8c1ef08
MD5: 6941e650acc328a77edde817941da0d2
First Seen Date: 2023-06-29 14:03:48 UTC
Number of Clients Seen: 4
Last Analysis Date: 2023-06-30 13:39:05 UTC
Human Expert Analysis Date: 2023-06-30 13:34:46 UTC
Human Expert Analysis Result: Clean
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-06-30 13:39:05 UTC	Clean
Static Analysis Overall Verdict	2023-06-30 13:39:05 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-06-30 13:39:05 UTC	No Match
Human Expert Analysis Overall Verdict	2023-06-30 13:34:46 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	Suspicious
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

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise NI Detector 3	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2023-06-29 14:03:17 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2023-06-29 14:03:17 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-06-29 17:47:58 UTC
Analysis End Date: 2023-06-30 13:34:46 UTC
File Upload Date: 2023-06-29 14:03:05 UTC
Human Expert Analyst Feedback: None
Verdict: Clean

Additional File Information

Vendor Validation - Not Verified ✖

[+] Hithink RoyalFlush Information Network Co.,Ltd.

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] Hithink RoyalFlush Information Network Co.,Ltd.

Status	NotTimeValid (no effect on chain status)
Start Date	2016-12-01 02:00:00
End Date	2020-01-01 01:59:59
Sha256	9c662aae97d77d738f938d2299c7d72222bc266f2436ba120fc022165c6d7a75
Serial	013FFE0AB939B60955F0FE7DED7A49E4
Subject Name	Hithink RoyalFlush Information Network Co.,Ltd.
Subject Key Identifier	ac 47 bc 32 df 6c 4e 84 a4 16 c2 e7 74 5d 56 39 dc 14 d6 e6
Subject Organization	Hithink RoyalFlush Information Network Co.,Ltd.
Subject Locality	HangZhou
Subject State	ZheJiang
Subject Country	CN
Subject Organizational Unit	IT Department
Issuer Name	Symantec Class 3 SHA256 Code Signing CA
Issuer Key Identifier	96 3b 53 f0 79 33 97 af 7d 83 ef 2e 2b cc ca b7 86 1e 72 66
Issuer Organization	Symantec Corporation
Issuer Country	US
Issuer Organizational Unit	Symantec Trust Network
Crl link	http://sv.symcb.com/sv.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] Symantec Class 3 SHA256 Code Signing CA

Status	NoError
Start Date	2013-12-10 02:00:00
End Date	2023-12-10 01:59:59
Sha256	0649cde463467e8e26bb6b7c23965e030248f95df21f6dcf28c51507fbb77c08
Serial	3D78D7F9764960B2617DF4F01ECA862A
Subject Name	Symantec Class 3 SHA256 Code Signing CA
Subject Key Identifier	96 3b 53 f0 79 33 97 af 7d 83 ef 2e 2b cc ca b7 86 1e 72 66
Subject Organization	Symantec Corporation
Subject Country	US
Subject Organizational Unit	Symantec Trust Network
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://s1.symcb.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 02:00:00
End Date	2036-07-17 02:59:59
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	NotTimeValid ϟ (no effect on chain status)
Start Date	2012-12-21 02:00:00
End Date	2020-12-31 01:59:59
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
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	NotTimeValid (no effect on chain status)
Start Date	1997-01-01 02:00:00
End Date	2021-01-01 01:59:59
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	0x5C1C68A4 [Fri Dec 21 04:14:28 2018 UTC]
Debug Artifacts	[object Object]
Entry Point	0x14001909c (.text)
Exifinfo	[object Object]
File Size	596456
File Type Enum	7
Imphash	107506ead95bb3a22146341fa6291607
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Magic Literal Enum	4
Legal Copyright	Copyright (C) 2018
Internal Name	H14
File Version	1.0.0.1
Company Name	\u676d\u5dde\u6838\u65b0\u8f6f\u4ef6\u6280\u672f\u6709\u9650\u516c\u53f8
Product Name	\u540c\u82b1\u987a\u95ee\u8d22
Product Version	1.0.0.1
File Description	\u540c\u82b1\u987a\u667a\u80fd\u5212\u8bcd
Original Filename	hxsmartwordhelp.exe
Translation	0x0804 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	50dc88c8db59f0760ab2e17cd6f2f1ec61a763a3beca014b15216d98e84e1357
Ssdeep	12288:0mnlGy57lYDzJBZhR8EyokybvnzgWkpgvgf:3EEYxBPR3yJybvn0WPlf
Trid	87.3,Win64 Executable (generic),6.3,Generic Win/DOS Executable,6.3,DOS Executable Generic

File Paths

FILE PATH ON CLIENT	SEEN COUNT
ada.exe	2
C:\Users\JITech\AppData\Local\Temp\Rar$EXa8288.10316\ada.exe	2

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x3582c	0x35a00	6.42526366775	d53051c631749a800b3279737241b9a1
.rdata	0x37000	0x19f0c	0x1a000	5.01238804154	c01bc9bcc800ec827e85898037e547fa
.data	0x51000	0x2ff4	0x1600	3.45659368727	13a29e3c8b633dfad1f9ba0ac853982e
.pdata	0x54000	0x2e50	0x3000	5.38609638567	a4ab1a652c9d3fd335f90c8f9c3e225d
.gfids	0x57000	0x1c4	0x200	3.45812094087	68b60d02978e66acd8544762256d2dec
.tls	0x58000	0x9	0x200	0.0203931352361	1f354d76203061bfdd5a53dae48d5435
.rsrc	0x59000	0x3aaf8	0x3ac00	5.80110623377	a4d62d6d49cda54d550acdf83148728e
.reloc	0x94000	0xd44	0xe00	5.33462815151	f49870568825a1d0d9f67c69d60ab8bb