VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: wpsupdate.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: aa9d0182bc4af8a6595207b7f5bd7c8336617520
MD5: e32e98fb900366fd33e8003de1fc57c4
First Seen Date: 2018-06-14 02:35:07 UTC
Number of Clients Seen: 9
Last Analysis Date: 2018-07-01 13:31:56 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Trusted Vendor

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2018-07-01 13:31:56 UTC	Clean	✓
Static Analysis Overall Verdict	2018-07-01 13:31:56 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2018-07-01 13:31:56 UTC	No Match	?
File Certificate Validation		Certificate and Vendor name are 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	Clean	✓
Packer detection on signature database	Unknown	?
Based on the sections entropy check! file is possibly packed	Suspicious	!
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	Suspicious	!
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean	✓
TLS callback functions array detected	Clean	✓

Packer detection on signature database

UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus & Laszlo [overlay]

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	
Uses a function clandestinely	
Has no visible windows	

Behavioral Information

QueryFilePath

C:\wpsupdate.exe

ReadFile

C:\Windows\Fonts\staticcache.dat

OpenMutex

Global\wpspatch_C42D7A0A-2868-45FF-92EE-9B7AE7124588
Global\wpssetup_C42D7A0A-2868-45FF-92EE-9B7AE7124588
Global\wps_diff_patch_C42D7A0A-2868-45FF-92EE-9B7AE7124588
Global\wpsuninst_C42D7A0A-2868-45FF-92EE-9B7AE7124588

WriteFile

C:\Users\win7\AppData\Roaming\kingsoft\office6\update\log\wpsupdate_2018_06_14.log

CreateMutex

_#_UPD_LogFile_Z_MutxName_#_
Global_UPD_Session_MutexName_

LoadLibrary

KERNEL32.DLL
ADVAPI32.dll
COMCTL32.dll
GDI32.dll
ole32.dll
OLEAUT32.dll
PSAPI.DLL
SHELL32.dll
SHLWAPI.dll
urlmon.dll
USER32.dll
USERENV.dll
VERSION.dll
WININET.dll
WLDAP32.dll
WS2_32.dll
Ws2_32.dll
\auth.dll
C:\office6\auth.dll
C:/office6\auth.dll
comctl32.dll

UxTheme.dll

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0

QueryProcessAddress

OpenProcess
ReadProcessMemory
CreateProcessW
CreateProcessA
URLDownloadToFileW
InternetReadFile
WinExec
ShellExecuteW
ShellExecuteExW
IsDebuggerPresent

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2018-07-01 13:31:52 UTC	No Match		NotDetected
Static Precise Trojan Detector 5	2018-07-01 13:31:52 UTC	No Match		NotDetected
Static Precise Trojan Detector 7	2018-07-01 13:31:52 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2018-07-01 13:31:52 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2018-07-01 13:31:52 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2018-07-01 13:31:52 UTC	No Match		NotDetected
Static Precise Trojan Detector 2	2018-07-01 13:31:52 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2018-07-01 13:31:53 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2018-07-01 13:31:53 UTC	No Match		NotDetected
Static Precise Trojan Detector 10	2018-07-01 13:31:53 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2018-07-01 13:31:53 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2018-07-01 13:31:53 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Verified ✔

[+] Zhuhai Kingsoft Office Software Co., Ltd.

Status	Valid ✔

Certificate Validation - Success ✔

[+] Thawte Timestamping CA

Status	NoError ✔
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	null
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	null
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	null
Key Usage	null
Extended Usage	null

[+] Symantec Time Stamping Services CA - G2

Status	NoError ✔
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	null
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)"}

[+] 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	null
Issuer Organization	VeriSign, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

[+] VeriSign Class 3 Code Signing 2010 CA

Status	NoError ✔
Start Date	2010-02-08 02:00:00
End Date	2020-02-08 01:59:59
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)"}

[+] Zhuhai Kingsoft Office Software Co., Ltd.

Status	NoError ✔
Start Date	2017-04-21 03:00:00
End Date	2020-02-05 01:59:59
Sha256	07005bd0d7b0ec66946efc24a2c2e8efcf2d12073ebc1294a7052e6fe40af6c9
Serial	60864463BBBC2E4E67D42771E4CBD9A5
Subject Name	Zhuhai Kingsoft Office Software Co., Ltd.
Subject Key Identifier	bb 0e a0 f4 b7 6f 29 49 ae 83 cc 73 05 bb 4d 72 ec 12 60 f1
Subject Organization	Zhuhai Kingsoft Office Software Co., Ltd.
Subject Locality	Zhuhai
Subject State	Guangdong
Subject Country	CN
Subject Organizational Unit	RD Department
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)"}

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5B1E6E00 [Mon Jun 11 12:41:36 2018 UTC]
Debug Artifacts	
Entry Point	0x5ad3d0 (UPX1)
Exifinfo	[object Object]
File Size	648832
File Type Enum	6
Imphash	4566dad3e8aa8d1af7661805601c64af
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Copyright\xa91988-2018 Kingsoft Corporation. All rights reserved.
M I M E Type	
Internal Name	wpsupdate
File Version	10,1,0,7440
Company Name	Zhuhai Kingsoft Office Software Co.,Ltd
Product Name	WPS Office
Product Version	10,1,0,7440
File Description	WPS Office Expansion tool
Original Filename	wpsupdate.exe
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	9fc3678dac889a1e21cf66b395882339552bc879bd52302ea0d91f1f261da1cb
Ssdeep	6144:jcyVjE0YYwpp8AOKPYzWjr2NC3vkergoY0vPml0AsIglyphFkzLv3Xam8SeqAv9P:jcyVLjwdYrCBnLpIglGhFc/ru9rAui8T
Trid	28.6,Win64 Executable (generic),28,UPX compressed Win32 Executable,27.5,Win32 EXE Yoda's Crypter,6.8,Win32 Dynamic Link Library (generic),4.6,Win32 Executable (generic)

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x12d000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0x12e000	0x80000	0x7f600	7.94256490473	0ac3c3b67a7a13f54dc93b5b26b1db8d
.rsrc	0x1ae000	0x1c000	0x1be00	5.75139642409	a0a797ee9abb7d9c290849bd17980ccb