VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: KuaiZip_Setup_2.8.28.3.exe
SHA1: e82d7e762a074a7530e7298ba2a55b0eb9780a95
MD5: 7c9ece4b69ccd582b7ecbdd59b0c7514
First Seen Date: 2017-05-31 00:07:11 UTC
Number of Clients Seen: 3
Last Analysis Date: 2017-05-31 00:07:11 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2017-05-31 00:07:11 UTC	Malware
Static Analysis Overall Verdict	2017-05-31 00:07:11 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2017-05-31 00:07:11 UTC	No Threat Found
Precise Detectors Overall Verdict	2017-05-31 00:07:11 UTC	No Match
File Certificate Validation		Vendor is Gray Listed

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	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

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	!
Writes to address space of another process	!

Behavioral Information

RegCloseKey

180
188
178

QueryFilePath

C:\KuaiZip_Setup_2.8.28.3.exe
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll

ReadRegisteryKey

ProgramW6432Dir
Plane16
Plane14
Plane15
Plane12
Plane13
Plane10
Plane11
Plane4
Plane5
Plane6
Disable
Plane7
Plane1
Plane2
Plane3
DataFilePath
Plane8
Plane9

CreateFile

{"dwCreationDisposition": "3", "path": "C:\\Windows\\Fonts\\staticcache.dat", "dwDesiredAccess": "80000000", "dwShareMode": "5"}
{"dwCreationDisposition": "3", "path": "\\\\.\\Nsi", "dwDesiredAccess": "0", "dwShareMode": "3"}

OpenRegisteryKey

{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\KuaiZipSFX\\"}
{"hKey": "188", "phkResult": "0", "lpSubKey": "Microsoft YaHei"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\KuaiZip\\Install"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\FontLink\\SystemLink"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows\\CurrentVersion"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\LanguagePack\\DataStore_V1.0"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\LanguagePack\\SurrogateFallback"}

CreateMutex

Install_renmingbao_19900126
Global\{84DDE91F-5045-411e-9D77-4AE3AADD679C}

OpenMutex

Local\MSCTF.Asm.MutexDefault1

LoadLibrary

kernel32.dll
msimg32.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
ADVAPI32.dll
OLEAUT32.DLL

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Uninstaller FP Detector	2017-05-31 00:06:38 UTC	No Match		No match.
Yara Rule Static Malware Detector	2017-05-31 00:06:38 UTC	No Match		No match.
Static Precise PUA Detector 1	2017-05-31 00:06:38 UTC	No Match		NotDetected
Static Precise Virus Detector	2017-05-31 00:06:38 UTC	No Match		NotDetected
Static Precise Trojan Detector	2017-05-31 00:06:38 UTC	No Match		NotDetected
Malicious Url Detector	2017-05-31 00:07:11 UTC	No Match		No match.

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Gray Listed

[+]

Status	Not Valid

Certificate Validation - Success

[+]

Status	NoError ✔
Start Date	2015-06-15 00:00:00+00:00
End Date	2017-09-13 23:59:59+00:00
Sha256	2f4269c21502277713910b9fea00cb7d290c659b483ff8b4a9b9e4f3ff4fbcc9
Serial	02B30EE595AD3BBE219E68DC6A431AF2
Subject Name	□□□□□□□□□□□□
Subject Key Identifier	04 6d 2d 29 ab 38 59 36 17 9c 4f 36 16 0e 43 ae 0e 13 54 09
Subject Organization	□□□□□□□□□□□□
Subject Locality	□□
Subject State	□□
Subject Country	CN
Subject Organizational Unit	□□
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