VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: AnyDesk.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 6ccdae5524dac0ccd033985557775df0b7735157
MD5: c2a98ef73f583a46cc861e01b1a86555
First Seen Date: 2017-05-19 00:42:51 UTC
Number of Clients Seen: 11
Last Analysis Date: 2017-05-30 16:17:10 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	2017-05-30 16:17:10 UTC	Clean	✓
Static Analysis Overall Verdict	2017-05-30 16:17:10 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2017-05-30 16:17:10 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!	Suspicious	!
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	Suspicious	!
TLS callback functions array detected	Clean	✓

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

SUSPICIOUS BEHAVIORS	
Injects code to another process	!
Creates a child process	!
Writes to address space of another process	!
Uses a function clandestinely	!
Reads memory of another process	!
Opens a file in a system directory	!
Has no visible windows	!

Behavioral Information

LoadLibrary

ADVAPI32.dll
ntmarta.dll
kernel32.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
OLEAUT32.dll
SHLWAPI.dll
ole32.dll
C:\Windows\system32\EhStorShell.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
propsys.dll
C:\Windows\system32\ntshrui.dll
srvcli.dll
cscapi.dll
slc.dll
c:\windows\system32\imageres.dll
WindowsCodecs.dll
SspiCli.dll
dwmapi.dll
UxTheme.dll
IMM32.dll
USER32.dll
ntshrui.dll
CRYPTBASE.dll
SXS.DLL
OLEAUT32
netutils.dll

ReadRegisteryKey

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

CreateFile

{"dwCreationDisposition": "4", "path": "C:\\Users\\win7\\AppData\\Roaming\\AnyDesk\\service.conf", "dwDesiredAccess": "80000000", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "C:\\AnyDesk.exe", "dwDesiredAccess": "80", "dwShareMode": "7"}
{"dwCreationDisposition": "3", "path": "C:\\Users\\win7\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations\\75fdacd8330bac18.customDestinations-ms", "dwDesiredAccess": "80000000", "dwShareMode": "1"}
{"dwCreationDisposition": "3", "path": "C:\\Windows\\SysWOW64\\ieframe.dll", "dwDesiredAccess": "80000000", "dwShareMode": "5"}
{"dwCreationDisposition": "2", "path": "C:\\Users\\win7\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations\\PBR8M3D8J5J020PYD741.temp", "dwDesiredAccess": "c0000000", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "C:\\Users\\win7\\AppData\\Local\\Microsoft\\Windows\\Caches\\cversions.1.db", "dwDesiredAccess": "80000000", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "C:\\Users\\win7\\AppData\\Local\\Temp\\win7.bmp", "dwDesiredAccess": "80000000", "dwShareMode": "1"}
{"dwCreationDisposition": "3", "path": "C:\\Windows\\SysWOW64\\stdole2.tlb", "dwDesiredAccess": "80000000", "dwShareMode": "5"}
{"dwCreationDisposition": "4", "path": "C:\\Users\\win7\\AppData\\Roaming\\AnyDesk\\ad.trace", "dwDesiredAccess": "c0000000", "dwShareMode": "7"}
{"dwCreationDisposition": "3", "path": "C:\\Windows\\system32\\rsaenh.dll", "dwDesiredAccess": "80000000", "dwShareMode": "1"}
{"dwCreationDisposition": "4", "path": "C:\\Users\\win7\\AppData\\Roaming\\AnyDesk\\user.conf", "dwDesiredAccess": "c0000000", "dwShareMode": "3"}
{"dwCreationDisposition": "4", "path": "C:\\Users\\win7\\AppData\\Roaming\\AnyDesk\\system.conf", "dwDesiredAccess": "80000000", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "C:\\Windows\\SysWOW64\\shell32.dll", "dwDesiredAccess": "80000000", "dwShareMode": "5"}
{"dwCreationDisposition": "3", "path": "C:\\AnyDesk.exe", "dwDesiredAccess": "80", "dwShareMode": "0"}
{"dwCreationDisposition": "3", "path": "C:\\Windows\\Fonts\\staticcache.dat", "dwDesiredAccess": "80000000", "dwShareMode": "5"}
{"dwCreationDisposition": "3", "path": "\\??\\C:\\Windows\\system32\\ntshrui.dll", "dwDesiredAccess": "80", "dwShareMode": "7"}
{"dwCreationDisposition": "3", "path": "C:\\", "dwDesiredAccess": "100081", "dwShareMode": "7"}
{"dwCreationDisposition": "3", "path": "\\??\\C:\\Windows\\system32\\EhStorShell.dll", "dwDesiredAccess": "80", "dwShareMode": "7"}
{"dwCreationDisposition": "3", "path": "C:\\Users\\win7\\AppData\\Local\\Microsoft\\Windows\\Caches\\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db", "dwDesiredAccess": "80000000", "dwShareMode": "1"}
{"dwCreationDisposition": "3", "path": "\\\\.\\PIPE\\srvsvc", "dwDesiredAccess": "c0000000", "dwShareMode": "3"}

OpenRegisteryKey

{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\AnyDesk"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\PDH"}
{"hKey": "23c", "phkResult": "0", "lpSubKey": "Segoe UI"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\FontLink\\SystemLink"}
{"hKey": "238", "phkResult": "0", "lpSubKey": "Segoe UI"}
{"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

<NULL>
Local\ad_trace_mtx
Local\ad_system_mtx
Local\ad_mailbox_3056_2886095820_0_mtx
Local\ad_mailbox_3056_2886095820_1_mtx
Session\1\ad_connect_queue_1424_2907814570_mtx

CreateProcess

"C:\AnyDesk.exe" --local-service

QueryFilePath

C:\AnyDesk.exe
C:\Windows\system32\EhStorShell.dll

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Uninstaller FP Detector	2017-05-30 16:17:00 UTC	No Match		No match.
Yara Rule Static Malware Detector	2017-05-30 16:17:00 UTC	No Match		No match.
Static Precise PUA Detector 1	2017-05-30 16:17:00 UTC	No Match		NotDetected
Static Precise Virus Detector	2017-05-30 16:17:00 UTC	No Match		NotDetected
Static Precise Trojan Detector	2017-05-30 16:17:00 UTC	No Match		NotDetected
Malicious Url Detector	2017-05-30 16:17:10 UTC	No Match		No match.

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Verified ✔

[+] philandro Software GmbH

Status	Valid ✔

Certificate Validation - Success ✔

[+] Thawte Timestamping CA

Status	NoError ✔
Start Date	1997-01-01 00:00:00
End Date	2020-12-31 23:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Name	Thawte Timestamping CA
Subject Key Identifier	null
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Crl link	null
Key Usage	null
Extended Usage	null

[+] Symantec Time Stamping Services CA - G2

Status	NoError ✔
Start Date	2012-12-21 00:00:00
End Date	2020-12-30 23:59:59
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
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
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)"}

[+] GlobalSign Root CA

Status	NoError ✔
Start Date	1998-09-01 12:00:00
End Date	2028-01-28 12:00:00
Sha256	8890262a3cd37c0b6c37c0239b9533f33244fb4ec82b6d846f6bd379ed2184b7
Serial	040000000001154B5AC394
Subject Name	GlobalSign Root CA
Subject Key Identifier	60 7b 66 1a 45 0d 97 ca 89 50 2f 7d 04 cd 34 a8 ff fc fd 4b
Issuer Name	GlobalSign Root CA
Issuer Key Identifier	null
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

[+] GlobalSign CodeSigning CA - G2

Status	NoError ✔
Start Date	2011-04-13 10:00:00
End Date	2019-04-13 10:00:00
Sha256	0974b40dbdea3bde1011dcb6e170c0d534df2f3d5eb0fcc5a160a0bfd732b7aa
Serial	0400000000012F4EE1355C
Subject Name	GlobalSign CodeSigning CA - G2
Subject Key Identifier	08 6e d8 b6 9c 8a bf ed 3e d7 c3 74 5d cc 80 1f a8 2f 50 7a
Issuer Name	GlobalSign Root CA
Issuer Key Identifier	60 7b 66 1a 45 0d 97 ca 89 50 2f 7d 04 cd 34 a8 ff fc fd 4b
Crl link	http://crl.globalsign.net/root.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

[+] philandro Software GmbH

Status	NotTimeValid ϟ (no effect on chain status)
Start Date	2013-09-23 08:08:33
End Date	2015-09-24 08:08:33
Sha256	d633c1066b69e2fe4a13acd829ce0f754d65744e687661603ce8163e73cabda1
Serial	112183F6AC0A7E594EA257BD986725A61ECF
Subject Name	philandro Software GmbH
Subject Key Identifier	e1 96 cb 0b 74 d4 fa ca a5 48 d8 de 7a 3f e2 c6 32 7d 9d 50
Issuer Name	GlobalSign CodeSigning CA - G2
Issuer Key Identifier	08 6e d8 b6 9c 8a bf ed 3e d7 c3 74 5d cc 80 1f a8 2f 50 7a
Crl link	http://crl.globalsign.com/gs/gscodesigng2.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	0x553ED075 [Tue Apr 28 00:12:37 2015 UTC]
Entry Point	0x402028 (.text)
File Size	1344608
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	(C) 2015 philandro Software GmbH
File Version	1.3.2.0
Company Name	philandro Software GmbH
Product Name	AnyDesk
Product Version	1.3
File Description	AnyDesk
Translation	0x0000 0x04e4
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	640e91cb448c0b0ade87bbd2747337ef8eef33f048365bc21efade5ed1d1eac3

File Paths

FILE PATH ON CLIENT	SEEN COUNT
6ccdae5524dac0ccd033985557775df0b7735157	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2c05	0x2e00	6.51619168914	b1303d7163d68ac1ac8ea2b56dd78b2b
.itext	0x4000	0x3d2200	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x3d7000	0x388	0x400	6.58054331142	20a2cfe19f5a8a604a03c517c75c1f7d
.data	0x3d8000	0x13d744	0x13d400	7.99985455112	65d23ec37bcb06f5a2a62b7a5ef17c48
.rsrc	0x516000	0x5ef8	0x6000	5.55090312418	1c5f50d21e19cc7999d5295bab3949de
.reloc	0x51c000	0x3f0	0x400	1.58570121045	bccf4139c02bdef92b18a34e5a5f3bb7