VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: PalmInputService.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 2fc4797f37798570609628e7e3d4b672440cedaa
MD5: 60f4de46fe1e1f0e7dfdbbca5dbad5e4
First Seen Date: 2017-04-12 17:56:14 UTC
Number of Clients Seen: 4
Last Analysis Date: 2017-10-17 19:57:36 UTC
Human Expert Analysis Date: 2017-10-16 18:50:57 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2017-10-17 19:57:36 UTC	Clean
Static Analysis Overall Verdict	2017-10-17 19:57:36 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2017-10-17 19:57:36 UTC	Highly Suspicious
Precise Detectors Overall Verdict	2017-10-17 19:57:36 UTC	No Match
Human Expert Analysis Overall Verdict	2017-10-16 18:50:57 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	Clean
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

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

SUSPICIOUS BEHAVIORS	
Operation successfully finished.	

Behavioral Information

OpenMutex

{803D6FB3-D77D-4C57-B2FF-88544C940593}
{EBA13986-25C7-429C-AF3C-63982B4F96DF}

QueryFilePath

C:\[uPalmInputService.exe]

ReadRegisteryKey

ServiceName
SyncMode5
FEATURE_CLIENTAUTHCERTFILTER
FromCacheTimeout
SecureProtocols
DisableKeepAlive
IdnEnabled
PreConnectLimit
PreResolveLimit
SqmHttpStreamRandomUploadPoolSize
CacheMode
EnableHttp1_1
ProxyHttp1.1
EnableNegotiate
DisableBasicOverClearChannel
ClientAuthBuiltInUI
DisableReadRange
SocketSendBufferLength
SocketReceiveBufferLength
KeepAliveTimeout
MaxHttpRedirects
MaxConnectionsPerServer
MaxConnectionsPer1_0Server
MaxConnectionsPerProxy
ServerInfoTimeout
ConnectTimeOut
ConnectRetries
SendTimeOut
ReceiveTimeOut
DisableNTLMPreAuth
ScavengeCacheLowerBound
CertCacheNoValidate
ScavengeCacheFileLifeTime
ScavengeCacheFileLimit
HttpDefaultExpiryTimeSecs
FtpDefaultExpiryTimeSecs
LeashLegacyCookies
SendExtraCRLF
WpadSearchAllDomains
DontUseDNSLoadBalancing
ShareCredsWithWinHttp
DnsCacheEnabled
DnsCacheEntries
DnsCacheTimeout
WarnOnPost
WarnAlwaysOnPost
WarnOnZoneCrossing
WarnOnBadCertRecving

WarnOnPostRedirect
AlwaysDrainOnRedirect
WarnOnHTTPSToHTTPRedirect
TcpAutotuning
BadProxyExpiresTime
FrameTabWindow
FrameMerging
SessionMerging
AdminTabProcs
TabProcGrowth
AutoProxyDetectType
WpadOverride
DisableBranchCache
UseFirstAvailable
CombineFalseStartData
DisableFalseStartBlocklist
EnforceP3PValidity
DuoProtocols
EnableSpdyDebugAsserts
SystemSetupInProgress
ProxyEnable
ProxyServer
ProxyOverride
AutoConfigURL
AutoDetect
SavedLegacySettings
DefaultConnectionSettings
WpadDecision
WpadDecisionTime
WpadExpirationDays
DisableSecuritySettingsCheck
CreateUriCacheSize
EnablePunycode
WpadDecisionReason
WpadDhcp
WpadDns
WpadDetectedUrl

CreateRegisteryKey

SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
{69DC4768-446B-4F82-A6B0-63966A243064}
52-54-00-12-35-02

CreateFile

\\.\PhysicalDrive0
\\.\{CFE68B1E-656A-488B-8077-738CA67BA3A5}
C:\Users\win7\AppData\LocalLow\PalmInput\Dict\Cate\Palminput-cate-rec-list.xml
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
\\.\Nsi
C:\Windows\system32\rsaenh.dll

OpenRegisteryKey

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards
Software\PalmInput
SYSTEM\CurrentControlSet\Control\Keyboard Layouts\041f0409\
Software\Microsoft\CTF\SortOrder\AssemblyItem\0x00000804\{34745C63-B2F0-4784-8B67-5E12C8701A31}
Keyboard Layout\Preload\
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
Software\Microsoft\Internet Explorer\Main\FeatureControl
FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
RETRY_HEADERONLYPOST_ONCONNECTIONRESET
FEATURE_MIME_HANDLING
FEATURE_BYPASS_CACHE_FOR_CREDPOLICY_KB936611

FEATURE_IGNORE_MAPPINGS_FOR_CREDPOLICY
FEATURE_INCLUDE_PORT_IN_SPN_KB908209
FEATURE_BUFFERBREAKING_818408
FEATURE_SKIP_POST_RETRY_ON_INTERNETWRITEFILE_KB895954
FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DOWNLOAD_KB843289
FEATURE_USE_CNAME_FOR_SPN_KB911149
FEATURE_PERMIT_CACHE_FOR_AUTHENTICATED_FTP_KB910274
FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
FEATURE_DISALLOW_NULL_IN_RESPONSE_HEADERS
FEATURE_DIGEST_NO_EXTRAS_IN_URI
FEATURE_ENABLE_PASSPORT_SESSION_STORE_KB948608
FEATURE_EXCLUDE_INVALID_CLIENT_CERT_KB929477
FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB967545
FEATURE_RETURN_FAILED_CONNECT_CONTENT_KB942615
FEATURE_PRESERVE_SPACES_IN_FILENAMES_KB952730
FEATURE_ENABLE_PROXY_CACHE_REFRESH_KB2983228
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Policies
Software
Software\Policies\Microsoft\Internet Explorer
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN_KB2385266
FEATURE_COMPAT_USE_CONNECTION_BASED_NEGOTIATE_AUTH_KB2151543
FEATURE_SCH_SEND_AUX_RECORD_KB_2618444
Software\Microsoft\Internet Explorer\Main
Software\Policies\Microsoft\Internet Explorer\Main
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
Software\Policies\Microsoft\PeerDist\Service
Software\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
System\Setup
{69DC4768-446B-4F82-A6B0-63966A243064}
Content
Cookies
History
FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915
FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Microsoft\Internet Explorer\Security
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
FEATURE_LOCALMACHINE_LOCKDOWN
FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562

CreateMutex

<NULL>
{803D6FB3-D77D-4C57-B2FF-88544C940593}
{EBA13986-25C7-429C-AF3C-63982B4F96DF}
InputTSF.Service.MutexName
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

LoadLibrary

C:\[uPalmInputService.exe]
API-MS-Win-Security-LSALookup-L1-1-0.dll
Advapi32.dll
ntmarta.dll
shell32.dll
ADVAPI32.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
Secur32.dll
SHELL32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
WS2_32.dll
winhttp.dll
IPHLPAPI.DLL
api-ms-win-downlevel-shlwapi-l2-1-0.dll
DNSAPI.dll
ole32.dll

CRYPTBASE.dll
OLEAUT32.dll
dhcpcsvc.DLL
urlmon.dll
Comctl32.dll
imm32.dll
C:\Windows\system32\ws2_32

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2017-10-17 19:55:18 UTC	No Match		NotDetected
Static Precise Virus Detector	2017-10-17 19:55:18 UTC	No Match		NotDetected
Static Precise Trojan Detector	2017-10-17 19:55:18 UTC	No Match		NotDetected
Static Precise Adware InstallCore Detector 1	2017-10-17 19:55:18 UTC	No Match		NotDetected
Static Precise Trojan Detector 2	2017-10-17 19:55:18 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2017-10-17 19:55:18 UTC	No Match		NotDetected
Static Precise Trojan Generic Cryptor Detector 1	2017-10-17 19:55:18 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2017-10-17 19:55:18 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2017-10-16 11:19:13 UTC
Analysis End Date: 2017-10-16 18:50:57 UTC
File Upload Date: 2017-04-12 17:56:15 UTC
Human Expert Analyst Feedback:
Verdict: Clean

Additional File Information

Vendor Validation - Not Verified ✖

[+] □□□□□□□□□□□□□□□

Status	Not Valid ✖

[+] □□□□□□□□□□□□□□□

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] UTN-USERFirst-Object

Status	NoError ✔
Start Date	1999-07-09 18:31:20
End Date	2019-07-09 18:40:36
Sha256	2acd612cf8f03b495f01de23e4f5d695350d00ff6d27f0255362c79df0eca403
Serial	44BE0C8B500024B411D3362DE0B35F1B
Subject Name	UTN-USERFirst-Object
Subject Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b 3c c9 d8
Issuer Name	UTN-USERFirst-Object
Issuer Key Identifier	null
Crl link	http://crl.usertrust.com/UTN-USERFirst-Object.crl
Key Usage	{"Digital Signature",Non-Repudiation,"Certificate Signing","Off-line CRL Signing","CRL Signing (c6)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

[+] COMODO SHA-1 Time Stamping Signer

Status	NoError ✔
Start Date	2015-12-31 00:00:00
End Date	2019-07-09 18:40:36
Sha256	f49570a2c3e23ad1d7ef62a2c137f08af02d8a2855bd96053e2365e354572fe2
Serial	1688F039255E638E69143907E6330B
Subject Name	COMODO SHA-1 Time Stamping Signer
Subject Key Identifier	8e 6b 2d 33 6b f4 33 a7 93 b3 13 9a a5 e0 0a f7 12 35 6a 88
Issuer Name	UTN-USERFirst-Object
Issuer Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b 3c c9 d8
Crl link	http://crl.usertrust.com/UTN-USERFirst-Object.crl
Key Usage	{"Digital Signature","Non-Repudiation (c0)"}
Extended Usage	{"Time Stamping (1.3.6.1.5.5.7.3.8)"}

[+] Certification Authority of WoSign

Status	NoError ✔
Start Date	2009-08-08 01:00:01
End Date	2039-08-08 01:00:01
Sha256	c80c68104746f7ee9efadeab5e1db95f232ea9190fe6a99f17cd47ffed5177f9
Serial	5E68D61171946350560068F33EC9C591
Subject Name	Certification Authority of WoSign
Subject Key Identifier	e1 66 cf 0e d1 f1 b3 4b b7 06 20 14 fe 87 12 d5 f6 fe fb 3e
Issuer Name	Certification Authority of WoSign
Issuer Key Identifier	null
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

[+] WoSign Class 3 Code Signing CA

Status	NoError ✔
Start Date	2009-08-08 01:00:05
End Date	2024-08-08 01:00:05
Sha256	a19cbca98ed09596344892abb595d6970ff7013a22998bd9a2f6aaffec67ae1f
Serial	46BBB340FAB9C17928938C93DA108679
Subject Name	WoSign Class 3 Code Signing CA
Subject Key Identifier	f5 02 aa 4b d3 e0 1a 8e 77 50 d6 1a bb eb df b9 83 70 b0 4e
Issuer Name	Certification Authority of WoSign
Issuer Key Identifier	e1 66 cf 0e d1 f1 b3 4b b7 06 20 14 fe 87 12 d5 f6 fe fb 3e
Crl link	http://crls1.wosign.com/ca1.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)"}

[+] □□□□□□□□□□□□□□

Status	NoError ✔
Start Date	2016-02-22 06:40:05
End Date	2018-03-22 06:40:05
Sha256	64a959f5ac3f37303ace14bf7749c70923ad8238b51f13921cbddb60cd1d984a
Serial	684A4BEDF03283EE53282B04ABC26E85
Subject Name	□□□□□□□□□□□□□□
Subject Key Identifier	29 4a 5a eb 29 1e 6a ee 9b 99 73 6e f6 f6 aa aa bf 2f d1 50
Issuer Name	WoSign Class 3 Code Signing CA
Issuer Key Identifier	f5 02 aa 4b d3 e0 1a 8e 77 50 d6 1a bb eb df b9 83 70 b0 4e
Crl link	http://crls1.wosign.com/ca1-code-3.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	0x586F0B59 [Fri Jan 6 03:13:29 2017 UTC]
Entry Point	0x5694de (.text)
File Size	3595728
File Type Enum	6
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	(C) xinshuru.com All Rights Reserved.
Internal Name	PalmInputService
File Version	2.7.0.1686
Company Name	\u5317\u4eac\u9177\u777f\u8499\u6570\u5b57\u79d1\u6280\u6709\u9650\u516c\u53f8
Product Name	\u624b\u5fc3\u8f93\u5165\u6cd5
Product Version	2.7.0.1686
File Description	\u624b\u5fc3\u8f93\u5165\u6cd5 \u670d\u52a1\u7a0b\u5e8f
Original Filename	PalmInputService.exe
Translation	0x0804 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	caf9fe4a5953d850c4f8b5e8cb674d3a4535ae604a565099b7f3046b0d0542c6

File Paths

FILE PATH ON CLIENT	SEEN COUNT
2fc4797f37798570609628e7e3d4b672440cedaa	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x19e9fa	0x19ea00	6.60668059987	fff307fec07f909d30d9f49f1ee46018
.rdata	0x1a0000	0x1544d6	0x154600	6.7553344625	ef9e38180a2b77a19d96cf8ccf78e98e
.data	0x2f5000	0x76320	0xda00	3.76891105839	989bcda0e4605a3ec78c49ecacffca9e
.rsrc	0x36c000	0x42d08	0x42e00	6.91432849507	27ebe897dc56269b08100839ac5a8f3f
.reloc	0x3af000	0x26ae0	0x26c00	4.15765017578	4a5b5fc5e2a008309cfc82f8be08f0e9