VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: CIMB_BANK_-STATEMENTPDF.exe
File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: ddc8f16b0ca5d84a92789f4a2ea1440cd3324ce2
MD5: 2d58b4a0571941e3301ad0632705b170
First Seen Date: 2017-01-03 03:27:49 UTC
Number of Clients Seen: 3
Last Analysis Date: 2017-01-03 03:27:49 UTC
Human Expert Analysis Date: 2017-01-09 02:25:58 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2017-01-03 03:27:49 UTC	Malware
Static Analysis Overall Verdict	2017-01-03 03:27:49 UTC	Highly Suspicious
Dynamic Analysis Overall Verdict	2017-01-03 03:27:49 UTC	Highly Suspicious
Human Expert Analysis Overall Verdict	2017-01-09 02:25:58 UTC	Malware
File Certificate Validation		Not Applicable

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

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	Clean
TLS callback functions array detected	Clean

Packer detection on signature database

- Microsoft Visual C# / Basic .NET
- .NET executable

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	!

SUSPICIOUS BEHAVIORS	
Injects code to another process	!
Opens a file in a system directory	!
Modifies Windows Service Keys	!
Uses a function clandestinely	!

Behavioral Information

OpenMutex

Global\CLR_CASOFF_MUTEX
Global\.net data provider for sqlserver

QueryFilePath

C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\CIMB_BANK_-STATEMENTPDF.exe
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\assembly\GAC_32\System.Data\2.0.0.0__b77a5c561934e089\System.Data.dll
C:\Windows\SysWOW64\schannel.dll
C:\Windows\SysWOW64\msv1_0.DLL

LowerChar

file

ReadRegisteryKey

InstallRoot
CLRLoadLogDir
OnlyUseLatestCLR
GCStressStart
GCStressStartAtJit
DisableConfigCache
CacheLocation
DownloadCacheQuotaInKB
EnableLog
LoggingLevel
ForceLog
LogFailures
VersioningLog
LogResourceBinds
UseLegacyIdentityFormat
DisableMSIPeek
NoClientChecks
DevOverrideEnable
LatestIndex
NIUsageMask
ILUsageMask
DisplayName
ConfigMask
ConfigString
MVID

EvalationData
Status
ILDependencies
NIDependencies
MissingDependencies
Modules
SIG
LastModTime
mscorlib
Latest
index1
LegacyPolicyTimeStamp
System.Drawing
System
System.Xml
System.Configuration
System.Windows.Forms
System.Deployment
System.Runtime.Serialization.Formatters.Soap
Accessibility
System.Security
System.Data
System.EnterpriseServices
Microsoft.VisualC
System.Transactions
IJWEntrypointCompatMode
Microsoft.VisualBasic
System.Web
System.Management
System.Runtime.Remoting
DbgJITDebugLaunchSetting
DbgManagedDebugger
Library
IsMultiInstance
First Counter
CategoryOptions
FileMappingSize
Counter Names
System.Data.SqlXml
System.DirectoryServices
UserContextLockCount
UserContextListCount

CreateRegisteryKey

Software\Microsoft\Fusion\GACChangeNotification\Default
System\CurrentControlSet\Control\SecurityProviders\Schannel

CreateFile

C:\CIMB_BANK_-STATEMENTPDF.exe.config
C:\CIMB_BANK_-STATEMENTPDF.exe
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index1c2.dat
C:\Windows\system32\l_intl.nls
C:\Windows\assembly\pubpol1.dat
C:\Windows\assembly\GAC_32\System.Data\2.0.0.0__b77a5c561934e089\System.Data.dll
C:\Windows\system32\TestFile.txt
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Config\machine.config
C:\Windows\assembly\GAC_32\System.Transactions\2.0.0.0__b77a5c561934e089\System.Transactions.dll
C:\Windows\system32\rsaenh.dll
\\.\Nsi

OpenRegisteryKey

Software\Microsoft\.NETFramework\Policy\
v2.0
Software\Microsoft\.NETFramework
Upgrades
Standards
AppPatch
Software\Microsoft\.NETFramework\Policy\Standards
v2.0.50727
Software\Microsoft\Fusion
Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\CIMB_BANK_-STATEMENTPDF.exe
Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Software\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets
Internet
LocalIntranet
Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3979321414-2393373014-2172761192-1000
Software\Microsoft\.NETFramework\v2.0.50727\Security\Policy
Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32
index1c2
NI\181938c6\7950e2c5
NI\181938c6\7950e2c5\16
IL\7950e2c5\4b5f28af\5f
NI\39f3b04c\1ce531e3
Software\Microsoft\StrongName
Software\Microsoft\Fusion\PublisherPolicy\Default
policy.2.0.System.Drawing__b03f5f7f11d50a3a
NI\3cca06a0\6dc7d4c0
NI\3cca06a0\6dc7d4c0\b
IL\6dc7d4c0\c47ad54\56
NI\30bc7c4f\3f50fe4f\18
IL\424bd4d8\324708cb\5c
IL\19ab8d57\c91dbb2\5e
IL\3f50fe4f\265c633d\60
policy.2.0.System__b77a5c561934e089
policy.2.0.System.Xml__b77a5c561934e089
policy.2.0.System.Configuration__b03f5f7f11d50a3a
SOFTWARE\Microsoft\.NETFramework\Policy\APTCA
policy.2.0.System.Windows.Forms__b77a5c561934e089
NI\61e7e666\c991064
NI\61e7e666\c991064\a
IL\475dce40\1c022996\5b
IL\2dd6ac50\553abeb3\58
IL\41c04c7e\4bf62c79\50
IL\3ced59c5\48d69eb2\54
IL\c991064\5086dba8\51
policy.2.0.System.Deployment__b03f5f7f11d50a3a
policy.2.0.System.Runtime.Serialization.Formatters.Soap__b03f5f7f11d50a3a
policy.2.0.Accessibility__b03f5f7f11d50a3a
policy.2.0.System.Security__b03f5f7f11d50a3a
policy.2.0.System.Data__b77a5c561934e089
NI\226b2009\5b43ba09
NI\226b2009\5b43ba09\2
IL\3b249b34\27fafbb2\48
IL\3d590c3f\59f3b67b\5d
IL\85e83df\71a5f57e\49
IL\5b43ba09\32355fde\4e
policy.2.0.System.EnterpriseServices__b03f5f7f11d50a3a
policy.8.0.Microsoft.VisualC__b03f5f7f11d50a3a
policy.2.0.System.Transactions__b77a5c561934e089
SOFTWARE\Microsoft\BidInterface\Loader
policy.8.0.Microsoft.VisualBasic__b03f5f7f11d50a3a
NI\1c22df2f\4f99a7c9
NI\1c22df2f\4f99a7c9\66
IL\f6e8397\628bc3e2\47
IL\2b1a4e4\3822b536\f
IL\24bf93f6\708deaf7\46
IL\4f99a7c9\191b956f\66
policy.2.0.System.Web__b03f5f7f11d50a3a
policy.2.0.System.Management__b03f5f7f11d50a3a
policy.2.0.System.Runtime.Remoting__b77a5c561934e089
SYSTEM\CurrentControlSet\Services\.NET Data Provider for SqlServer\Performance
SYSTEM\CurrentControlSet\Services\.net data provider for sqlserver\Performance
NI\159a66b8\424bd4d8
NI\159a66b8\424bd4d8\17
NI\6faf58\19ab8d57

NI\6faf58\19ab8d57\15
IL\75638fee\27002c8f\5a
policy.2.0.System.Data.SqlXml__b77a5c561934e089
Software\Microsoft\MSSQLServer\Client\SuperSocketNetLib
NI\6eae2d34\3b249b34
NI\6eae2d34\3b249b34\1
NI\57d4b1bf\85e83df
NI\57d4b1bf\85e83df\19
IL\3a6a696d\59152bf2\4a
policy.2.0.System.DirectoryServices__b03f5f7f11d50a3a
SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo

CreateMutex

<NULL>
Global\.net data provider for sqlserver

LoadLibrary

ADVAPI32.dll
SHLWAPI.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
mscoree.dll
ntdll
advapi32.dll
shell32.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\38bf604432e1a30c954b2ee40d6a2d1c\mscorlib.ni.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
ole32.dll
kernel32.dll
AdvApi32.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\908ba9e296e92b4e14bdc2437edac603\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\5a401fd2a7689ff13fb54182953f9c40\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\6949c4470a81970ec3de0a575d93babc\System.Windows.Forms.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Data\4b335bfaa07fc54f2d72213d33f53e97\System.Data.ni.dll
C:\Windows\assembly\GAC_32\System.Data\2.0.0.0__b77a5c561934e089\System.Data.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\12dc10e5c0e8d176cf21a16a6fc5fc3b\Microsoft.VisualBasic.ni.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Gdiplus.dll
gdiplus.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
user32.dll
gdi32.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\007fc007edc388d9806dff94ee04f129\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\d49908aa93a23c84847b1f8b1b667860\System.Xml.ni.dll
ntdll.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Transactions\f45bc0251cceb599622f55cc1c7f4aba\System.Transactions.ni.dll
C:\Windows\assembly\GAC_32\System.Transactions\2.0.0.0__b77a5c561934e089\System.Transactions.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.EnterpriseSe#\abecd46ce0b212dad31a9e8f9adf073f\System.EnterpriseServices.ni.dll
Ole32
API-MS-Win-Security-LSALookup-L1-1-0.dll
CRYPTBASE.dll
C:\Windows\system32\security.dll
C:\Windows\system32\secur32.dll
C:\Windows\system32\ntdsapi.dll
C:\Windows\system32\netapi32.dll
C:\Windows\system32\kernel32.dll
C:\Windows\system32\ws2_32

QueryProcessAddress

OpenProcess
OpenProcessW

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2017-01-09 02:11:47 UTC
Analysis End Date: 2017-01-09 02:25:58 UTC
File Upload Date: 2017-01-03 03:28:42 UTC
Human Expert Analyst Feedback: Backdoor.Win32.Androm
Verdict: Malware
Malware Family: Backdoor.Win32.Androm
Malware Type: Backdoor

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5865F879 [Fri Dec 30 06:02:33 2016 UTC]
Entry Point	0x426c2e (.text)
File Size	163840
Machine Type	Intel 386 or later - 32Bit
Translation	0x0000 0x04b0
Legal Copyright	2016 (C) Ck. All rights reserved
Assembly Version	12.5.17.7
Internal Name	8888888.scr.exe
File Version	6.18.7.3
Company Name	Ck Company
Legal Trademarks	Ck
Comments	Ck Company
Product Name	Ck
Product Version	6.18.7.3
File Description	Ck
Original Filename	8888888.scr.exe
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	36f87dd5e6e691de0544a5a1fe469215e609c5acdc5d9feba3765c187960c159

File Paths

FILE PATH ON CLIENT	SEEN COUNT
ddc8f16b0ca5d84a92789f4a2ea1440cd3324ce2	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0x24c34	0x25000	7.924901[SUSPICIOUS]	-
.rsrc	0x28000	0xe30	0x1000	2.054936	-
.reloc	0x2a000	0xc	0x1000	0.016408[SUSPICIOUS]	-