VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: 6e0c1d7c503e8244f8fce01c932732fa.zip
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: b84215267063427cf01b086a9595901d12fb3fe5
MD5: 6e0c1d7c503e8244f8fce01c932732fa
First Seen Date: 2017-05-02 21:45:16 UTC
Number of Clients Seen: 7
Last Analysis Date: 2020-11-05 15:54:20 UTC
Human Expert Analysis Date: 2020-11-05 15:54:20 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2020-11-05 15:54:20 UTC	Malware
Static Analysis Overall Verdict	2020-11-05 15:54:20 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2020-11-05 15:54:20 UTC	No Threat Found
Precise Detectors Overall Verdict	2020-11-05 15:54:20 UTC	No Match
Human Expert Analysis Overall Verdict	2020-11-05 15:54:20 UTC	Malware
File Certificate Validation		Not Applicable

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!	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

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	
Creates a child process	
Has no visible windows	
Reads memory of another process	

Behavioral Information

QueryFilePath

C:\Windows\system32\ODBC32.dll
C:\Windows\System32\msxml3.dll
C:\Windows\system32\MSFTEDIT.DLL
C:\Windows\syswow64\MSCTF.dll
C:\Windows\system32\UIRibbon.dll
C:\Windows\System32\msxml6.dll
C:\Windows\syswow64\USER32.dll

ReadRegisteryKey

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

CreateRegisteryKey

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Management
Auto Activation Languages
Ribbon
SOFTWARE\System32\Configuration\

CreateFile

C:\Users\win7\AppData\Local\Temp\DD4CE9D8.rtf
C:\Windows\Fonts\staticcache.dat
C:\
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db
C:\Users\desktop.ini
C:\Users
C:\Users\win7

C:\Users\win7\AppData
C:\Users\win7\AppData\Local
C:\Users\win7\AppData\Local\Temp
\\?\C:\Users\win7\AppData\Local\Temp\dd_vcredist_amd64_20150610171551_0_vcRuntimeMinimum_x64.log
\\?\C:\Users\win7\AppData\Local\Temp\dd_vcredist_amd64_20150610171551.log
\\?\C:\ProgramData\System32\xfs
\\?\C:\Users\win7\AppData\Local\Temp\DD4CE9D8.rtf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Sidebar\Settings.ini
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Wrinkled_Paper.gif
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\White_Chocolate.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\To_Do_List.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Tiki.gif
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Tanspecks.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Stucco.gif
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Stars.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\SoftBlue.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Soft Blue.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Small_News.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Shorthand.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\ShadesOfBlue.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Shades of Blue.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Seyes.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Sand_Paper.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Roses.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Psychedelic.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Pretty_Peacock.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Pine_Lumber.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Peacock.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\OrangeCircles.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Orange Circles.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Notebook.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Music.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Month_Calendar.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Monet.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Memo.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\HandPrints.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Hand Prints.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\GreenBubbles.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Green Bubbles.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Graph.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Genko_2.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Genko_1.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Garden.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Dotted_Lines.emf
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Connectivity.gif
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Cave_Drawings.gif
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Blue_Gradient.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.jpg
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Stationery\Bears.htm
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\Backup\new\edb00001.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\oeold.xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\edb00001.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows Mail\edb.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V010000C.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V010000B.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V010000A.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V0100009.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V0100008.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V0100007.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V0100006.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V0100005.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V0100004.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V0100003.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\WebCache\V01.log
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1024.db
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db

\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin
\\?\C:\Users\win7\AppData\Local\Microsoft\Windows\UsrClass.dat
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\Tiles\pin9728060290\msapplication.xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Last Active\{CF36B154-1421-11E5-BA75-080027F0A770}.dat
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Last Active\RecoveryStore.{AEDD392D-1421-11E5-BA75-080027F0A770}.dat
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\imagestore\2xeh1w7\imagestore.dat
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\DOMStore\KHBIN2T7\www.youtube[1].xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\DOMStore\HV6WWNXJ\www.msn[1].xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\DOMStore\HV6WWNXJ\www.google.com[1].xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\DOMStore\683K235F\www.microsoft[1].xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\DOMStore\683K235F\googleads.g.doubleclick[1].xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\DOMStore\48JBUR80\ls.hit.gemius[2].xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\DOMStore\48JBUR80\ls.hit.gemius[1].xml
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\tabiconcache.dat
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\frameiconcache.dat
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
\\?\C:\Users\win7\AppData\Local\Microsoft\Internet Explorer\brndlog.bak
\\?\C:\Users\win7\AppData\Local\GDIPFONTCACHEV1.DAT
\\?\C:\Users\win7\.idlerc\recent-files.lst
\\?\C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg
\\?\C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg
\\?\C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg
\\?\C:\Users\Public\Pictures\Sample Pictures\Koala.jpg
\\?\C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg
\\?\C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg
\\?\C:\Users\Public\Pictures\Sample Pictures\Desert.jpg
\\?\C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg
\\?\C:\Users\Default\NTUSER.DAT.LOG
\\?\C:\Users\All Users\Microsoft\Windows NT\MSScan\WelcomeScan.jpg
\\?\C:\Users\All Users\Microsoft\Windows NT\MSFax\VirtualInbox\en-US\WelcomeFax.tif
\\?\C:\Users\All Users\Microsoft\Windows Defender\Support\MPLog-07132009-221007.log
\\?\C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Service\History.Log
\\?\C:\Users\All Users\Microsoft\Windows Defender\Scans\History\CacheManager\MpSfc.bin
\\?\C:\Users\All Users\Microsoft\Windows Defender\Scans\mpcache-892AE4E20C5CD2BF74BA97F2AD969461A67ACB8B.bin
\\?\C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_x64_d473a376adfb18a7b165c5e3c26de43cd8bccb_cab_07087674\DMI7607.tmp.log.xml
\\?\C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_0_ff109b8e6ff4d05d9a6d51ed29594fae5ed875d_cab_077bf59b\client_manifest.txt
\\?\C:\Users\All Users\Microsoft\Windows\Power Efficiency Diagnostics\energy-report.html
\\?\C:\Users\All Users\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-latest.xml
\\?\C:\Users\All Users\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2017-05-03.xml
\\?\C:\Users\All Users\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2015-07-27.xml
\\?\C:\Users\All Users\Microsoft\Windows\Power Efficiency Diagnostics\energy-report-2015-06-11.xml
\\?\C:\Users\All Users\Microsoft\Windows\Caches\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000002.db
\\?\C:\Users\All Users\Microsoft\Windows\Caches\{8CA4AB4C-5F2D-4223-BEAC-550A09840C77}.2.ver0x0000000000000001.db
\\?\C:\Users\All Users\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x000000000000000c.db
\\?\C:\Users\All Users\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x000000000000000a.db
\\?\C:\Users\All Users\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000007.db
\\?\C:\Users\All Users\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000006.db
\\?\C:\Users\All Users\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000005.db
\\?\C:\Users\All Users\Microsoft\Windows\Caches\cversions.2.db
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile44.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile43.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile42.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile41.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile40.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile39.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile38.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile37.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile36.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile35.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile34.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile33.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile32.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile31.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile30.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile29.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile28.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile27.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile26.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile25.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile24.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile23.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile22.bmp

\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile21.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile20.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile19.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile18.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile17.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile16.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile15.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile14.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile13.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile12.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile11.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile10.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\user.bmp
\\?\C:\Users\All Users\Microsoft\User Account Pictures\guest.bmp
\\?\C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSS00005.log
\\?\C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSS.log
\\?\C:\Users\All Users\Microsoft\RAC\StateData\RacWmiEventData.dat
\\?\C:\Users\All Users\Microsoft\RAC\StateData\RacWmiDataBookmarks.dat
\\?\C:\Users\All Users\Microsoft\RAC\StateData\RacMetaData.dat
\\?\C:\Users\All Users\Microsoft\Network\Downloader\qmgr1.dat
\\?\C:\Users\All Users\Microsoft\Network\Downloader\qmgr0.dat
\\?\C:\Users\All Users\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\en-US\resource.xml
\\?\C:\Users\All Users\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\tasks.xml
\\?\C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\en-US\resource.xml
\\?\C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\tasks.xml
\\?\C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\resource.xml
\\?\C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png
\\?\C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\behavior.xml
\\?\C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png
\\?\C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png
\\?\C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png
\\?\C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png
\\?\C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\behavior.xml
\\?\C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png
\\?\C:\Recovery\ed766916-0fa0-11e5-94d0-b217c66646b5\Winre.wim

OpenRegisteryKey

SOFTWARE\Microsoft\BidInterface\Loader
SOFTWARE\ODBC\ODBC.INI\ODBC
Options
Software\Microsoft\Windows\CurrentVersion\Wordpad\COMChecks
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
Ribbon
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
Segoe UI
Tahoma
SYSTEM\CurrentControlSet\Control\MiniNt
Arial
Arial Black
Calibri
SOFTWARE\System32\Configuration\

CreateMutex

Local\WinSpl64To32Mutex_1a0e8_0_3000
<NULL>

OpenMutex

Local\MSCTF.Asm.MutexDefault1

CreateProcess

C:\Windows\splwow64.exe 12288

LoadLibrary

C:\Windows\system32\odbcint.dll
MSVCRT.DLL
ADVAPI32.dll
propsys.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
C:\Windows\System32\msxml3r.dll
MSFTEDIT.DLL
WINSPOOL.DRV
API-MS-Win-Security-SDDL-L1-1-0.dll
RPCRT4.dll
winspool.drv
COMCTL32.DLL
ole32.dll
OLEACCRC.DLL
OLEAUT32.DLL
OLEAUT32.dll
msls31.dll
UxTheme.dll
comctl32.dll
IMM32.dll
Comctl32.dll
UIRibbonRes.dll
C:\Windows\system32\UIRibbon.dll
UXTHEME.DLL
dwmapi.dll
PROPSYS.dll
C:\Windows\System32\msxml6r.dll
C:\Windows\system32\fms.dll
USP10.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
ntmarta.dll
SHELL32.dll
imageres.dll
Ntdll.dll

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Uninstaller FP Detector	2017-05-02 21:44:52 UTC	No Match		No match.
Yara Rule Static Malware Detector	2017-05-02 21:44:52 UTC	No Match		No match.
Static Precise PUA Detector 1	2017-05-02 21:44:52 UTC	No Match		NotDetected
Static Precise Virus Detector	2017-05-02 21:44:52 UTC	No Match		NotDetected
Static Precise Trojan Detector	2017-05-02 21:44:52 UTC	No Match		NotDetected
Malicious Url Detector	2017-05-02 21:45:16 UTC	No Match		No match.

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2020-11-05 15:53:00 UTC
Analysis End Date: 2020-11-05 15:54:20 UTC
File Upload Date: 2020-11-05 15:17:12 UTC
Human Expert Analyst Feedback:
Verdict: Malware
Malware Family:

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x590844B4 [Tue May 2 08:35:00 2017 UTC]
Entry Point	0x401030 (.text)
File Size	1347584
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	Copyright \xa9 2012
Internal Name	java-rmi
File Version	7.0.40.20
Full Version	1.7.0_04-b20
Company Name	Oracle Corporation
Product Name	Java(TM) Platform SE 7 U4
Product Version	7.0.40.20
File Description	Java(TM) Platform SE binary
Original Filename	java-rmi.exe
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	f441a63249cf73224f1c8f15968ff1cb4765d36b71ee4ea69b7973ce08b6cacf

File Paths

FILE PATH ON CLIENT	SEEN COUNT
b84215267063427cf01b086a9595901d12fb3fe5	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2f549	0x2f600	5.028113	-
.rdata	0x31000	0x1189f0	0x118a00	7.106245[SUSPICIOUS]	-
.data	0x14a000	0x164	0x200	2.074694	-
.rsrc	0x14b000	0x93988	0xa00	4.610830	-