VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: bf352825a70685039401abde5daf1712fd968d6eee233ea72393cbc6faffe5a2.bin
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 949f1903642e72575e107ee492faba670c8e0006
MD5: 5384f752e3a2b59fad9d0f143ce0215a
First Seen Date: 2015-11-06 21:18:52 UTC
Number of Clients Seen: 13
Last Analysis Date: 2019-08-25 10:06:23 UTC
Human Expert Analysis Date: 2019-08-25 10:05:03 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2019-08-25 10:06:23 UTC	Malware	
Static Analysis Overall Verdict	2019-08-25 10:06:23 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2019-08-25 10:06:23 UTC	Highly Suspicious	
Human Expert Analysis Overall Verdict	2019-08-25 10:05:03 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	
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	
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	
Packer detection on signature database	Unknown	
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	

Anti-debug calls

- UnhandledExceptionFilter
- IsDebuggerPresent
- OutputDebugStringW

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	
Uses a function clandestinely	
Has no visible windows	

Behavioral Information

CreateFile

C:\Users\win7\AppData\Local\Temp\Autodesk-WebInstall3StubGUI-execution.log
C:\Windows\system32\rsaenh.dll
C:\sample
\\.\Nsi
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C46E7B0F942663A1EDC8D9D6D7869173_6043FC604A395E1485AF7AC16D16B7CE
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C46E7B0F942663A1EDC8D9D6D7869173_DF4CA81DC775CDA9B3214BDB5B55900E
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\40C68D5626484A90937F0752C8B950AB
C:\
C:\Windows
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\win7\AppData\Local\Temp\nseBE2B.tmp\System.dll
C:\sample.config
C:\Users\win7\AppData\Local\Temp\toolbar_log.txt
1.215.2481.0_TO_1.215.2627.0_MPASDLTA.VDM._P
1.215.2481.0_TO_1.215.2627.0_MPAVDLTA.VDM._P
C:\Windows\Fonts\staticcache.dat
C:\Users\win7\AppData\Local\Temp\is-S66P9.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-S66P9.tmp_isetup_shfoldr.dll
C:\Users\desktop.ini
C:\Users
C:\Users\win7
C:\Users\win7\AppData
C:\Users\win7\AppData\Local\Zemana\Tracer\sample.trace
C:\Users\win7\AppData\Local\Temp\{882A187A-D51F-4652-9FB0-2AF3C9A36DCB}.cat
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8890A77645B73478F5B1DED18ACBF795_E1EDEF0C21AE75D448F7327475DF4C9E
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8890A77645B73478F5B1DED18ACBF795_DEE69D93E594A5FDFDC011ECAA8298A2
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2659C1A560AB92C9C29D4B2B25815AE8
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0270780F846F08BEFE0DD8112D932FEF
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3781B4A3713292956206932165FA4132_EEDF05831C87F45FF7C351C81E35FA0B
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3781B4A3713292956206932165FA4132_858B41199908939D4057DA237C57D76D
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5781E92BE36651A8ED64685F2F3CF507
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B3342430143A0BE2B139C3444FED0820
C:\Windows\System32\ntdll.dll
1.215.2624.0_TO_1.215.2653.0_MPASDLTA.VDM._P
1.215.2624.0_TO_1.215.2653.0_MPAVDLTA.VDM._P
C:\Windows\Temp\IntelChip\Chipins.log
config.json
C:\ucbrowsermd.pak
C:\Users\win7\AppData\Local\Temp\is-NRR02.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-NRR02.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-5FTD6.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-5FTD6.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\jusched.log
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\mbahost.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\es\AdguardInstaller.resources.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\sr\AdguardInstaller.resources.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\BootstrapperCore.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\mbapreq.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\mbapreq.thm

C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\mbapreq.png
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1028\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1029\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1030\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1031\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1032\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1035\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1036\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1038\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1040\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1041\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1042\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1043\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1044\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1045\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1046\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1049\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1051\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1053\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1055\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\1060\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\2052\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\2070\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\3082\mbapreq.wxl
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\AdguardInstaller.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\BootstrapperCore.config
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\ru\AdguardInstaller.resources.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\de\AdguardInstaller.resources.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\pt\AdguardInstaller.resources.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\ja\AdguardInstaller.resources.dll
C:\Users\win7\AppData\Local\Temp\{9c620124-6fbe-49a4-9bd3-0a4457f57dc4}\.ba1\BootstrapperApplicationData.xml
C:\Users\win7\AppData\Local\Temp\Adguard_20160323194515.log
\\.\pipe\BurnPipe.{344CDA8B-C287-4C0F-9A91-76227F5A80C1}
C:\Users\win7\AppData\Local\Temp\Setup_20160323194515_Failed.txt
\\.\PIPE\wkssvc
C:\C:\sample
C:\Users\win7\AppData\Local\Temp\ptn47AC.tmp
C:\Users\win7\AppData\Local\Temp\is-UAE11.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-UAE11.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-UAE11.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\CR_7CD65.tmp\CHROME_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\CR_7CD65.tmp\SETUP_PATCH.PACKED.7Z
C:\Windows\system32\en-US\erofflps.txt
C:\Users\win7\AppData\Local\Temp\WERDE6A.tmp.WERInternalMetadata.xml
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\05DB87D2AB058205E5452E4516D5631B
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3151BAC9462B3E2DEE2326609B77DE7E
C:\Users\win7\AppData\Local\Temp\CR_49B0D.tmp\CHROME_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\CR_49B0D.tmp\SETUP_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\IconCache.db
\??\C:\Windows\system32\EhStorShell.dll
\??\C:\Windows\system32\ntshrui.dll
\\.\PIPE\srvsvc
C:\Users\win7\AppData\Local
C:\Users\win7\AppData\Local\Microsoft
C:\Users\win7\AppData\Local\Microsoft\Windows
C:\Users\win7\AppData\Local\Microsoft\Windows\History\desktop.ini
C:\Users\win7\AppData\Roaming
C:\Users\win7\AppData\Roaming\Microsoft\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft
C:\Users\win7\AppData\Roaming\Microsoft\Windows
C:\Users\win7\Favorites\desktop.ini

LoadLibrary

comctl32.dll
KERNEL32.DLL
ADVAPI32.dll
bcrypt.dll
credui.dll
CRYPT32.dll
dwmapi.dll
GDI32.dll
gdiplus.dll
ole32.dll

OLEAUT32.dll
SHELL32.dll
SHLWAPI.dll
USER32.dll
UxTheme.dll
WINHTTP.dll
WINTRUST.dll
uxtheme.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
CRYPTSP.dll
CRYPTBASE.dll
WINTRUST.DLL
C:\Windows\syswow64\CRYPT32.dll
imagehlp.dll
ncrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
USERENV.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
cryptnet.dll
C:\Windows\system32\cryptnet.dll
SensApi.dll
winhttp.dll
WS2_32.dll
kernel32.dll
SspiCli.dll
RPCRT4.dll
IPHLPAPI.DLL
ntdll.dll
NSI.dll
CFGMGR32.dll
API-MS-WIN-Service-Management-L1-1-0.dll
API-MS-WIN-Service-Management-L2-1-0.dll
API-MS-WIN-Service-winsvc-L1-1-0.dll
profapi.dll
DNSAPI.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
C:\sample
SHFOLDER
propsys.dll
ntmarta.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
C:\Users\win7\AppData\Local\Temp\nseBE2B.tmp\System.dll
C:\Windows\system32\kernel32.dll
C:\netcore.dll
IMM32.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL
C:\Users\win7\AppData\Local\Temp\is-A0HQA.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-A0HQA.tmp\sample.EN
imm32.dll
shell32.dll
C:\Users\win7\AppData\Local\Temp\is-S66P9.tmp_isetup_shfoldr.dll
shfolder.dll
Rstrtmgr.dll
C:\Windows\system32\imageres.dll
C:\Windows\system32\shell32.dll
C:\Windows\system32\shlwapi.dll
ADVAPI32.DLL
COMCTL32.DLL
COMDLG32.DLL
CRYPT32.DLL
DHCPCSVC.DLL
DNSAPI.DLL
FLTLIB.DLL
GDI32.DLL
IMAGEHLP.DLL
NETAPI32.DLL
NTDLL.DLL
OLE32.DLL
PSAPI.DLL
SFC.DLL
SHELL32.DLL
URLMON.DLL
USER32.DLL
USERENV.DLL
VERSION.DLL
WINHTTP.DLL

WININET.DLL
WINMM.DLL
WINSPOOL.DRV
WS2_32.DLL
WTSAPI32.DLL
BTHPROPS.DLL
BLUETOOTHAPIS.DLL
MSIMG32.DLL
IMM32.DLL
SETUPAPI.DLL
DWMAPI.DLL
UXTHEME.DLL
WINDOWSCODECS.DLL
WINSTA.dll
FaultRep.dll
olepro32.dll
security.dll
C:\Windows\syswow64\CRYPT32.DLL
Instngin.dll
api-ms-win-core-synch-l1-2-0
kernel32
api-ms-win-core-fibers-l1-1-1
advapi32
api-ms-win-core-localization-l1-2-1
api-ms-win-appmodel-runtime-l1-1-1
ext-ms-win-kernel32-package-current-l1-1-0
C:\PYTHON27.DLL
pythondll
imageres.dll
C:\Users\win7\AppData\Local\Temp\is-3QKG2.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-3QKG2.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-NRR02.tmp_isetup_shfoldr.dll
C:\Windows\SysWOW64\ProfMan64.dll
C:\Users\win7\AppData\Local\Temp\is-5FTD6.tmp_isetup_shfoldr.dll
Kernel32.dll
RICHED20.DLL
0x1b42003c.d
Secur32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
advapi32.dll
C:\Windows\system32\AdvApi32.dll
C:\Windows\system32\Msi.dll
C:\Windows\System32\msxml3r.dll
feclient.dll
cscapi.dll
user32.dll
Shlwapi.dll
gdi32.dll
msimg32.dll
oleaut32.dll
version.dll
winspool.drv
wlanapi.dll
wsock32.dll
C:\Users\win7\AppData\Local\Temp\is-UAE11.tmp_isetup_shfoldr.dll
C:\Windows\system32\wer.dll
C:\Windows\syswow64\KERNELBASE.dll
werui.dll
DUI70.dll
Comctl32.dll
DUser.dll
C:\Windows\system32\DUser.dll
C:\Windows\system32\RICHED20.DLL
C:\Windows\system32\xmllite.dll
secur32.dll
shlwapi.dll
Userenv.dll
WindowsCodecs.dll
C:\Windows\system32\EhStorShell.dll
C:\Windows\system32\ntshrui.dll
srvcli.dll
slc.dll
c:\windows\system32\imageres.dll
C:\Windows\system32\IconCodecService.dll
Mpr.dll
netutils.dll

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2019-08-25 09:16:08 UTC
Analysis End Date: 2019-08-25 10:05:03 UTC
File Upload Date: 2019-08-25 05:25:32 UTC
Human Expert Analyst Feedback:
Verdict: Malware
Malware Family: Trojware
Malware Type: 0

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x55A94114 [Fri Jul 17 17:53:24 2015 UTC]
Entry Point	0x42e44b (.text)
File Size	319488
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	(C) Panasonic and TRENDY Co.
Internal Name	SDFormatter
File Version	4, 0, 0, 0
Company Name	TRENDY Corporation
Private Build	TRENDY Corporation
Comments	SD Formatter Version 3.1.0.0
Product Name	SD Formatter V4.0.0.0
Special Build	TRENDY Corporation
Product Version	4, 0, 0, 0
File Description	Format Tool for SD Card [Normal Area Only]
Original Filename	SDFormatter.exe
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	bf352825a70685039401abde5daf1712fd968d6eee233ea72393cbc6faffe5a2

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x3bf14	0x3c000	6.435844	-
.rdata	0x3d000	0x2458	0x3000	4.185112	-
.data	0x40000	0x6490	0x4000	1.722991	-
.rsrc	0x47000	0xa000	0xa000	5.135115	-