VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: ComIntRep.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 23c180464f580dd24fc9c20557a06713a423b81b
MD5: ec54f7e5602874e387815b1f5ea5b959
First Seen Date: 2017-12-03 11:11:31 UTC
Number of Clients Seen: 3
Last Analysis Date: 2017-12-03 11:11:31 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	2017-12-03 11:11:31 UTC	Clean	
Static Analysis Overall Verdict	2017-12-03 11:11:31 UTC	No Threat Found	
Precise Detectors Overall Verdict	2017-12-03 11:11:31 UTC	No Match	
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	Suspicious	
Timestamp value suspicious	Clean	
Header Checksum is zero!	Suspicious	
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Suspicious	
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

UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus & Laszlo [overlay]

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

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

Behavioral Information

LoadLibrary

KERNEL32.DLL
ADVAPI32.dll
COMCTL32.dll
COMDLG32.dll
GDI32.dll
IPHLPAPI.DLL
MPR.dll
ole32.dll
OLEAUT32.dll
PSAPI.DLL
SHELL32.dll
USER32.dll
USERENV.dll
UxTheme.dll
VERSION.dll
WININET.dll
WINMM.dll
WSOCK32.dll
kernel32.dll
C:\ComIntRep.exe
comctl32.dll
IMM32.dll
gdi32.dll
shell32.dll
user32.dll
msimg32.dll
imageres.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL
propsys.dll
C:\Windows\SysWOW64\ieframe.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
urlmon.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
PROPSYS.dll
iertutil.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
ntdll.dll
DUser.dll
C:\Windows\system32\DUser.dll
dwmapi.dll
C:\Windows\system32\xmllite.dll

CreateProcess

"C:\Program Files\Internet Explorer\iexplore.exe" https://goo.gl/BWhZ4G

ReadFile

C:\Windows\Fonts\staticcache.dat

OpenMutex

Local\MSCTF.Asm.MutexDefault1

CreateMutex

Complete Internet Repair 5 : Build 3793 : 32-Bit
<NULL>

QueryFilePath

C:\ComIntRep.exe
C:\Windows\system32\DUser.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\syswow64\MSCTF.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Windows\syswow64\shlwapi.DLL

OpenRegistryKey

HKEY_CURRENT_USERControl Panel\Mouse
HKEY_CURRENT_USERSoftware\Policies\Microsoft\Internet Explorer\TabbedBrowsing
HKEY_LOCAL_MACHINESoftware\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINESoftware\Microsoft\Internet Explorer\Main
HKEY_CURRENT_USERSoftware\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_CURRENT_USERSoftware\Policies\Microsoft\Internet Explorer\Main
HKEY_CURRENT_USERSoftware\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINESoftware\Microsoft\Internet Explorer\TabbedBrowsing
HKEY_CURRENT_USERSoftware\Microsoft\Internet Explorer\Main
HKEY_CURRENT_USERSoftware\Policies\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINESoftware\Policies\Microsoft\Internet Explorer\TabbedBrowsing
HKEY_CURRENT_USERSoftware\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINESoftware\Policies\Microsoft\Internet Explorer\Main
HKEY_LOCAL_MACHINESoftware\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINESoftware\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_CURRENT_USERSoftware\AutoIt v3\AutoIt
HKEY_LOCAL_MACHINESoftware\Policies\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_CURRENT_USERSoftware\Microsoft\Internet Explorer\TabbedBrowsing

QueryProcessAddress

GetAsyncKeyState
OpenProcess
ReadProcessMemory
WriteProcessMemory
CreateProcessW
InternetReadFile
ShellExecuteExW
ShellExecuteW
IsDebuggerPresent

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2017-12-03 11:11:13 UTC	No Match	NotDetected
Static Precise Virus Detector	2017-12-03 11:11:13 UTC	No Match	NotDetected
Static Precise Trojan Detector	2017-12-03 11:11:13 UTC	No Match	NotDetected
Static Precise Adware InstallCore Detector 1	2017-12-03 11:11:13 UTC	No Match	NotDetected
Static Precise Trojan Detector 2	2017-12-03 11:11:13 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2017-12-03 11:11:13 UTC	No Match	NotDetected
Static Precise Trojan Generic Cryptor Detector 1	2017-12-03 11:11:13 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2017-12-03 11:11:13 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5A22DC53 [Sat Dec 2 17:01:07 2017 UTC]
Debug Artifacts	
Entry Point	0x5ec9a0 (UPX1)
Exifinfo	[object Object]
File Size	1209856
File Type Enum	6
Imphash	712f4a29c405ecb576101d367b2180fb
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	\xa9 2018 Rizonesoft
File Version	5.0.0.3793
Company Name	Rizonesoft
Comments	Complete Internet Repair
Product Name	Complete Internet Repair
Product Version	5
File Description	Complete Internet Repair
Home Page	https://www.rizonesoft.com
Auto It Version	3.3.15.0
Translation	0x0809 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	6a9125e1e52c5699c5c29a4b0587455353ceb1b151de6fd0dcafcf0b1dd84b60
Ssdeep	24576:kj8B3KleKsb0SIieVHUAwWfrL6lApdwqLKjkWEY6ulRsI+QNI:qw3KL5imHUD0H6lApKq2kWEGRsNQN
Trid	64.2,UPX compressed Win32 Executable,15.6,Win32 Dynamic Link Library (generic),10.6,Win32 Executable (generic),4.7,Generic Win/DOS Executable,4.7,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0xf6000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0xf7000	0xf6000	0xf5c00	7.85938090021	1537bf8a3067d5f5925f24a3c5f782ff
.rsrc	0x1ed000	0x32000	0x31600	6.55314509825	2117939d87d6edf1abb0bf3a7e2575ff