VALKYRIE

**CLEAN**
Valkyrie Final Verdict

**File Name:** PQACQWRECMYCOcaTgH.exe.xBAD
**File Type:** PE32 executable (GUI) Intel 80386, for MS Windows
**SHA1:** ecd328e049e23c9a826505335c0e2b9f64e7ec5e
**MD5:** 6cf9a0d989715773d49d5ff3ad601db3
**First Seen Date:** 2016-01-12 11:05:04 UTC
**Number of Clients Seen:** 12
**Last Analysis Date:** 2016-01-25 13:29:23 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 | 2016-01-25 13:29:23 UTC | Clean | ✓ |
| Static Analysis Overall Verdict | 2016-01-25 13:29:23 UTC | Highly Suspicious | ! |
| Dynamic Analysis Overall Verdict | 2016-01-25 13:29:23 UTC | No Threat Found | ? |
| File Certificate Validation | | Certificate Not Valid,Vendor name Valid | ? |

## 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 | ✓ |
| 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**

- TerminateProcess
- Process32FirstW
- Process32NextW
- OutputDebugStringW
- IsDebuggerPresent
- UnhandledExceptionFilter

FindWindowExW
FindWindowW
GetWindowThreadProcessId

## Dynamic Analysis

| DYNAMIC ANALYSIS OVERALL VERDICT | RESULT |
|---|---|
| No Threat Found | |

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

## Behavioral Information

### LoadLibrary

msctf.dll
MsftEdit.dll
C:\Windows\system32\EhStorShell.dll
comctl32.dll
propsys.dll
IMM32.dll
CRYPTBASE.dll
USER32.dll
C:\Windows\system32\ntshrui.dll
C:\Windows\System32\imageres.dll
ole32.dll
OLEAUT32.DLL
SHELL32.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
C:\Windows\system32\mssvp.dll
C:\msfte.dll
C:\Windows\system32\xmllite.dll
PROPSYS.dll
c:\windows\system32\imageres.dll
C:\msTracer.dll
ntdll.dll
DUser.dll
ADVAPI32.dll
C:\Windows\System32\davclnt.dll
srvcli.dll
dwmapi.dll
uxtheme.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
shell32.dll
kernel32.dll
C:\Windows\System32\ntlanman.dll
netutils.dll
C:\Windows\system32\VBoxMRXNP.dll
WindowsCodecs.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
WINTRUST.dll
C:\Windows\system32\networkexplorer.dll
C:\Windows\System32\drprov.dll
cscapi.dll
OLEAUT32.dll
UxTheme.dll
Comctl32.dll
msls31.dll
RPCRT4.dll
C:\Windows\system32\DUser.dll
C:\Windows\syswow64\MSCTF.dll
ntmarta.dll
user32.dll
slc.dll

explorerframe.dll
C:\Windows\system32\imageres.dll
C:\Windows\System32\ShellStyle.dll
C:\Windows\system32\ole32.dll

### LowerChar

.library-ms
a

### ReadRegisteryKey

Plane4
Plane8
DataFilePath
Plane2
Plane11
Plane15
Plane3
PreventIndexingOfflineFiles
<NULL>
Plane7
Plane10
Plane14
Disable
SwapMouseButtons
Plane6
Plane13
Plane5
Plane9
Plane12
Plane1
Plane16

### CreateFile

C:\Users\win7\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini
C:\Users\desktop.ini
C:\Users\win7\Favorites\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms
C:\Users\Public\Documents\My Videos\desktop.ini
C:\Users\win7\Documents\My Music\desktop.ini
\??\C:\Windows\system32\mssvp.dll
C:\Users\win7\Documents
C:\Windows\Fonts\staticcache.dat
\\.\PIPE\wkssvc
C:\Users\Public\Desktop
\\.\PIPE\srvsvc
C:\Users\Public\Videos\desktop.ini
C:\Users\win7\Documents\My Pictures\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms
C:\Users\Public
C:\Users\win7\Videos\desktop.ini
\\.\PIPE\DAV RPC SERVICE
C:\Users\Public\Documents\My Pictures\desktop.ini
\\.\VBoxGuest
\??\C:\Windows\system32\EhStorShell.dll
C:\Users\win7\AppData\Roaming\Microsoft\Windows
\\.\VBoxMiniRdrDN
C:\Users\win7\Desktop
C:\Users\win7\Downloads\desktop.ini
C:\Users
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms
C:\Users\win7
C:\Users\win7\Links\desktop.ini
C:\Users\win7\Links
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Network Shortcuts
C:\Users\win7\Documents\My Videos\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft

C:\Users\win7\AppData
C:\Windows\system32\rsaenh.dll
C:\Users\win7\AppData\Roaming
\??\C:\Windows\system32\NetworkExplorer.dll
C:\Users\win7\Links\Downloads.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Network Shortcuts\desktop.ini
C:\Users\win7\Links\RecentPlaces.lnk
C:\Users\Public\Documents\My Music\desktop.ini
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db
C:\
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Libraries
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
\??\C:\Windows\system32\ntshrui.dll
C:\Users\win7\Links\Desktop.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms
C:\Users\Public\Documents

**OpenRegisteryKey**

SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
Software\Microsoft\Windows\CurrentVersion\PropertySystem\PropertyHandlers\.library-ms
Segoe UI
Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap
SOFTWARE\Microsoft\Windows\Windows Search\Preferences
SOFTWARE\Policies\Microsoft\Windows\Windows Search
Software\AutoIt v3\AutoIt
Marlett
System
Tahoma
Software\Microsoft\Windows\CurrentVersion\PropertySystem\PropertyHandlers\.ini
Software\Microsoft\Windows Search
Control Panel\Mouse
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0

**CreateMutex**

Local\ShellCMruPidlList
Local\SHResolveLibrary:C:/Users/win7/AppData/Roaming/Microsoft/Windows/Libraries/Documents.library-ms
<NULL>

**OpenMutex**

Local\MSCTF.Asm.MutexDefault1
DefaultTabtip-MainUI

**QueryFilePath**

C:\sample
C:\Windows\syswow64\SHELL32.dll
C:\Windows\system32\EhStorShell.dll
C:\Windows\system32\ntshrui.dll
C:\Windows\system32\explorerframe.dll
C:\Windows\system32\MsftEdit.dll
C:\Windows\syswow64\MSCTF.dll
C:\Windows\system32\PROPSYS.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\system32\ieframe.DLL
C:\Windows\syswow64\shlwapi.DLL
C:\Windows\system32\DUser.dll
C:\Windows\syswow64\COMDLG32.dll
C:\Windows\system32\SearchFolder.dll

## Precise Detectors Analysis Results

No Detector Result Received

## Advance Heuristics

No Advanced Heuristic Analysis Result Received

## Additional File Information

**Vendor Validation** - Verified ✔

**[+] AutoIt Consulting Ltd**

| | |
|---|---|
| Status | Valid ✔ |

**Certificate Validation** - undefined ✖

**[+] undefined**

| | |
|---|---|
| Status | undefined ✖ |
| Start Date | 1998-09-01 12:00:00 |
| End Date | 2028-01-28 12:00:00 |
| Sha256 | undefined |
| Serial | undefined |
| Subject Key Identifier | undefined |
| Issuer Name | undefined |
| Issuer Key Identifier | undefined |
| Crl link | undefined |
| Key Usage | undefined |
| Extended Usage | undefined |

**[+] undefined**

| | |
|---|---|
| Status | undefined ✖ |
| Start Date | 1999-01-28 13:00:00 |
| End Date | 2017-01-27 12:00:00 |
| Sha256 | undefined |
| Serial | undefined |
| Subject Key Identifier | undefined |
| Issuer Name | undefined |
| Issuer Key Identifier | undefined |
| Crl link | undefined |
| Key Usage | undefined |
| Extended Usage | undefined |

**[+] undefined**

| | |
|---|---|
| Status | undefined ✖ |
| Start Date | 2009-03-18 11:00:00 |
| End Date | 2028-01-28 12:00:00 |
| Sha256 | undefined |
| Serial | undefined |
| Subject Key Identifier | undefined |
| Issuer Name | undefined |
| Issuer Key Identifier | undefined |
| Crl link | undefined |
| Key Usage | undefined |
| Extended Usage | undefined |

**[+] undefined**

| | |
|---|---|
| Status | undefined ✖ |
| Start Date | 2009-12-21 09:32:56 |
| End Date | 2020-12-22 09:32:56 |
| Sha256 | undefined |
| Serial | undefined |
| Subject Key Identifier | undefined |
| Issuer Name | undefined |
| Issuer Key Identifier | undefined |
| Crl link | undefined |
| Key Usage | undefined |
| Extended Usage | undefined |

**[+] undefined**

| | |
|---|---|
| Status | undefined ✖ |
| Start Date | 2011-05-25 09:43:07 |
| End Date | 2014-05-25 09:43:05 |
| Sha256 | undefined |
| Serial | undefined |
| Subject Key Identifier | undefined |
| Issuer Name | undefined |
| Issuer Key Identifier | undefined |
| Crl link | undefined |
| Key Usage | undefined |
| Extended Usage | undefined |

**[+] undefined**

| | |
|---|---|
| Status | undefined ✖ |
| Start Date | 2004-01-22 10:00:00 |
| End Date | 2017-01-27 10:00:00 |
| Sha256 | undefined |
| Serial | undefined |
| Subject Key Identifier | undefined |
| Issuer Name | undefined |
| Issuer Key Identifier | undefined |
| Crl link | undefined |
| Key Usage | undefined |
| Extended Usage | undefined |

### PE Headers

| PROPERTY | VALUE |
|---|---|
| Compilation Time Stamp | 0x4EF45F13 [Fri Dec 23 10:59:31 2011 UTC] |
| Entry Point | 0x4164e1 (.text) |
| File Size | 750320 |
| Machine Type | Intel 386 or later - 32Bit |
| Legal Copyright | \xa91999-2011 Jonathan Bennett & AutoIt Team |
| Internal Name | AutoIt3.exe |
| File Version | 3, 3, 8, 0 |
| Company Name | AutoIt Team |
| Comments | http://www.autoitscript.com/autoit3/ |
| Product Name | AutoIt v3 Script |
| Product Version | 3, 3, 8, 0 |
| File Description | AutoIt v3 Script |
| Original Filename | AutoIt3.exe |
| Translation | 0x0809 0x04b0 |
| Mime Type | application/x-dosexec |
| Number Of Sections | 5 |
| Sha256 | 0984d3bc6ce07e701241aa785fa057e8bba7eb2503a5bef726a06a8bd2d2f349 |

### File Paths

| FILE PATH ON CLIENT | SEEN COUNT |
|---|---|
| ecd328e049e23c9a826505335c0e2b9f64e7ec5e | 1 |

### PE Sections

| NAME | VIRTUAL ADDRESS | VIRTUAL SIZE | RAW SIZE | ENTROPY | MD5 |
|---|---|---|---|---|---|
| .text | 0x1000 | 0x805d8 | 0x80600 | 6.686522 | - |
| .rdata | 0x82000 | 0xdfa8 | 0xe000 | 4.797287 | - |
| .data | 0x90000 | 0x1a758 | 0x6800 | 2.154233 | - |
| .rsrc | 0xab000 | 0x18a9c | 0x18c00 | 7.345484[SUSPICIOUS] | - |
| .reloc | 0xc4000 | 0x758a | 0x7600 | 6.241861 | - |