VALKYRIE COMODO

Summary

File Name: af4bd7bf2fd6b49fe817a39e8d8549afa7309c5aa3f06c202fa8fa6812fd6a9b.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

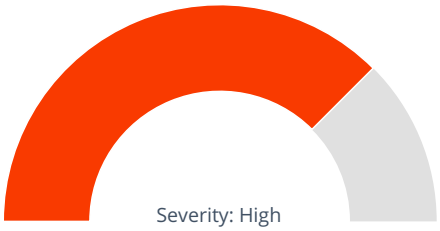
SHA1: 1e3b7d7731853c9d740b133d8771e2c8b15981d0

MD5: 12366ed478b434acf8e79da41ee470ba

MALWARE

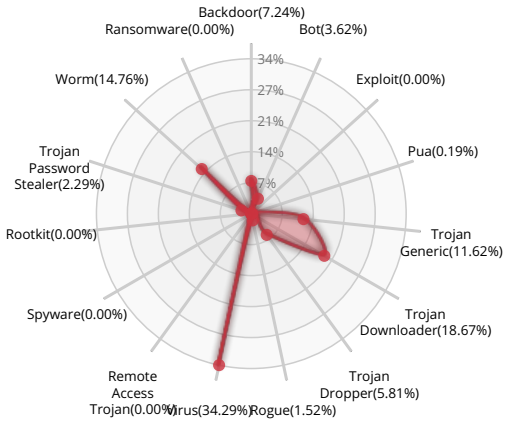
Valkyrie Final Verdict

DETECTION SECTION

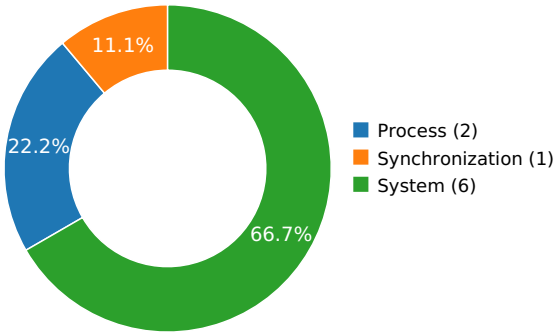


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Packer 1 (100.00%)

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

VALKYRIE COMODO

Behavior Graph

11:25:20 **11:25:20** **11:25:20**

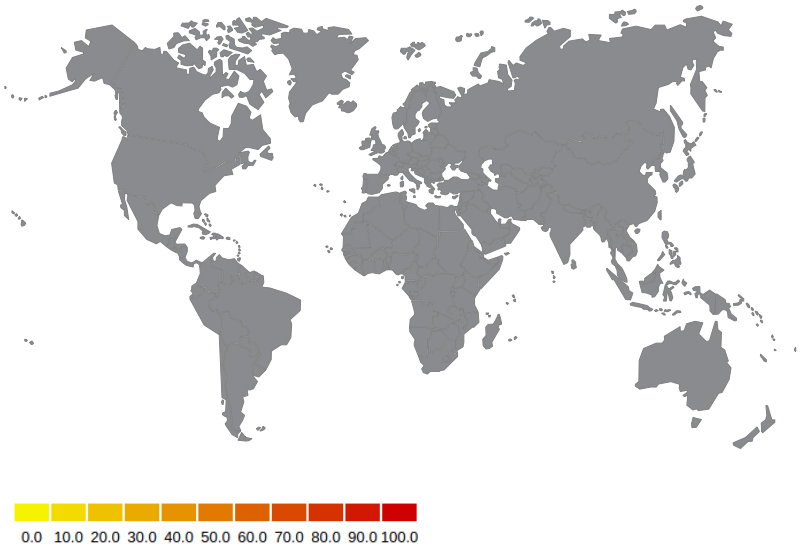
PID 1860

11:25:20	Create Process	The malicious file created a child process as 1e3b7d7731853c9d740b133d8771e2c8b15981d0.exe **(PPID 2576)**

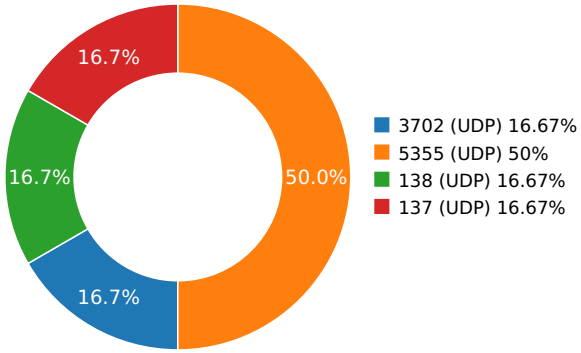
Behavior Summary

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.1290409565	Sandbox	224.0.0.252	5355
3.17897987366	Sandbox	192.168.56.255	137
3.26782393456	Sandbox	224.0.0.252	5355
3.82018780708	Sandbox	239.255.255.250	3702
5.84451293945	Sandbox	224.0.0.252	5355
9.21909999847	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	af4bd7bf2fd6b49fe817a39e8d8549afa7309c5aa3f06c202fa8fa6812fd6a9b.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	1e3b7d7731853c9d740b133d8771e2c8b15981d0
MD5:	12366ed478b434acf8e79da41ee470ba
First Seen Date:	2018-03-14 12:03:46.938791 (10 months ago)
Number Of Clients Seen:	3
Last Analysis Date:	2018-08-07 13:14:38.546618 (5 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'winmine.pdb\x00', u'GUID': u'{----}', u'timestamp': u'2001-08-17 20:54:13'}]
Number Of Sections	4
Trid	[[38.4, u'Win32 Dynamic Link Library (generic)'], [26.3, u'Win32 Executable (generic)'], [11.8, u'OS/2 Executable (generic)'], [11.6, u'Generic Win/DOS Executable'], [11.6, u'DOS Executable Generic']]
Compilation Time Stamp	0x3B7D8475 [Fri Aug 17 20:54:13 2001 UTC]
LegalCopyright	\xa9 Microsoft Corporation. All rights reserved.
InternalName	winmine
FileVersion	5.1.2600.0 (xpclient.010817-1148)
CompanyName	Microsoft Corporation
ProductName	Microsoft\xae Windows\xae Operating System
ProductVersion	5.1.2600.0
FileDescription	Entertainment Pack Minesweeper Game
OriginalFilename	WINMINE.EXE
Translation	0x0409 0x04b0
Entry Point	0x1003e21 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	222207
Ssdeep	
Sha256	af4bd7bf2fd6b49fe817a39e8d8549afa7309c5aa3f06c202fa8fa6812fd6a9b
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	de5490f8d3fb044d081bdaec5ef47bf7

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x3a56	0x3c00	6.29731758405	40cd613fa01003bf686400b4d2e2ecfa
.data	0x5000	0xb98	0x200	2.32243046284	9bc83e635ea1cff385de37e1878c7f90
.rsrc	0x6000	0x19160	0x19200	7.20386863791	acc5675296ca0b6b676581df29d5a54c
.udata	0x20000	0x12000	0x12000	0.0	f5d8d2bfbbca26e64933760e2833fd91

PE Imports

- msvcrt.dll
  - _controlfp
  - __set_app_type
  - __p__fmode
  - _except_handler3
  - _adjust_fdiv
  - __setusermatherr
  - _initterm
  - __getmainargs
  - _acmdln
  - exit
  - __p__commode
  - _cexit
  - _XcptFilter
  - _exit
  - _c_exit
  - srand
  - rand
- ADVAPI32.dll
  - RegQueryValueExW
  - RegSetValueExW
  - RegOpenKeyExA
  - RegQueryValueExA
  - RegCreateKeyExW
  - RegCloseKey
- KERNEL32.dll
  - FindResourceW
  - OutputDebugStringA
  - LockResource
  - LoadResource
  - lstrlenW
  - GetPrivateProfileIntW
  - GetPrivateProfileStringW
  - GetTickCount
  - GetModuleFileNameA
  - GetModuleHandleA
  - GetStartupInfoA
  - GetProcAddress
  - lstrcpyW
  - LoadLibraryA
- GDI32.dll
  - SetROP2
  - GetLayout
  - SetLayout
  - GetDeviceCaps
  - DeleteObject
  - LineTo
  - CreatePen
  - CreateCompatibleDC
  - CreateCompatibleBitmap
  - SelectObject
  - SetDIBitsToDevice
  - DeleteDC
  - MoveToEx
  - SetPixel
  - BitBlt
  - GetStockObject
- USER32.dll
  - LoadIconW
  - GetDesktopWindow
  - SetTimer

    - MessageBoxW
    - LoadCursorW
    - CheckMenuItem
    - SetMenu
    - GetDlgItemInt
    - RegisterClassW
    - LoadStringW
    - LoadMenuW
    - ReleaseCapture
    - PeekMessageW
    - MapWindowPoints
    - SetCapture
    - PtInRect
    - WinHelpW
    - SetDlgItemInt
    - EndDialog
    - SetDlgItemTextW
    - wsprintfW
    - SendMessageW
    - GetDlgItem
    - GetDlgItemTextW
    - GetSystemMetrics
    - InvalidateRect
    - SetRect
    - MoveWindow
    - GetMenuItemRect
    - DialogBoxParamW
    - DefWindowProcW
    - ReleaseDC
    - GetDC
    - PostMessageW
    - ShowWindow
    - PostQuitMessage
    - KillTimer
    - EndPaint
    - BeginPaint
    - DispatchMessageW
    - TranslateMessage
    - TranslateAcceleratorW
    - GetMessageW
    - UpdateWindow
    - CreateWindowExW
    - LoadAcceleratorsW
- SHELL32.dll
    - ShellAboutW
- WINMM.dll
    - PlaySoundW
- COMCTL32.dll
    - InitCommonControlsEx

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'WAVE', u'offset': 59072, u'sha256': u'a8689af3b0f5bac05bbee73d90b855ddaee06d9146d1914c053cf4b9102a5bd2', u'type': u'RIFF (little-endian) data, WAVE audio, Microsoft PCM, 8 bit, mono 22050 Hz', u'size': 1360}

{u'lang': u'LANG_ENGLISH', u'name': u'WAVE', u'offset': 60432, u'sha256': u'2394cbf4a4f6a15b5662b1b87a1e3119e474597b407518b47741da193583ad45', u'type': u'RIFF (little-endian) data, WAVE audio, Microsoft PCM, 8 bit, mono 22050 Hz', u'size': 37960}

{u'lang': u'LANG_ENGLISH', u'name': u'WAVE', u'offset': 98392, u'sha256': u'd492324891bbfd582a9d230f5720d1ea65bd06b69e10db5c44ddc7d6b172cc75', u'type': u'RIFF (little-endian) data, WAVE audio, Microsoft PCM, 8 bit, mono 22050 Hz', u'size': 25711}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 50312, u'sha256': u'74ef286c9c4b8a988d32b17f63774ff19d6217f9d69fd2b99515f7f7a52b62df', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 2152}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 52464, u'sha256': u'cb169965853ddcbc71e15da614cf7a518a60a05882c8ecd3eb6fff689822cd6d', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1072}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 53536, u'sha256': u'3c7e4b856fa4497d162adb9f717d8d0a760a3fec28d5328c4f4ad22a52bc9087', u'type': u'data', u'size': 2312}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 55848, u'sha256': u'3a94995ed1b3130136b3a6d7db81a5dd1d62b0b71af1039f3834ff9a0dfaef71', u'type': u'dBase III DBT, version number 0, next free block index 40, 1st item "?\\340"', u'size': 1152}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 57000, u'sha256': u'ac6c04d16861e7869a48a558e7191128ae6679a137d4e9196dca43972f86495f', u'type': u'data', u'size': 1544}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 58544, u'sha256': u'f51a0c1c67c6f9f05016ad364231cdb264bb6593370363d2c878675fa6783619', u'type': u'data', u'size': 528}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 26760, u'sha256': u'44b0905d9ed7bcbbcc5bfb7bdd0343878a9b124eedb393b26a11b874f9d28645', u'type': u'data', u'size': 744}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 27504, u'sha256': u'0b87c2cd01db8f26a8b92729ce78a355d0898ebc0ad4b85bf03964eaf7d04193', u'type': u'data', u'size': 304}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 27808, u'sha256': u'0f25171c9c7793f124dd9e6b67d3c630d8060beb0bc905d77b0b6a8924ce566c', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 31560, u'sha256': u'79652897e765ffd8cf026400a92cb827b394326880f47ad43811ec50b1259ec5', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 33776, u'sha256': u'bf73d7152585afd4336ae5337e2466f77638a97bed28629471e079f84e7464c7', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 35160, u'sha256': u'f0e35e890a2cb17c2862200529eb72f708e93810ab060d809ad70826d37334c5', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 44800, u'sha256': u'd41885e826cd36fe1c353e4a5b5816e9a2f9eac160ca7c1b38818d3021d33b9a', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 49064, u'sha256': u'c493c4248050514b068a5360718447bb68b798a4d323ccab2b2890c77526ed5d', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MENU', u'offset': 125096, u'sha256': u'cc37fbb24d3861d7a6e40a455a16e8ee1e8064dae5cf702538939e0befe0bbce', u'type': u'data', u'size': 452}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 124104, u'sha256': u'2558faafa02d22ef5c462c1aade0f93862e63f9bfea06a6f129cf947971f87f0', u'type': u'data', u'size': 354}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 124464, u'sha256': u'a08f109f40fc406ee3a22dfe8f82c79db56bb5a3dd0783a6e14a25551ac53721', u'type': u'data', u'size': 138}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 124608, u'sha256': u'6bbb8314a9060488fccbcab8ba440157ee7959445d480a94766a7056c54da17b', u'type': u'data', u'size': 482}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 126488, u'sha256': u'5e04341a02252b3abae53c18add725dd88e808194608216efade683627beea92', u'type': u'data', u'size': 838}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ACCELERATOR', u'offset': 125552, u'sha256': u'4d70f07577de089c346c55f126a25487d5110d2ecb58c4dd5da68e8ef8195911', u'type': u'data', u'size': 16}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 50192, u'sha256': u'755a925e9acc2318b084fc4bc7199debfa1de89a7eb86978fd3fb1ee8c5f6fba', u'type': u'MS Windows icon resource - 8 icons, 32x32, 16 colors', u'size': 118}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 125568, u'sha256': u'4d205fbb2dfb8f508c9a222272d77903d70e66da633f7c9d0a6b6ca7752db3c8', u'type': u'data', u'size': 916}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 26096, u'sha256': u'e8fe2be83ac3ca01340215c76809178a31712168144810a63d5613cae031acee', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 661}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS