VALKYRIE COMODO

Summary

File Name: 1710161010_3.exe

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

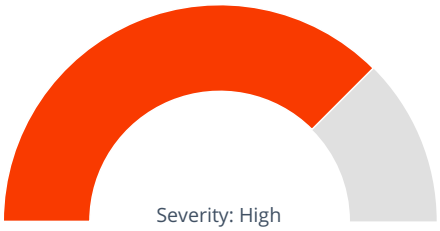
SHA1: 09c069d12e80da48ea79ca786ec7da828fb66530

MD5: c5dadf5a7070a8c1c0dc0dc99dad8b20

MALWARE

Valkyrie Final Verdict

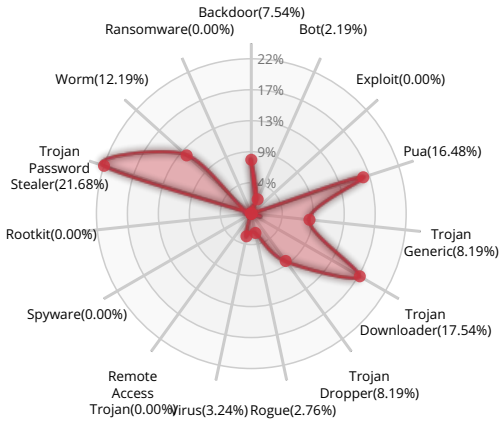
DETECTION SECTION



Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION

ACTIVITY OVERVIEW

Static Anomaly 1 (100.00%)

VALKYRIE COMODO

Activity Details

STATIC ANOMALY

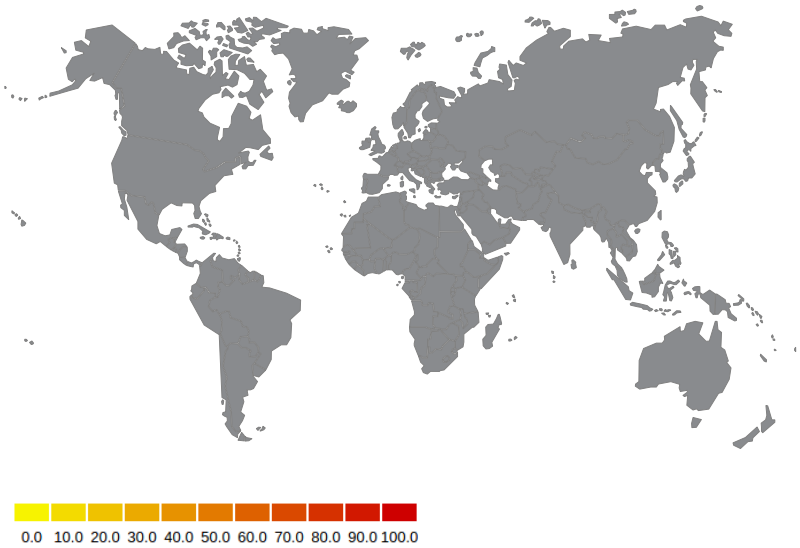
Anomalous binary characteristics Show sources

Behavior Graph

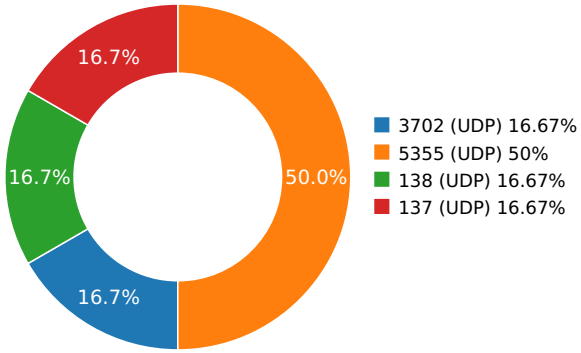
Behavior Summary

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
3.02684998512	Sandbox	224.0.0.252	5355
3.02767682076	Sandbox	224.0.0.252	5355
3.04400777817	Sandbox	239.255.255.250	3702
3.07822084427	Sandbox	192.168.56.255	137
5.57919788361	Sandbox	224.0.0.252	5355
9.07844185829	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:	1710161010_3.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	09c069d12e80da48ea79ca786ec7da828fb66530
MD5:	c5dadf5a7070a8c1c0dc0dc99dad8b20
First Seen Date:	2017-10-28 17:12:13.654687 (about a year ago)
Number Of Clients Seen:	3
Last Analysis Date:	2017-10-28 17:12:13.654687 (about a year ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	8
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
LegalCopyright	Copyright (C) 2000-2016 by Bitvise Limited.
InternalName	stnlc
FileVersion	7.15.0.0
CompanyName	Bitvise Limited
PrivateBuild	
LegalTrademarks	
Comments	
ProductName	Bitvise SSH Client
SpecialBuild	
ProductVersion	7.15
FileDescription	Bitvise SSH Client command line tunneling client
OriginalFilename	stnlc.exe
Translation	0x0409 0x04b0
Entry Point	0x46b96c (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	1922619
Sha256	4d7461333f8e8d012b1cff8c6ed9d241eeef4ddbe5e79607ba1badc5a3f454e4
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x6a9b4	0x6aa00	6.46612533371	910b5c918080886ecf60abfd09dc2564
DATA	0x6c000	0x11d0	0x1200	4.08800656492	cc7b590ce91bdab7a18913abca4b4878
BSS	0x6e000	0x3aed	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x72000	0x20b0	0x2200	4.90905576644	cd0bf39f6e9910778a64648539ce419e
.tls	0x75000	0x10	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x76000	0x18	0x200	0.206920017787	e3bcc4c41b8438a8ab917d7d03e3d5cb
.reloc	0x77000	0x64d0	0x6600	6.63870355493	dfac77862509f7165ee1d2af6502c17b
.rsrc	0x7e000	0xe800	0xe800	4.27795885858	afa63b410b7161472e12cc012a88c417

PE Imports

- kernel32.dll
  - DeleteCriticalSection
  - LeaveCriticalSection
  - EnterCriticalSection
  - InitializeCriticalSection
  - VirtualFree
  - VirtualAlloc
  - LocalFree
  - LocalAlloc
  - GetVersion
  - GetCurrentThreadId
  - InterlockedDecrement
  - InterlockedIncrement
  - VirtualQuery
  - WideCharToMultiByte
  - MultiByteToWideChar
  - lstrlenA
  - lstrcpynA
  - LoadLibraryExA
  - GetThreadLocale
  - GetStartupInfoA
  - GetProcAddress
  - GetModuleHandleA
  - GetModuleFileNameA
  - GetLocaleInfoA
  - GetCommandLineA
  - FreeLibrary
  - FindFirstFileA
  - FindClose
  - ExitProcess
  - WriteFile
  - UnhandledExceptionFilter
  - RtlUnwind
  - RaiseException
  - GetStdHandle
- user32.dll
  - GetKeyboardType
  - LoadStringA
  - MessageBoxA
  - CharNextA
- advapi32.dll
  - RegQueryValueExA
  - RegOpenKeyExA
  - RegCloseKey
- oleaut32.dll
  - SysFreeString
  - SysReAllocStringLen
  - SysAllocStringLen
- kernel32.dll
  - TlsSetValue
  - TlsGetValue
  - LocalAlloc
  - GetModuleHandleA
- advapi32.dll

    - RegQueryValueExA
    - RegOpenKeyExA
    - RegCloseKey
- kernel32.dll
    - lstrcpyA
    - WriteFile
    - WaitForSingleObject
    - VirtualQuery
    - VirtualAlloc
    - Sleep
    - SizeofResource
    - SetThreadLocale
    - SetFilePointer
    - SetEvent
    - SetErrorMode
    - SetEndOfFile
    - ResetEvent
    - ReadFile
    - MulDiv
    - LockResource
    - LoadResource
    - LoadLibraryA
    - LeaveCriticalSection
    - InitializeCriticalSection
    - GlobalUnlock
    - GlobalSize
    - GlobalReAlloc
    - GlobalHandle
    - GlobalLock
    - GlobalFree
    - GlobalFindAtomA
    - GlobalDeleteAtom
    - GlobalAlloc
    - GlobalAddAtomA
    - GetVersionExA
    - GetVersion
    - GetTickCount
    - GetThreadLocale
    - GetSystemInfo
    - GetStringTypeExA
    - GetStdHandle
    - GetProfileStringA
    - GetProcAddress
    - GetModuleHandleA
    - GetModuleFileNameA
    - GetLocaleInfoA
    - GetLocalTime
    - GetLastError
    - GetFullPathNameA
    - GetDiskFreeSpaceA
    - GetDateFormatA
    - GetCurrentThreadId
    - GetCurrentProcessId
    - GetCPInfo
    - GetACP
    - FreeResource
    - InterlockedExchange
    - FreeLibrary
    - FormatMessageA
    - FindResourceA
    - EnumCalendarInfoA
    - EnterCriticalSection
    - DeleteCriticalSection
    - CreateThread
    - CreateFileA
    - CreateEventA
    - CompareStringA
    - CloseHandle
- version.dll
    - VerQueryValueA
    - GetFileVersionInfoSizeA
    - GetFileVersionInfoA
- gdi32.dll
    - UnrealizeObject
    - StretchBlt

    - SetWindowOrgEx
    - SetViewportOrgEx
    - SetTextColor
    - SetStretchBltMode
    - SetROP2
    - SetPixel
    - SetDIBColorTable
    - SetBrushOrgEx
    - SetBkMode
    - SetBkColor
    - SelectPalette
    - SelectObject
    - SaveDC
    - RestoreDC
    - Rectangle
    - RectVisible
    - RealizePalette
    - PatBlt
    - MoveToEx
    - MaskBlt
    - LineTo
    - IntersectClipRect
    - GetWindowOrgEx
    - GetTextMetricsA
    - GetTextExtentPoint32A
    - GetSystemPaletteEntries
    - GetStockObject
    - GetPixel
    - GetPaletteEntries
    - GetObjectA
    - GetDeviceCaps
    - GetDIBits
    - GetDIBColorTable
    - GetDCOrgEx
    - GetCurrentPositionEx
    - GetClipBox
    - GetBrushOrgEx
    - GetBitmapBits
    - ExtTextOutA
    - ExcludeClipRect
    - EndPage
    - EndDoc
    - DeleteObject
    - DeleteDC
    - CreateSolidBrush
    - CreatePenIndirect
    - CreatePalette
    - CreateICA
    - CreateHalftonePalette
    - CreateFontIndirectA
    - CreateDIBitmap
    - CreateDIBSection
    - CreateDCA
    - CreateCompatibleDC
    - CreateCompatibleBitmap
    - CreateBrushIndirect
    - CreateBitmap
    - BitBlt
- user32.dll
    - CreateWindowExA
    - WindowFromPoint
    - WinHelpA
    - WaitMessage
    - UpdateWindow
    - UnregisterClassA
    - UnhookWindowsHookEx
    - TranslateMessage
    - TranslateMDISysAccel
    - TrackPopupMenu
    - SystemParametersInfoA
    - ShowWindow
    - ShowScrollBar
    - ShowOwnedPopups
    - ShowCursor
    - SetWindowsHookExA

- SetWindowTextA
- SetWindowPos
- SetWindowPlacement
- SetWindowLongA
- SetTimer
- SetScrollRange
- SetScrollPos
- SetScrollInfo
- SetRect
- SetPropA
- SetParent
- SetMenuItemInfoA
- SetMenu
- SetForegroundWindow
- SetFocus
- SetCursor
- SetClassLongA
- SetCapture
- SetActiveWindow
- SendMessageA
- ScrollWindow
- ScreenToClient
- RemovePropA
- RemoveMenu
- ReleaseDC
- ReleaseCapture
- RegisterWindowMessageA
- RegisterClipboardFormatA
- RegisterClassA
- RedrawWindow
- PtInRect
- PostQuitMessage
- PostMessageA
- PeekMessageA
- OffsetRect
- OemToCharA
- MessageBoxA
- MapWindowPoints
- MapVirtualKeyA
- LoadStringA
- LoadKeyboardLayoutA
- LoadIconA
- LoadCursorA
- LoadBitmapA
- KillTimer
- IsZoomed
- IsWindowVisible
- IsWindowEnabled
- IsWindow
- IsRectEmpty
- IsIconic
- IsDialogMessageA
- IsChild
- InvalidateRect
- IntersectRect
- InsertMenuItemA
- InsertMenuA
- InflateRect
- GetWindowThreadProcessId
- GetWindowTextA
- GetWindowRect
- GetWindowPlacement
- GetWindowLongA
- GetWindowDC
- GetTopWindow
- GetSystemMetrics
- GetSystemMenu
- GetSysColorBrush
- GetSysColor
- GetSubMenu
- GetScrollRange
- GetScrollPos
- GetScrollInfo
- GetPropA
- GetParent

    - GetWindow
    - GetMenuStringA
    - GetMenuState
    - GetMenuItemInfoA
    - GetMenuItemID
    - GetMenuItemCount
    - GetMenu
    - GetLastActivePopup
    - GetKeyboardState
    - GetKeyboardLayoutList
    - GetKeyboardLayout
    - GetKeyState
    - GetKeyNameTextA
    - GetIconInfo
    - GetForegroundWindow
    - GetFocus
    - GetDesktopWindow
    - GetDCEx
    - GetDC
    - GetCursorPos
    - GetCursor
    - GetClientRect
    - GetClassNameA
    - GetClassInfoA
    - GetCapture
    - GetActiveWindow
    - FrameRect
    - FindWindowA
    - FillRect
    - EqualRect
    - EnumWindows
    - EnumThreadWindows
    - EndPaint
    - EnableWindow
    - EnableScrollBar
    - EnableMenuItem
    - DrawTextA
    - DrawMenuBar
    - DrawIconEx
    - DrawIcon
    - DrawFrameControl
    - DrawFocusRect
    - DrawEdge
    - DispatchMessageA
    - DestroyWindow
    - DestroyMenu
    - DestroyIcon
    - DestroyCursor
    - DeleteMenu
    - DefWindowProcA
    - DefMDIChildProcA
    - DefFrameProcA
    - CreatePopupMenu
    - CreateMenu
    - CreateIcon
    - ClientToScreen
    - CheckMenuItem
    - CallWindowProcA
    - CallNextHookEx
    - BeginPaint
    - CharNextA
    - CharLowerA
    - CharToOemA
    - AdjustWindowRectEx
    - ActivateKeyboardLayout
- kernel32.dll
    - Sleep
- oleaut32.dll
    - SafeArrayPtrOfIndex
    - SafeArrayGetUBound
    - SafeArrayGetLBound
    - SafeArrayCreate
    - VariantChangeType
    - VariantCopy
    - VariantClear

- VariantInit
- comctl32.dll
  - ImageList_SetIconSize
  - ImageList_GetIconSize
  - ImageList_Write
  - ImageList_Read
  - ImageList_GetDragImage
  - ImageList_DragShowNolock
  - ImageList_SetDragCursorImage
  - ImageList_DragMove
  - ImageList_DragLeave
  - ImageList_DragEnter
  - ImageList_EndDrag
  - ImageList_BeginDrag
  - ImageList_Remove
  - ImageList_DrawEx
  - ImageList_Draw
  - ImageList_GetBkColor
  - ImageList_SetBkColor
  - ImageList_ReplaceIcon
  - ImageList_Add
  - ImageList_SetImageCount
  - ImageList_GetImageCount
  - ImageList_Destroy
  - ImageList_Create
- winspool.drv
  - OpenPrinterA
  - EnumPrintersA
  - DocumentPropertiesA
  - ClosePrinter
- comdlg32.dll
  - PageSetupDlgA

PE Resources

RT_CURSOR
RT_BITMAP
RT_ICON
RT_DIALOG
RT_STRING
RT_RCDATA
RT_GROUP_CURSOR
RT_GROUP_ICON
RT_VERSION

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS