VALKYRIE COMODO

Summary

File Name: malware_18.exe

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

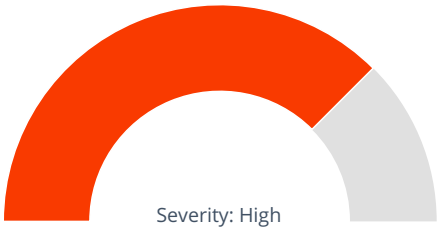
SHA1: ef6dc297e8016e3ffea966172d6d36e19e32a8bd

MD5: 9d14ac0e8c2fc7742a10a92d44c120d4

MALWARE

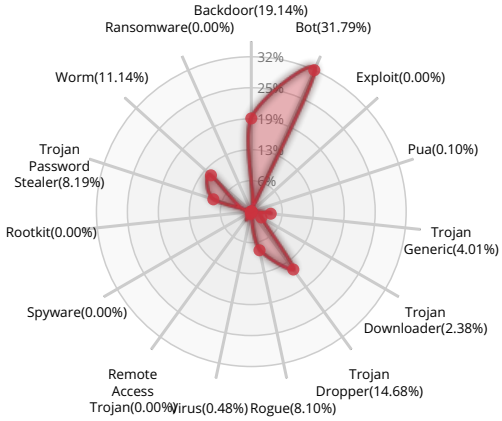
Valkyrie Final Verdict

DETECTION SECTION

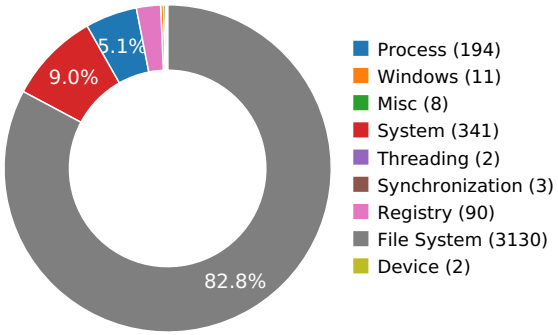


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

STATIC ANOMALY

Anomalous binary characteristics — Show sources

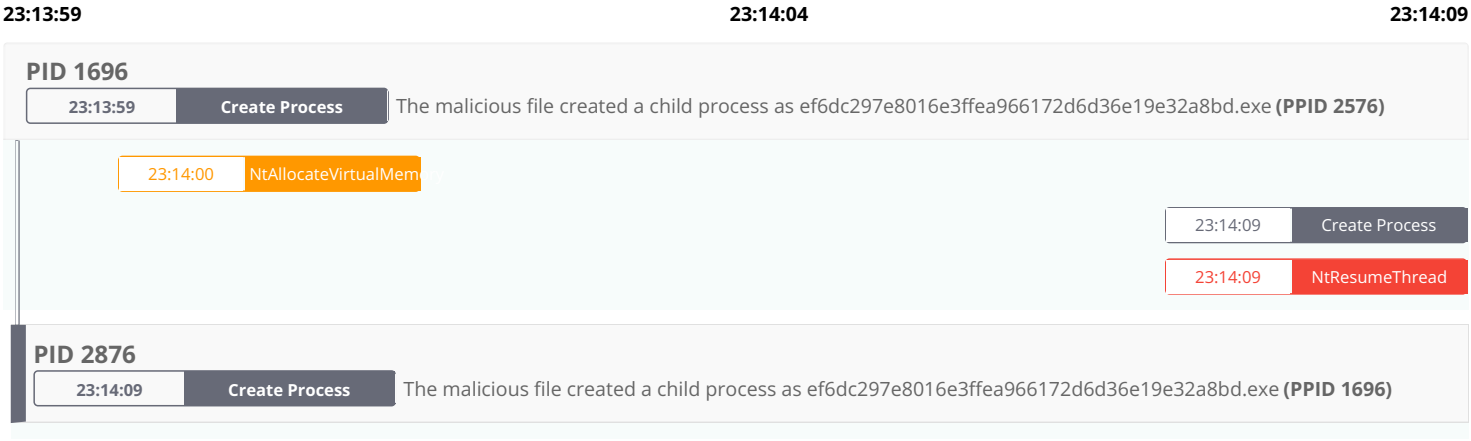
HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

Executed a process and injected code into it, probably while unpacking — Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\ef6dc297e8016e3ffea966172d6d36e19e32a8bd.exe.cfg
C:\Windows\sysnative\C_932.NLS
C:\Windows\sysnative\C_949.NLS
C:\Windows\sysnative\C_950.NLS
C:\Windows\sysnative\C_936.NLS
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\user64.DLL
C:\Windows\System32\user64.DLL
C:\Windows\system\user64.DLL
C:\Windows\user64.DLL
C:\ProgramData\Oracle\Java\javapath\user64.DLL
C:\Windows\System32\wbem\user64.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\user64.DLL
C:\Program Files\Microsoft Network Monitor 3\user64.DLL
C:\Program Files (x86)\Universal Extractor\user64.DLL
C:\Program Files (x86)\Universal Extractor\bin\user64.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\user64.DLL
C:\Python27\user64.DLL
C:\Python27\Scripts\user64.DLL
C:\tools\sysinternals\user64.DLL
C:\tools\user64.DLL
C:\tools\IDA_Pro_v6\python\user64.DLL
C:\Windows\SysWOW64\ntdll.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16

RESOLVED APIS

cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
oleaut32.dll.OleLoadPictureEx
oleaut32.dll.DispCallFunc
oleaut32.dll.LoadTypeLibEx
oleaut32.dll.UnRegisterTypeLib
oleaut32.dll.CreateTypeLib2
oleaut32.dll.VarDateFromUdate
oleaut32.dll.VarUdateFromDate
oleaut32.dll.GetAltMonthNames
oleaut32.dll.VarNumFromParseNum
oleaut32.dll.VarParseNumFromStr
oleaut32.dll.VarDecFromR4
oleaut32.dll.VarDecFromR8
oleaut32.dll.VarDecFromDate

oleaut32.dll.VarDecFromI4
oleaut32.dll.VarDecFromCy
oleaut32.dll.VarR4FromDec
oleaut32.dll.GetRecordInfoFromTypeInfo
oleaut32.dll.GetRecordInfoFromGuids
oleaut32.dll.SafeArrayGetRecordInfo
oleaut32.dll.SafeArraySetRecordInfo
oleaut32.dll.SafeArrayGetIID
oleaut32.dll.SafeArraySetIID
oleaut32.dll.SafeArrayCopyData
oleaut32.dll.SafeArrayAllocDescriptorEx
oleaut32.dll.SafeArrayCreateEx
oleaut32.dll.VarFormat
oleaut32.dll.VarFormatDateTime
oleaut32.dll.VarFormatNumber
oleaut32.dll.VarFormatPercent
oleaut32.dll.VarFormatCurrency
oleaut32.dll.VarWeekdayName
oleaut32.dll.VarMonthName
oleaut32.dll.VarAdd
oleaut32.dll.VarAnd
oleaut32.dll.VarCat
oleaut32.dll.VarDiv
oleaut32.dll.VarEqv
oleaut32.dll.VarIdiv
oleaut32.dll.VarImp
oleaut32.dll.VarMod
oleaut32.dll.VarMul
oleaut32.dll.VarOr
oleaut32.dll.VarPow
oleaut32.dll.VarSub
oleaut32.dll.VarXor
oleaut32.dll.VarAbs
oleaut32.dll.VarFix
oleaut32.dll.VarInt

oleaut32.dll.VarNeg
oleaut32.dll.VarNot
oleaut32.dll.VarRound
oleaut32.dll.VarCmp
oleaut32.dll.VarDecAdd
oleaut32.dll.VarDecCmp
oleaut32.dll.VarBstrCat
oleaut32.dll.VarCyMull4
oleaut32.dll.VarBstrCmp
ole32.dll.CoCreateInstanceEx
ole32.dll.CLSIDFromProgIDEx
sxs.dll.SxsOleAut32MapIIDOrCLSIDToTypeLibrary
user32.dll.GetSystemMetrics
user32.dll.MonitorFromWindow
user32.dll.MonitorFromRect
user32.dll.MonitorFromPoint
user32.dll.EnumDisplayMonitors
user32.dll.GetMonitorInfoA
dwmapi.dll.DwmIsCompositionEnabled
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Codepage
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936

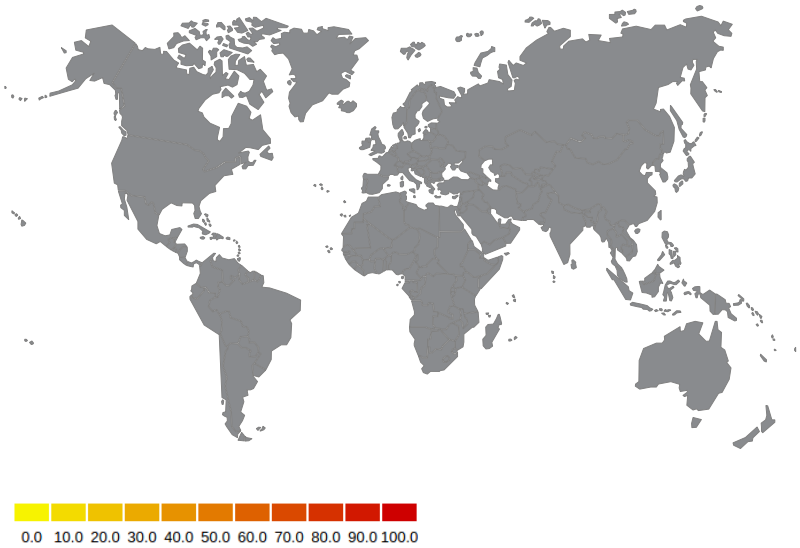
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\ef6dc297e8016e3ffea966172d6d36e19e32a8bd.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLEAUT\UserEra
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International\Calendars\TwoDigitYearMax
HKEY_CURRENT_USER\Control Panel\International\Calendars\TwoDigitYearMax

READ FILES

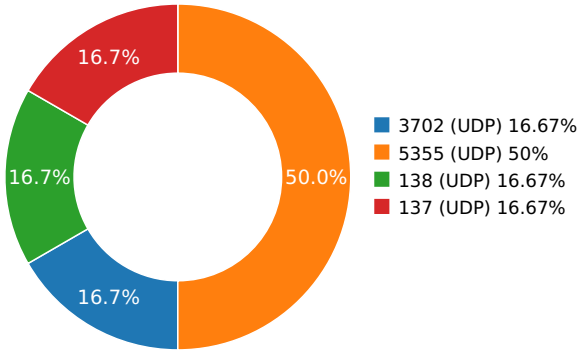
\Device\KsecDD
C:\Windows\Fonts\staticcache.dat
C:\Windows\SysWOW64\ntdll.dll

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
3.20692610741	Sandbox	192.168.56.255	137
3.22570705414	Sandbox	224.0.0.252	5355
3.22616910934	Sandbox	224.0.0.252	5355
3.43262314796	Sandbox	239.255.255.250	3702
5.78550410271	Sandbox	224.0.0.252	5355
9.23661708832	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:	malware_18.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	ef6dc297e8016e3ffea966172d6d36e19e32a8bd
MD5:	9d14ac0e8c2fc7742a10a92d44c120d4
First Seen Date:	2018-06-03 18:29:38.803403 (7 months ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-06-03 18:29:38.803403 (7 months 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
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	3
Trid	[[90.6, u'Win32 Executable Microsoft Visual Basic 6'], [4.9, u'Win32 Executable (generic)'], [2.2, u'Generic Win/DOS Executable'], [2.2, u'DOS Executable Generic']]
Compilation Time Stamp	0x5B0EB74C [Wed May 30 14:38:04 2018 UTC]
Translation	0x0409 0x04b0
LegalCopyright	BLUestaca SYSTEme Fnq.
InternalName	Sandladen6
FileVersion	6.06
CompanyName	Dvdvidaosofa gaq.
LegalTrademarks	DRAPBOe, Vnu.
Comments	vorTAW TEOX
ProductName	speeA guade Wnb.
ProductVersion	6.06
FileDescription	capOEV saiV
OriginalFilename	Sandladen6.exe
Entry Point	0x40175c (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1003520
Ssdeep	12288:9YdhuVcm2skZJudFELzJXbaQZkGbYn/j+:S/WN1sJh9Xb3ZkG8y
Sha256	b031075b8ad2558ee3ee7f0749c2b24484dd6fab7252fad71548276514b9b766
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/e/f/6/d/ef6dc297e8016e3ffea966172d6d36e19e32a8bd', u'EXE:OriginalFileName': u'Sandladen6.exe', u'EXE:ProductName': u'speeA guade Wnb.', u'EXE:InternalName': u'Sandladen6', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:06:03 18:29:04+00:00', u'EXE:InitializedDataSize': 380928, u'File:FileModifyDate': u'2018:06:03 18:28:58+00:00', u'EXE:FileVersionNumber': u'6.6.0.0', u'EXE:FileVersion': 6.06, u'File:FileSize': u'980 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:LegalTrademarks': u'DRAPBOe, Vnu.', u'EXE:ProductVersion': 6.06, u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Dvdvidaosofa gaq.', u'File:FileName': u'ef6dc297e8016e3ffea966172d6d36e19e32a8bd', u'EXE:ImageVersion': 6.6, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2018:05:30 14:38:04+00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LegalCopyright': u'BLUestaca SYSTEme Fnq.', u'EXE:LinkerVersion': 6.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/e/f/6/d', u'EXE:FileDescription': u'capOEV saiV', u'EXE:EntryPoint': u'0x175c', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 622592, u'EXE:Comments': u'vorTAW TEOX', u'File:FileInodeChangeDate': u'2018:06:03 18:28:58+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'6.6.0.0'}]
Mime Type	application/x-dosexec
Imphash	361faad8a85e5eb8a620cea515d19ffb

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x97ed4	0x98000	6.38891922939	2c2ea40882a88519b5dc72929532df59
.data	0x99000	0x12c4	0x1000	0.0	620f0b67a91f7f74151bc5be745b7110
.rsrc	0x9b000	0x5aaac	0x5b000	0.538696636556	941ba4afb9759f07b2e5dd1434b8d2dc

PE Imports

- MSVBVM60.DLL
  - _CIcos
  - _adj_fptan
  - __vbaVarMove
  - __vbaFreeVar
  - __vbaStrVarMove
  - __vbaFreeVarList
  - _adj_fdiv_m64
  - None
  - _adj_fprem1
  - __vbaStrCat
  - __vbaSetSystemError
  - __vbaHresultCheckObj
  - __vbaLenBstrB
  - _adj_fdiv_m32
  - __vbaObjSet
  - __vbaOnError
  - _adj_fdiv_m16i
  - __vbaObjSetAddref
  - _adj_fdivr_m16i
  - None
  - _CIsin
  - None
  - __vbaChkstk
  - __vbaFileClose
  - EVENT_SINK_AddRef
  - __vbaStrCmp
  - __vbaVarTstEq
  - __vbaObjVar
  - DllFunctionCall
  - None
  - _adj_fpatan
  - EVENT_SINK_Release
  - _CIsqrt
  - EVENT_SINK_QueryInterface
  - __vbaUI1I4
  - __vbaExceptHandler
  - _adj_fprem
  - _adj_fdivr_m64
  - None
  - None
  - __vbaFPException
  - _CIlog
  - __vbaFileOpen
  - None
  - __vbaNew2
  - _adj_fdiv_m32i
  - _adj_fdivr_m32i
  - __vbaStrCopy
  - __vbaFreeStrList
  - _adj_fdivr_m32
  - __vbaR8Var
  - _adj_fdiv_r
  - None
  - __vbaVarTstNe
  - __vbaVarAdd
  - __vbaStrComp
  - _CIatan
  - __vbaStrMove
  - None
  - _allmul
  - _CItan
  - None

- _CIexp
- __vbaFreeObj
- __vbaFreeStr
- None

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 635352, u'sha256': u'30b87f24949925fde9aec1d68c37b8933d8759e47c0cbe02100cf8e68891644e', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 270376}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 905728, u'sha256': u'461d3efa0866bbb859cbb2cc58fed7661f78a2032646072c6066660d191ca621', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 906856, u'sha256': u'731f85ea3b57873cd4385d3d23e4618a43e474fb51e7797187819fcde0e53a5c', u'type': u'dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 916496, u'sha256': u'e6fb0f86d786e11a69111ad6d4b05209680e5e41078d1c14ce1672b1c8883b2b', u'type': u'dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 920760, u'sha256': u'b5c0e56938e0cdd377e311a172f3ee2b022a5cd8d7b131311105b65faae2584b', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 67624}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 988384, u'sha256': u'baee07dca12a5ecbe557b72c213b1bfabe5b51804f543ca36c58f5fead139be6', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0', u'size': 16936}

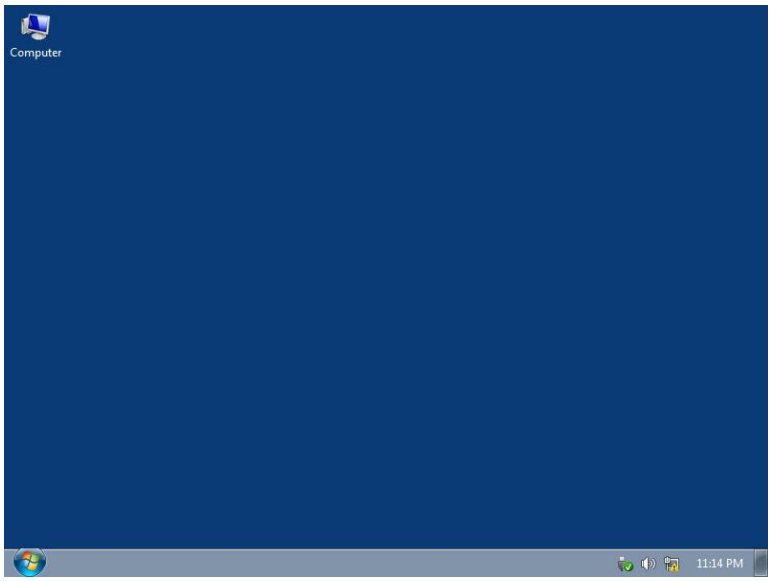
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 1005320, u'sha256': u'b3d066b10578e4a63a9e16dd19918531242399758b182986710b62975fe24574', u'type': u'MS Windows icon resource - 6 icons, 256x256', u'size': 90}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 1005412, u'sha256': u'c4b7570f2b49b8954d2ab88b3f62a20c28d5dd96babcd4ae7131aa0f8168cd4e', u'type': u'data', u'size': 840}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

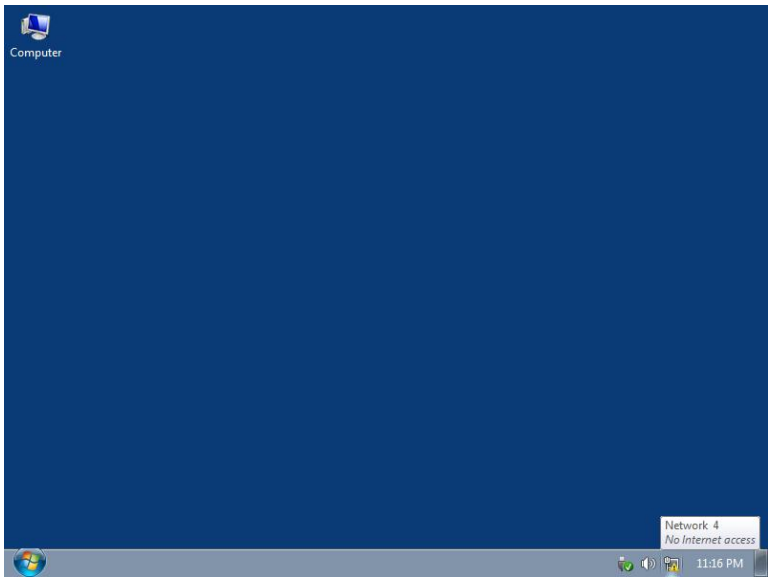
SCREENSHOTS




Computer
11:16 PM


Computer
11:14 PM


Computer
11:13 PM


Computer
Network 4
No Internet access
11:16 PM