VALKYRIE COMODO

Summary

File Name: font_install.exe

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

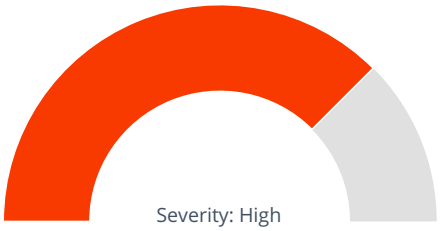
SHA1: 9c45fca5872329cef99439ae95100bbc19a95d83

MD5: 74be528fda1823c547f7aa6af6ebd433

MALWARE

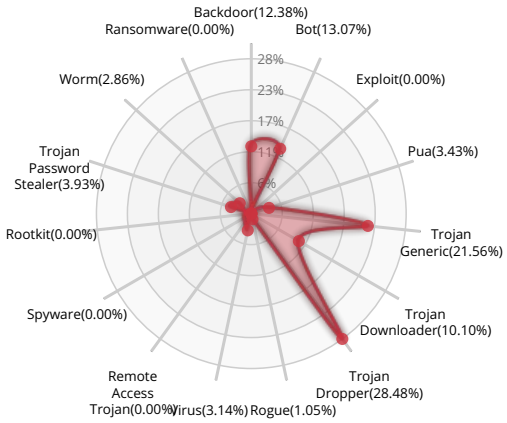
Valkyrie Final Verdict

DETECTION SECTION

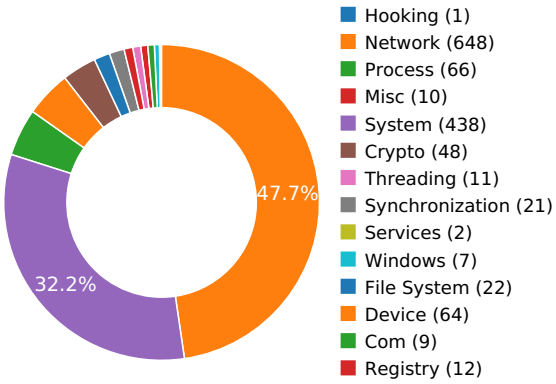


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

NETWORKING

HTTP traffic contains suspicious features which may be indicative of malware related traffic Show sources

Performs some HTTP requests Show sources

MALWARE ANALYSIS SYSTEM EVASION

Mimics the system's user agent string for its own requests

A process attempted to delay the analysis task. Show sources

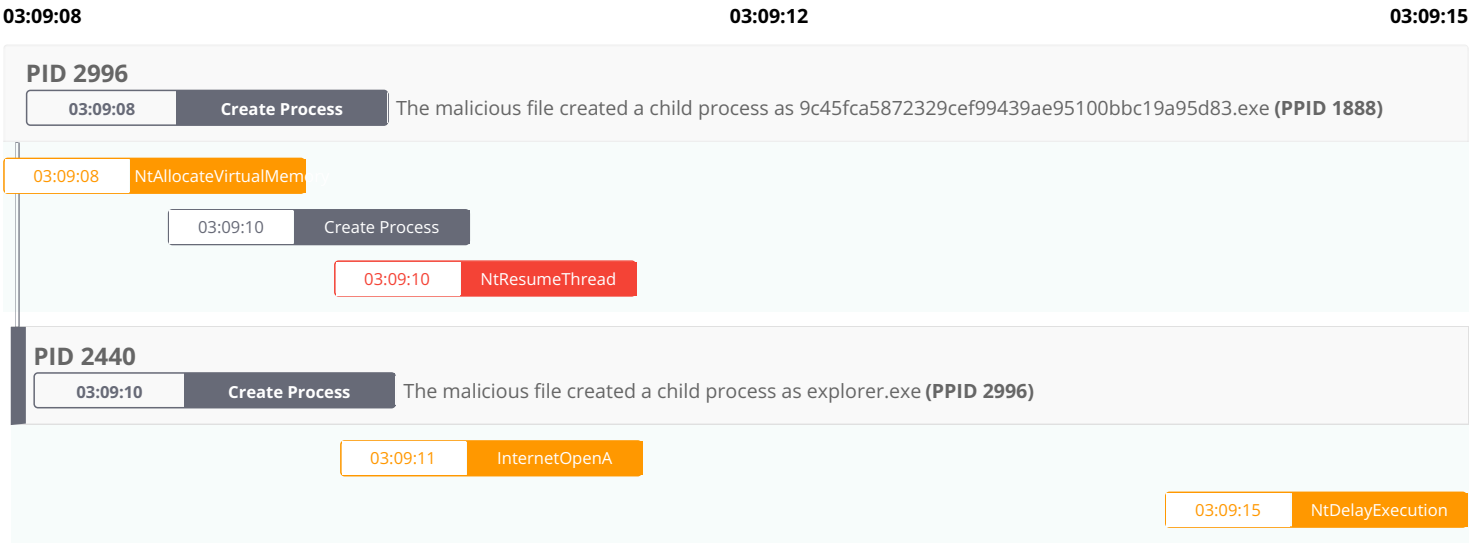
HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory

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

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\l\x07
\Device\KsecDD
C:\Windows\inf\l\x07
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\DriverStore\infpub.dat
C:\Windows\System32\DriverStore\infstor.dat
C:\Windows\System32\DriverStore\infstrng.dat
C:\Windows\System32\DriverStore\drvindex.dat
C:\Windows\System32\DriverStore\INFCACHE.0
C:\Windows\System32\DriverStore\INFCACHE.1
C:\Windows\System32\DriverStore\INFCACHE.2
C:\Users\user\AppData\Local\Temp\product.inf
C:\Windows\inf\
C:\Windows\System32\
C:\Users\user\AppData\Local\Temp\emf

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.IsProcessorFeaturePresent
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
kernel32.dll.HeapCreate
cryptbase.dll.SystemFunction036
oleaut32.dll.#500
ole32.dll.CoInitializeEx

user32.dll.UnregisterDeviceNotification
user32.dll.RegisterDeviceNotificationW
ntmarta.dll.GetMartaExtensionInterface
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
kernel32.dll.RegOpenKeyExW
kernel32.dll.RegCloseKey
devrtl.dll.DevRtlGetThreadLogToken
spfileq.dll.SpFileQueueOpen
spfileq.dll.SpFileQueueSetFlags
spinf.dll.SpInfSetDirIdHandler
sechost.dll.ConvertStringSecurityDescriptorToSecurityDescriptorW
spinf.dll.SpInfLoadInfFile
user32.dll.MessageBoxW
ws2_32.dll.#22
ws2_32.dll.#11
ws2_32.dll.#115
ws2_32.dll.freeaddrinfo
ws2_32.dll.getaddrinfo
ws2_32.dll.#3
ws2_32.dll.#4
ws2_32.dll.#23
ws2_32.dll.#12
dnsapi.dll.DnsQuery_A
dnsapi.dll.DnsFree
wininet.dll.DeleteUrlCacheEntryA
wininet.dll.InternetReadFile
wininet.dll.HttpSendRequestA
wininet.dll.HttpQueryInfoA
wininet.dll.HttpOpenRequestA
wininet.dll.InternetQueryOptionW
wininet.dll.InternetSetOptionW
wininet.dll.InternetQueryOptionA
wininet.dll.InternetConnectA
wininet.dll.InternetCloseHandle

wininet.dll.InternetSetOptionA
wininet.dll.InternetOpenA
wininet.dll.InternetCrackUrlA
kernel32.dll.MultiByteToWideChar
kernel32.dll.LocalFree
kernel32.dll.LocalAlloc
kernel32.dll.ExitProcess
kernel32.dll.Sleep
kernel32.dll.CreateThread
kernel32.dll.WaitForSingleObject
kernel32.dll.GetCurrentProcessId
kernel32.dll.CloseHandle
kernel32.dll.ReadFile
kernel32.dll.CreateFileW
kernel32.dll.FlushFileBuffers
kernel32.dll.WriteFile
kernel32.dll.GetTickCount
kernel32.dll.SetFileAttributesW
kernel32.dll.DeleteFileW
kernel32.dll.VirtualAlloc
kernel32.dll.GetFileSizeEx
kernel32.dll.VirtualFree
kernel32.dll.GetProcessHeap
kernel32.dll.HeapFree
kernel32.dll.HeapAlloc
kernel32.dll.HeapReAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.GetProcAddress
kernel32.dll.OutputDebugStringA

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\DirectShow\PushClock
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\System\Setup

HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress

HKEY_CURRENT_USER\Software\Microsoft\fe84f842c

READ FILES

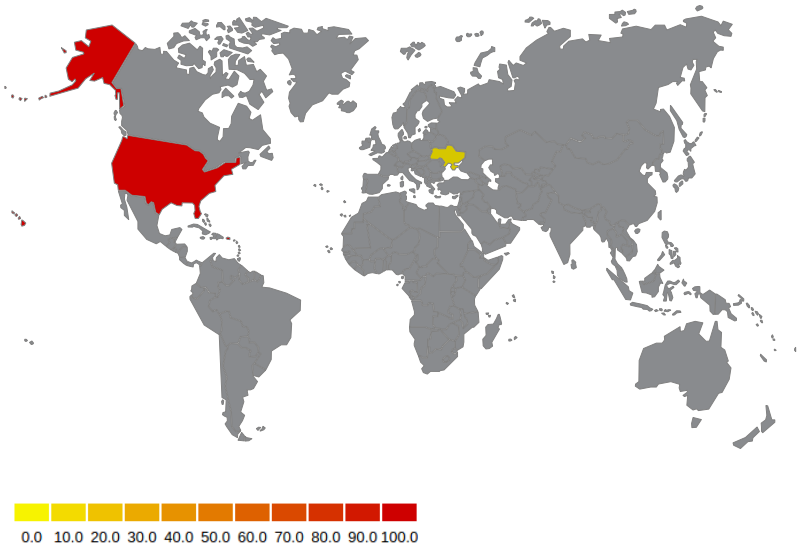
\Device\KsecDD

C:\Windows\Globalization\Sorting\sortdefault.nls

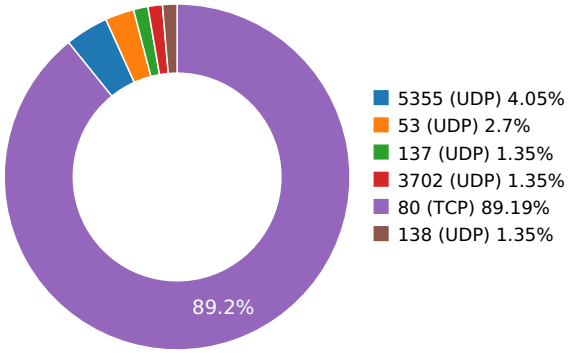
C:\Users\user\AppData\Local\Temp\emf

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Communications, Inc.	Malware Process
	8.8.8.8	United States	15169	Level 3 Communications, Inc.	Malware Process
	79.171.124.211	Ukraine	34700	Maxnet Ltd., Kharkiv Unity Of ...	Malware Process
marginalelement.com	93.76.179.27	Ukraine	25229	Volia Kharkov	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	6	11.5368571281
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	6	39.2326540947
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	6	66.9504799843
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	6	94.6122739315
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	6	122.258424044
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	6	234.968583107
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	6	262.813816071
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	6	297.103016138
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	6	325.159193039
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						
marginalelement.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	2	361.812669992
Path: /www/secur.php **URI:** http://marginalelement.com/www/secur.php						

DNS QUERIES

Request	Type
marginalelement.com	A

Answers
- 213.231.25.168 (A)
- 5.149.221.94 (A)
- 176.103.201.70 (A)
- 46.185.49.156 (A)
- 217.73.90.59 (A)
- 178.151.116.49 (A)
- 178.136.221.227 (A)
- 79.171.124.211 (A)
- 141.101.21.128 (A)
- 86.123.104.1 (A)

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
11.5368571281	Sandbox	79.171.124.211	80
11.9515571594	Sandbox	79.171.124.211	80
17.405408144	Sandbox	79.171.124.211	80
17.8566050529	Sandbox	79.171.124.211	80
23.3094480038	Sandbox	79.171.124.211	80
23.7462339401	Sandbox	79.171.124.211	80
39.2326540947	Sandbox	79.171.124.211	80
39.6686611176	Sandbox	79.171.124.211	80
45.1143341064	Sandbox	79.171.124.211	80
45.548746109	Sandbox	79.171.124.211	80
51.0126399994	Sandbox	79.171.124.211	80
51.4627871513	Sandbox	79.171.124.211	80
66.9504799843	Sandbox	79.171.124.211	80
67.3797039986	Sandbox	79.171.124.211	80
72.8270511627	Sandbox	79.171.124.211	80
73.2512969971	Sandbox	79.171.124.211	80
78.7225799561	Sandbox	79.171.124.211	80
79.1424069405	Sandbox	79.171.124.211	80
94.6122739315	Sandbox	79.171.124.211	80
95.0488140583	Sandbox	79.171.124.211	80
100.484118938	Sandbox	79.171.124.211	80
100.906193018	Sandbox	79.171.124.211	80
106.362009048	Sandbox	79.171.124.211	80
106.790337086	Sandbox	79.171.124.211	80

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
122.258424044	Sandbox	79.171.124.211	80
122.668121099	Sandbox	79.171.124.211	80
128.125255108	Sandbox	79.171.124.211	80
128.550014019	Sandbox	79.171.124.211	80
133.964311123	Sandbox	79.171.124.211	80
134.380666018	Sandbox	79.171.124.211	80
234.968583107	Sandbox	79.171.124.211	80
235.392842054	Sandbox	79.171.124.211	80
240.868871927	Sandbox	79.171.124.211	80
241.313049078	Sandbox	79.171.124.211	80
246.768940926	Sandbox	79.171.124.211	80
247.326653004	Sandbox	79.171.124.211	80
262.813816071	Sandbox	79.171.124.211	80
269.496803045	Sandbox	79.171.124.211	80
274.985878944	Sandbox	79.171.124.211	80
275.436548948	Sandbox	79.171.124.211	80
280.993618011	Sandbox	79.171.124.211	80
281.421931028	Sandbox	79.171.124.211	80
297.103016138	Sandbox	79.171.124.211	80
297.661000013	Sandbox	79.171.124.211	80
303.092616081	Sandbox	79.171.124.211	80
303.672565937	Sandbox	79.171.124.211	80
309.10858202	Sandbox	79.171.124.211	80
309.523414135	Sandbox	79.171.124.211	80
325.159193039	Sandbox	79.171.124.211	80
325.573522091	Sandbox	79.171.124.211	80
330.997157097	Sandbox	79.171.124.211	80
331.476951122	Sandbox	79.171.124.211	80
345.917634964	Sandbox	79.171.124.211	80
346.33604598	Sandbox	79.171.124.211	80
361.812669992	Sandbox	79.171.124.211	80
362.245182991	Sandbox	79.171.124.211	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.09248304367	Sandbox	224.0.0.252	5355
3.1488161087	Sandbox	192.168.56.255	137
3.15163207054	Sandbox	224.0.0.252	5355
3.15616512299	Sandbox	239.255.255.250	3702
5.7466571331	Sandbox	224.0.0.252	5355
7.85640311241	Sandbox	8.8.4.4	53
8.85554814339	Sandbox	8.8.8.8	53
9.18403100967	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:	font_install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	9c45fca5872329cef99439ae95100bbc19a95d83
MD5:	74be528fda1823c547f7aa6af6ebd433
First Seen Date:	2017-04-15 01:50:38.287341 (2 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2017-05-01 14:24:27.894405 (2 years 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
Number Of Sections	4
Compilation Time Stamp	0x57FB077A [Mon Oct 10 03:14:02 2016 UTC]
LegalCopyright	Weiying (C) 2007-2015
InternalName	Dots
FileVersion	7.7.1.2
CompanyName	Weiying
PrivateBuild	7.7.1.2
LegalTrademarks	Weiying (C) 2007-2015
Comments	Nsa Exreskit Dutainment Ab
ProductName	Dots
Languages	English
ProductVersion	7.7.1.2
FileDescription	Nsa Exreskit Dutainment Ab
OriginalFilename	Dots.exe
Translation	0x0409 0x04b0
Entry Point	0x40b3e6 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	331776
Sha256	d8eece3e1453de635e140def1f677107416e2abf3175ba0c85735f96acdd10e4
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x19a1a	0x1a000	6.846606	-
.rdata	0x1b000	0x79a4	0x8000	6.148038	-
.data	0x23000	0x34f8	0x2000	2.826543	-
.rsrc	0x27000	0x2b6a4	0x2c000	7.365569[SUSPICIOUS]	-

PE Imports

- KERNEL32.dll
  - GetStringTypeA
  - LCMapStringW
  - LCMapStringA
  - MultiByteToWideChar

- WriteConsoleW
- GetConsoleOutputCP
- WriteConsoleA
- SetStdHandle
- InitializeCriticalSection
- HeapSize
- GetOEMCP
- GetACP
- GetCPInfo
- GetConsoleMode
- GetConsoleCP
- SetFilePointer
- GetCurrentProcessId
- GetTickCount
- QueryPerformanceCounter
- SetHandleCount
- GetEnvironmentStringsW
- WideCharToMultiByte
- FreeEnvironmentStringsW
- GetEnvironmentStrings
- FreeEnvironmentStringsA
- GetStdHandle
- GetStringTypeW
- HeapReAlloc
- VirtualAlloc
- DeleteCriticalSection
- VirtualFree
- HeapCreate
- HeapDestroy
- LeaveCriticalSection
- EnterCriticalSection
- InterlockedDecrement
- SetLastError
- InterlockedIncrement
- TlsFree
- TlsSetValue
- TlsAlloc
- TlsGetValue
- VirtualQuery
- GetStartupInfoA
- GetProcessHeap
- GetVersionExA
- GetCommandLineA
- HeapFree
- RtlUnwind
- RaiseException
- IsDebuggerPresent
- SetUnhandledExceptionFilter
- UnhandledExceptionFilter
- TerminateProcess
- GetLocaleInfoA
- FlushFileBuffers
- CreateFileA
- GetFileType
- GetFileSize
- GetFileTime
- FileTimeToSystemTime
- SystemTimeToTzSpecificLocalTime
- CloseHandle
- CreateEventA
- WaitForSingleObject
- SleepEx
- GlobalAlloc
- GetUserDefaultLangID
- FindResourceExA
- LoadResource
- LoadLibraryA
- GetProcAddress
- ExitProcess
- GetFileAttributesA
- HeapAlloc
- Sleep
- GetSystemTimeAsFileTime
- GetCurrentProcess
- GetProcessTimes

- GetCurrentThreadId
- GlobalLock
- GetModuleHandleA
- GetLastError
- GetModuleFileNameA
- lstrcmpA
- WriteFile

- USER32.dll
  - AppendMenuA
  - GetMenuItemCount
  - GetDlgCtrlID
  - GetWindowThreadProcessId
  - IsWindow
  - GetWindowTextA
  - GetMenuItemID
  - DeleteMenu
  - WindowFromPoint
  - GetCursorPos
  - GetDlgItem
  - UpdateLayeredWindow
  - GetForegroundWindow
  - CheckMenuItem
  - CreateWindowExA
  - SetMenu
  - AppendMenuW
  - EnableWindow
  - ShowWindow
  - SendMessageA
  - GetCursorInfo
  - CopyIcon
  - SetClipboardViewer
  - EndDialog
  - GetPropA
  - SetPropA
  - DestroyWindow
  - LoadBitmapA
  - GetPriorityClipboardFormat
  - CountClipboardFormats
  - GetAsyncKeyState
  - OpenClipboard
  - OffsetRect
  - MapWindowPoints
  - GetWindowRect
  - GetSystemMetrics
  - DefWindowProcA
  - BeginPaint
  - CreateMenu
  - FillRect
  - SetRect
  - GetDC
  - InsertMenuItemA
  - PostQuitMessage
  - GetActiveWindow
  - GetDCEx
  - DrawTextA
  - ReleaseDC
  - SetProcessWindowStation
  - OpenDesktopA
  - SetThreadDesktop
  - GetWindowDC
  - MonitorFromPoint
  - GetMonitorInfoA
  - CreateIconFromResourceEx
  - GetWindowLongA
  - DialogBoxIndirectParamA
  - LoadImageA
  - GetClientRect
  - EndPaint
  - RegisterWindowMessageA
  - LoadIconA
  - LoadCursorA
  - SetCapture
  - MessageBoxW
  - InflateRect
  - EmptyClipboard

    - SetClipboardData
    - CloseClipboard
    - DefWindowProcW
    - IsClipboardFormatAvailable
    - EnableMenuItem
    - GetIconInfo
    - IsWindowEnabled
    - TrackPopupMenu
    - MessageBoxA
    - CreatePopupMenu
- GDI32.dll
    - CreateCompatibleBitmap
    - SelectObject
    - SaveDC
    - SetTextColor
    - CreateFontIndirectA
    - BitBlt
    - RestoreDC
    - DeleteDC
    - CreateSolidBrush
    - SetDCPenColor
    - BeginPath
    - MoveToEx
    - AngleArc
    - LineTo
    - EndPath
    - StrokePath
    - CloseFigure
    - CreateCompatibleDC
    - CreateDIBSection
    - SelectPalette
    - RealizePalette
    - CreateHalftonePalette
    - GetDeviceCaps
    - GetEnhMetaFileA
    - GetEnhMetaFileHeader
    - PlayEnhMetaFile
    - DeleteEnhMetaFile
    - Ellipse
    - Rectangle
    - SetWorldTransform
    - SetGraphicsMode
    - CreatePatternBrush
    - SetBkMode
    - SetDCBrushColor
    - CreateRectRgnIndirect
    - CreateRectRgn
    - DeleteObject
    - GetObjectA
    - CombineRgn
- ADVAPI32.dll
    - GetNamedSecurityInfoA
    - AllocateAndInitializeSid
    - SetEntriesInAclA
- SHELL32.dll
    - DragQueryFileA
    - Shell_NotifyIconA
- ole32.dll
    - OleInitialize
    - CoGetClassObject
    - StgCreateDocfile
    - CreateFileMoniker
    - CoInitialize
    - CoLockObjectExternal
    - RegisterDragDrop
    - RevokeDragDrop
    - OleUninitialize
    - CoInitializeEx
    - CoCreateInstance
    - CoUninitialize
    - ReleaseStgMedium
- OLEAUT32.dll
    - VariantInit
    - VariantChangeType
    - VariantClear

- NETAPI32.dll
  - NetWkstaGetInfo
- PSAPI.DLL
  - GetProcessMemoryInfo
- WINMM.dll
  - mmioCreateChunk
  - mmioDescend
  - mmioRenameW
  - mmioRead
  - mmioFlush
  - mmioGetInfo
- VERSION.dll
  - GetFileVersionInfoA
  - GetFileVersionInfoW
- SHLWAPI.dll
  - PathFileExistsA
- pdh.dll
  - PdhBrowseCountersA
- gdiplus.dll
  - GdipLoadImageFromFile
  - GdipCloneImage
  - GdipFree
  - GdipAlloc
  - GdipLoadImageFromFileICM
  - GdipDisposeImage
- OPENGL32.dll
  - glLoadIdentity
  - glViewport
  - glMaterialfv
  - glRotatef
  - glEnable
  - glBlendFunc
  - glClearColor
  - glMatrixMode
  - glPushMatrix
- SETUPAPI.dll
  - SetupCloseInfFile
  - SetupOpenInfFileA
  - SetupOpenFileQueue
  - SetupDiDestroyDeviceInfoList
  - SetupDiDestroyDriverInfoList
  - SetupDefaultQueueCallbackA
  - SetupDiGetDeviceRegistryPropertyA
  - SetupDiGetDeviceInstallParamsA
  - SetupDiCreateDeviceInfoList
  - SetupInitDefaultQueueCallbackEx
- UxTheme.dll
  - CloseThemeData
  - DrawThemeBackground
  - GetThemeSysColor
  - OpenThemeData
- snmpapi.dll
  - SnmpUtilMemReAlloc

PE Resources

RT_CURSOR
RT_ICON
RT_STRING
RT_GROUP_CURSOR
RT_GROUP_ICON
RT_VERSION
RT_MANIFEST

CERTIFICATE VALIDATION

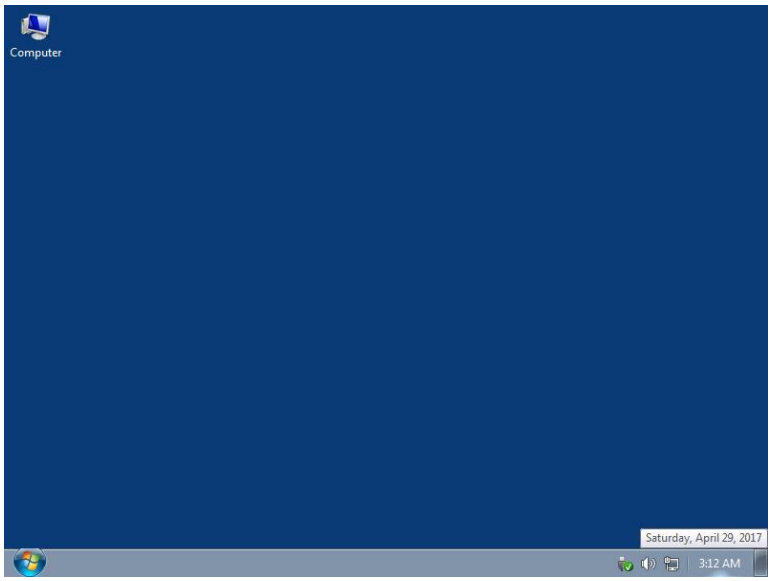
- Certificate Validation is not Applicable ?

SCREENSHOTS


Computer
3:12 AM

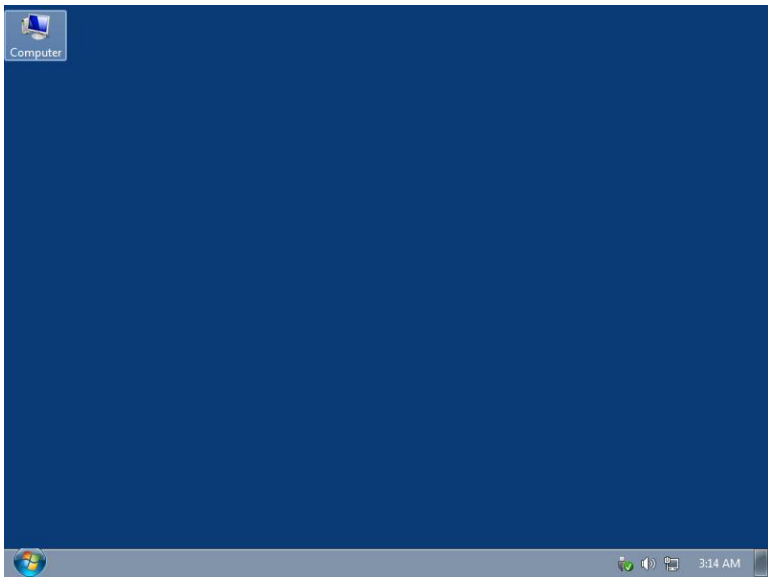

Computer
3:14 AM


Computer
3:14 AM


Computer
Saturday, April 29, 2017
3:12 AM


Computer
3:09 AM


Computer
3:14 AM


Computer
3:14 AM