VALKYRIE COMODO

Summary

File Name: php.exe

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

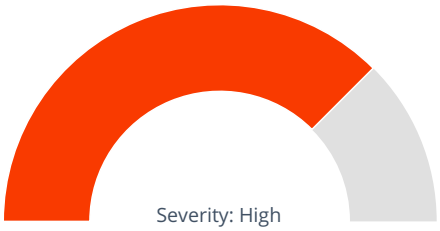
SHA1: ccd3d0e091167fca1cfd06dfb3850c68730c64c1

MD5: 05c9668dc4efca3354a88dc773c4a736

MALWARE

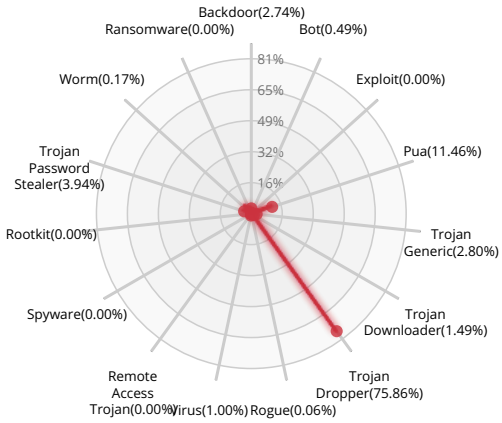
Valkyrie Final Verdict

DETECTION SECTION

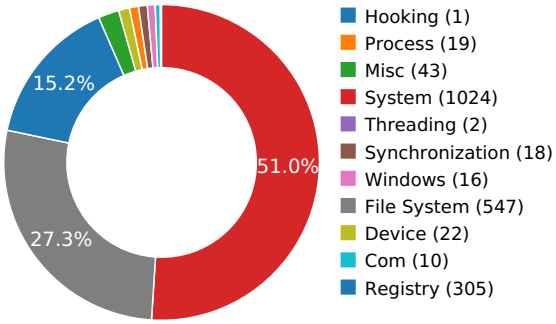


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Attempts to repeatedly call a single API many times in order to delay analysis time — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

VALKYRIE COMODO

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Windows\System32\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Windows\system\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Windows\<pi-ms-win-core-synch-l1-2-0.DLL
C:\ProgramData\Oracle\Java\javapath\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Windows\System32\wbem\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Program Files\Microsoft Network Monitor 3\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Program Files (x86)\Universal Extractor\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Program Files (x86)\Universal Extractor\bin\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Python27\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Python27\Scripts\<pi-ms-win-core-synch-l1-2-0.DLL
C:\tools\sysinternals\<pi-ms-win-core-synch-l1-2-0.DLL
C:\tools\<pi-ms-win-core-synch-l1-2-0.DLL
C:\tools\IDA_Pro_v6\python\<pi-ms-win-core-synch-l1-2-0.DLL
C:\Users\user\AppData\Local\Temp\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\system\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\ProgramData\Oracle\Java\javapath\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\wbem\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files\Microsoft Network Monitor 3\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\Scripts\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\tools\sysinternals\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\tools\<pi-ms-win-core-fibers-l1-1-1.DLL
C:\tools\IDA_Pro_v6\python\<pi-ms-win-core-fibers-l1-1-1.DLL

C:\Users\user\AppData\Local\Temp\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Windows\system\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Windows\<pi-ms-win-core-localization-l1-2-1.DLL
C:\ProgramData\Oracle\Java\javapath\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\wbem\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Program Files\Microsoft Network Monitor 3\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Python27\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Python27\Scripts\<pi-ms-win-core-localization-l1-2-1.DLL
C:\tools\sysinternals\<pi-ms-win-core-localization-l1-2-1.DLL
C:\tools\<pi-ms-win-core-localization-l1-2-1.DLL
C:\tools\IDA_Pro_v6\python\<pi-ms-win-core-localization-l1-2-1.DLL
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\DXGIDebug.dll
C:\Users\user\AppData\Local\Temp\lpk.dll
C:\Users\user\AppData\Local\Temp\usp10.dll
C:\Users\user\AppData\Local\Temp\clbcatq.dll
C:\Users\user\AppData\Local\Temp\comres.dll
C:\Users\user\AppData\Local\Temp\ws2_32.dll
C:\Users\user\AppData\Local\Temp\ws2help.dll
C:\Users\user\AppData\Local\Temp\psapi.dll
C:\Users\user\AppData\Local\Temp\ieframe.dll
C:\Users\user\AppData\Local\Temp\ntshrui.dll
C:\Users\user\AppData\Local\Temp\atl.dll
C:\Users\user\AppData\Local\Temp\setupapi.dll
C:\Users\user\AppData\Local\Temp\apphelp.dll
C:\Users\user\AppData\Local\Temp\userenv.dll
C:\Users\user\AppData\Local\Temp\netapi32.dll
C:\Users\user\AppData\Local\Temp\shdocvw.dll
C:\Users\user\AppData\Local\Temp\crypt32.dll
C:\Users\user\AppData\Local\Temp\msasn1.dll

C:\Users\user\AppData\Local\Temp\cryptui.dll
C:\Users\user\AppData\Local\Temp\wintrust.dll
C:\Users\user\AppData\Local\Temp\shell32.dll
C:\Users\user\AppData\Local\Temp\secur32.dll
C:\Users\user\AppData\Local\Temp\cabinet.dll
C:\Users\user\AppData\Local\Temp\oleaccrc.dll
C:\Users\user\AppData\Local\Temp\ntmarta.dll
C:\Users\user\AppData\Local\Temp\profapi.dll
C:\Users\user\AppData\Local\Temp\WindowsCodecs.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInset
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragMinDist
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInterval
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
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\AutoSuggest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Always Use Tab
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Client\(Default)
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\RarSFX0__tmp_rar_sfx_access_check_35646765
C:\Users\user\AppData\Local\Temp\RarSFX0\php5ts.dll
C:\Users\user\AppData\Local\Temp\RarSFX0\ssleay32.dll

C:\Users\user\AppData\Local\Temp\RarSFX0\ext\php_curl.dll
C:\Users\user\AppData\Local\Temp\RarSFX0\VkLock v1.9.exe
C:\Users\user\AppData\Local\Temp\RarSFX0\libeay32.dll
C:\Users\user\AppData\Local\Temp\RarSFX0\ext
C:\Users\user\AppData\Local\Temp\PSE20\3f9b32e8c488ba5f4851a5306f07e440\php.ini

RESOLVED APIS

kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
advapi32.dll.EventRegister
kernel32.dll.FlsGetValue
kernel32.dll.LCMapStringEx
kernel32.dll.SetDllDirectoryW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ole32.dll.OleInitialize
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
user32.dll.LoadIconW
user32.dll.LoadBitmapW
comctl32.dll.InitCommonControlsEx
shell32.dll.SHGetMalloc
ole32.dll.CoGetMalloc
user32.dll.DialogBoxParamW
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
uxtheme.dll.EnableThemeDialogTexture
uxtheme.dll.OpenThemeData
uxtheme.dll.IsThemePartDefined
uxtheme.dll.GetThemeMargins
uxtheme.dll.GetThemeBool
uxtheme.dll.GetThemeInt
comctl32.dll.HIMAGELIST_QueryInterface

comctl32.dll.DrawShadowText
comctl32.dll.DrawSizeBox
comctl32.dll.DrawScrollBar
comctl32.dll.SizeBoxHwnd
comctl32.dll.ScrollBar_MouseMove
comctl32.dll.ScrollBar_Menu
comctl32.dll.HandleScrollCmd
comctl32.dll.DetachScrollBars
comctl32.dll.AttachScrollBars
comctl32.dll.CCSetScrollInfo
comctl32.dll.CCGetScrollInfo
comctl32.dll.CCEnableScrollBar
comctl32.dll.QuerySystemGestureStatus
uxtheme.dll.#49
uxtheme.dll.CloseThemeData
uxtheme.dll.SetWindowTheme
uxtheme.dll.GetThemeFont
uxtheme.dll.GetThemeColor
imm32.dll.ImmIsIME
user32.dll.GetWindowRect
user32.dll.GetClientRect
user32.dll.GetWindowTextW
user32.dll.SetWindowTextW
user32.dll.GetSystemMetrics
user32.dll.GetWindow
user32.dll.SendMessageW
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW

gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
gdi32.dll.GdiIsMetaPrintDC
user32.dll.SendDlgItemMessageW
user32.dll.GetDC
gdi32.dll.GetDeviceCaps
user32.dll.ReleaseDC
user32.dll.GetDlgItem
user32.dll.GetClassNameW
user32.dll.FindWindowExW
shlwapi.dll.SHAutoComplete
ole32.dll.CoCreateInstance

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInset
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragMinDist
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInterval
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\Policies
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software
HKEY_LOCAL_MACHINE\Software
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\AutoSuggest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Always Use Tab
HKEY_CLASSES_ROOT\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\InProcServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\InProcServer32\(Default)
HKEY_CLASSES_ROOT\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\InProcServer32

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete\Client\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Client\(Default)
HKEY_CURRENT_USER\Control Panel\Desktop
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\Dynamic DST
HKEY_CURRENT_USER\Software\WinRAR SFX
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\ccd3d0e091167fca1cfd06dfb3850c68730c64c1.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\ccd3d0e091167fca1cfd06dfb3850c68730c64c1.exe
C:\Windows\System32\UXTheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\win.ini
C:\Windows\Fonts\staticcache.dat
C:\Windows\SysWOW64\shell32.dll
C:\Users\user\AppData\Local\Temp\RarSFX0__tmp_rar_sfx_access_check_35646765
C:\Users\user\AppData\Local\Temp\RarSFX0\VkLock v1.9.exe
C:\Users\user\AppData\Local\Temp\PSE20\3f9b32e8c488ba5f4851a5306f07e440\php.ini

MUTEXES

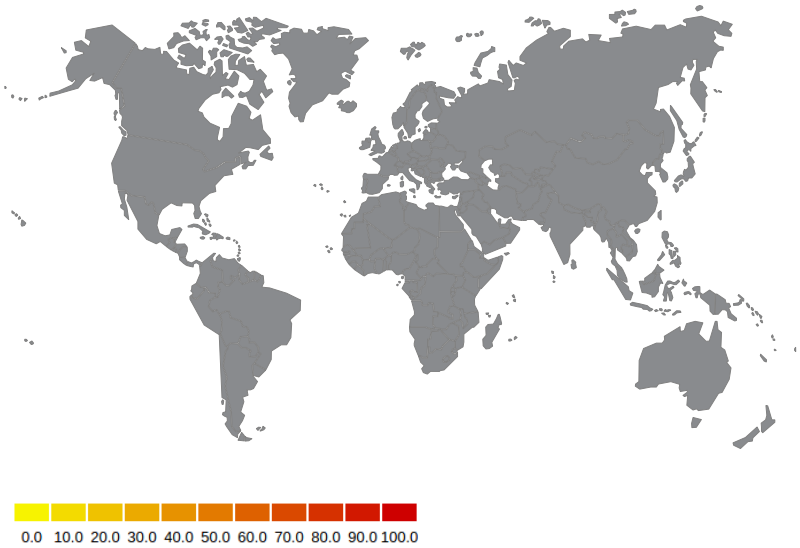
DefaultTabtip-MainUI
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

MODIFIED REGISTRY KEYS

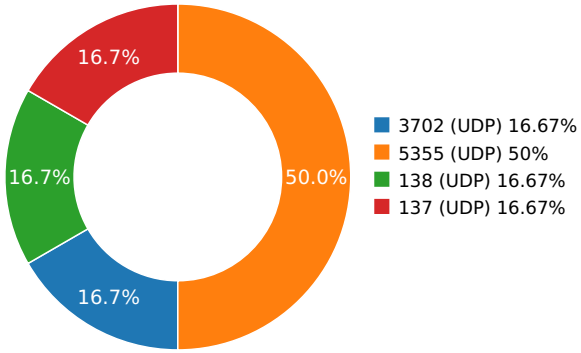
HKEY_CURRENT_USER\Software\WinRAR SFX
HKEY_CURRENT_USER\Software\WinRAR SFX\c%%

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
3.19393205643	Sandbox	224.0.0.252	5355
3.22236514091	Sandbox	224.0.0.252	5355
3.24097204208	Sandbox	239.255.255.250	3702
3.26640796661	Sandbox	192.168.56.255	137
5.78318309784	Sandbox	224.0.0.252	5355
9.26536417007	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\RarSFX0\VkLock V1.9.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 3f9b32e8c488ba5f4851a5306f07e440 **SHA-1 :** 4a7348185479d9c63a6678e45c59ee0df8b010a3 **SHA-256 :** 0686e65718d54b9f90ff0c313c4cc5728d1e34f2b **SHA-512 :** e26297b70124a7cf5d2817cb90e58da6e7f669da **Size :** 1672.67 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\Ssleay32.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386, for MS Windows **MD5 :** 557e5bae44dfae09c38d5480fa66fbf4 **SHA-1 :** a46e6443127a417cbc643a1f6c7206c019220afc **SHA-256 :** 72d5703b14bfb77ce6eb600cbcaebff164b55ead **SHA-512 :** a5b61cd3874771ee3504c2a6c213ad2c7bc83f0b **Size :** 209.92 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\Php5ts.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386, for MS Windows **MD5 :** c9aff68f6673fae7580527e8c76805b6 **SHA-1 :** bb62cc1db82cfe07a8c08a36446569dfc9c76d10 **SHA-256 :** 9b2c8b8c4cec301c4303f58ca4e8b261d516f10fe **SHA-512 :** c7836f46e535046562046fdd8d3264cd712a78c0 **Size :** 6831.616 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\Ext\Php_curl.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** e8977ab00a9c709195a931e264f71720 **SHA-1 :** cf5bf7185309f74b53da1fd3631191647a9c84cd **SHA-256 :** 4223cd949379213c38561399e99c62067b0b0d5 **SHA-512 :** d641a660907634a6373bc47c138d414a26f8278a **Size :** 443.904 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\Libeay32.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386, for MS Windows **MD5 :** a5b591cf17429ee27b4f2c8d19656aaa **SHA-1 :** ea5ba6d93f6dd1ea1b93a1926d1116a98184edae **SHA-256 :** 375b4cb49ce113498d94c78efac16a8a1eafb508f **SHA-512 :** 7c1300b5f10c131d4a79ce32cb1df292c760f4366 **Size :** 1019.904 Kilobytes.
C:\Users\User\AppData\Local\Temp\PSE20\3f9b32e8c488ba5f4851a5306f07e440\Php.Ini	**Type :** ASCII text, with CRLF, LF line terminators **MD5 :** e8ce9609d57c12e77bd3424d062ccb30 **SHA-1 :** 181453bb793367619ef0b437214c80505ecbcc48 **SHA-256 :** c5b64ff3e715abd23d3fe218596ba34d5ffb3dbf1 **SHA-512 :** cd890bc519b6f257c5c014ef3194db64b2d8a429 **Size :** 6.214 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	php.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	ccd3d0e091167fca1cfd06dfb3850c68730c64c1
MD5:	05c9668dc4efca3354a88dc773c4a736
First Seen Date:	2017-09-08 20:59:16.516353 (about a year ago)
Number Of Clients Seen:	5
Last Analysis Date:	2017-09-09 01:58:22.245400 (about a year ago)
Human Expert Analysis Date:	2017-09-09 06:24:04.472540 (about a year ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	6
Compilation Time Stamp	0x57B0C365 [Sun Aug 14 19:15:49 2016 UTC]
Entry Point	0x41cab5 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	5083446
Sha256	1c0c0664aa8be0f678a7d50727a519462aa7f6fe34409a4e97506c7a36a33f19
Mime Type	application/x-dosexec

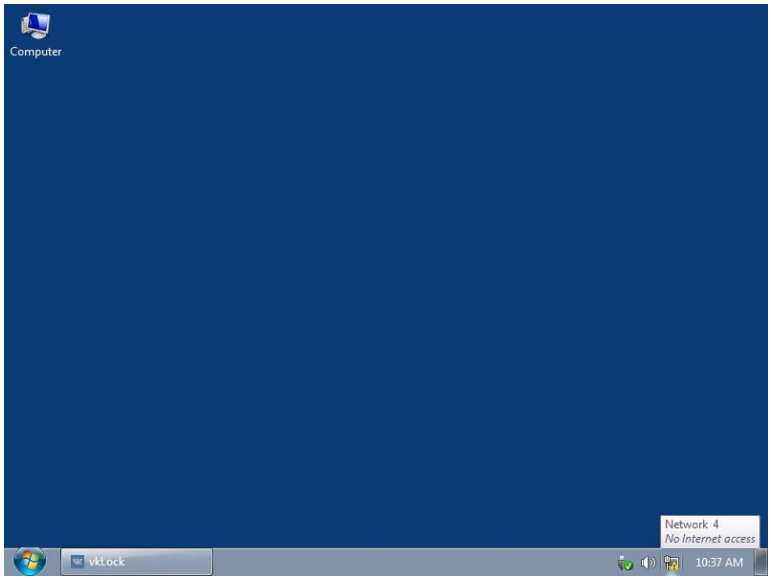
PE Sections

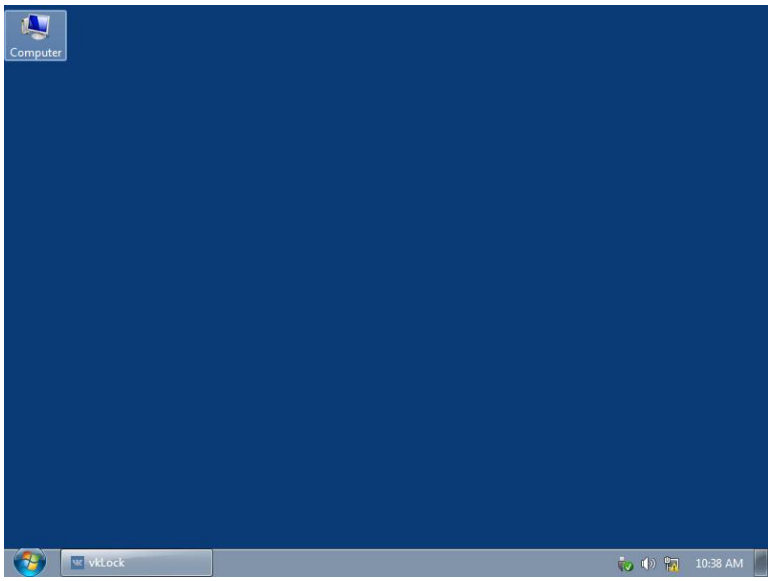
NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2dfe8	0x2e000	6.71024514176	2ae181684b1677561119f5765623448e
.rdata	0x2f000	0x99d0	0x9a00	5.15286519013	0e0f6a60d8fa917a060c8ef7becc0888
.data	0x39000	0x1f8b8	0xc00	3.29546719393	4e4aa728d9cced1622c2be27733e3fc5
.gfids	0x59000	0xf0	0x200	2.12366990435	c923099e27bf0e45a5c402d935d0620b
.rsrc	0x5a000	0x7660	0x7800	4.63785160881	6b3d45f596b89a11f579809f7fcb72cb
.reloc	0x62000	0x1f8c	0x2000	6.62985537968	d13d3f8a8adfe6861c49a01d81cf73ed

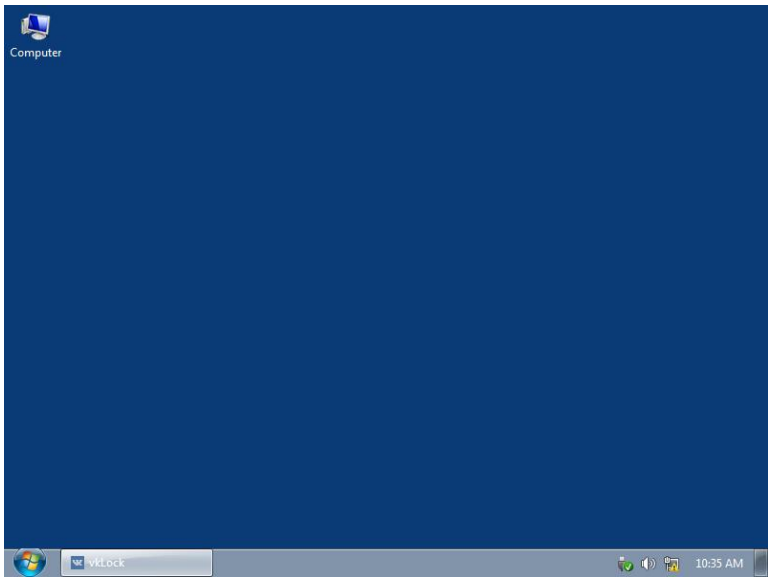
CERTIFICATE VALIDATION

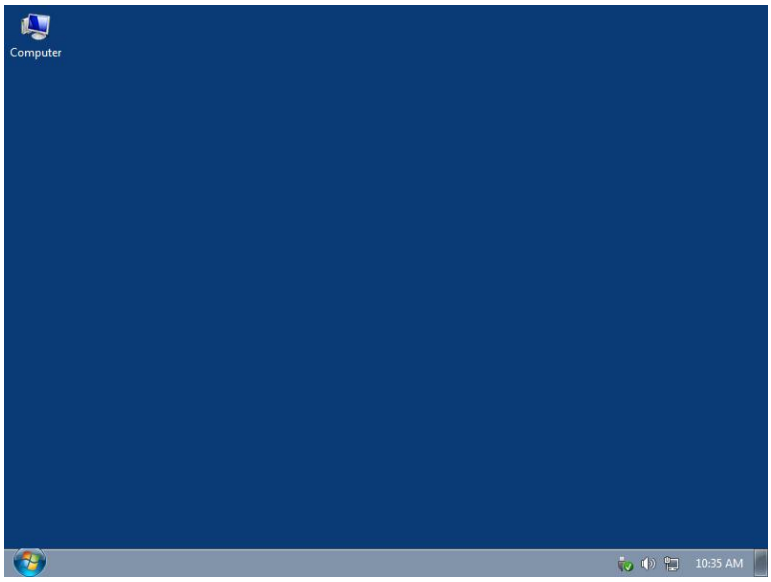
- Certificate Validation is not Applicable ?

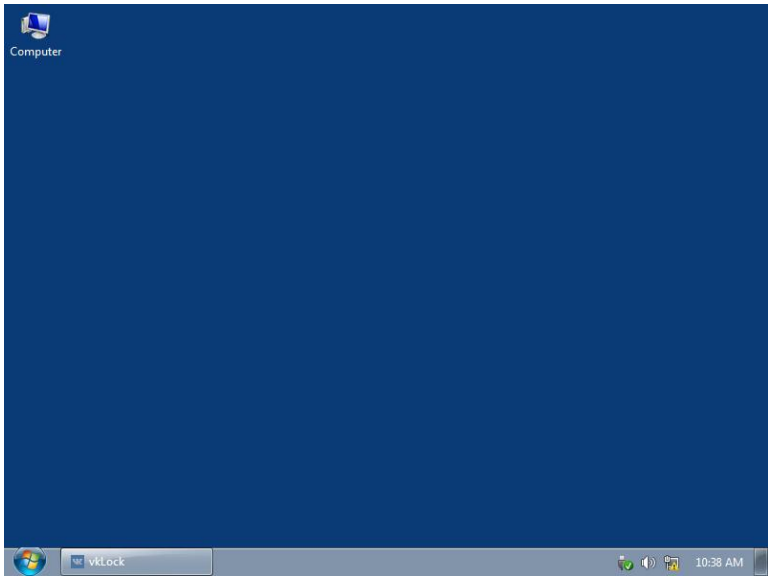
SCREENSHOTS

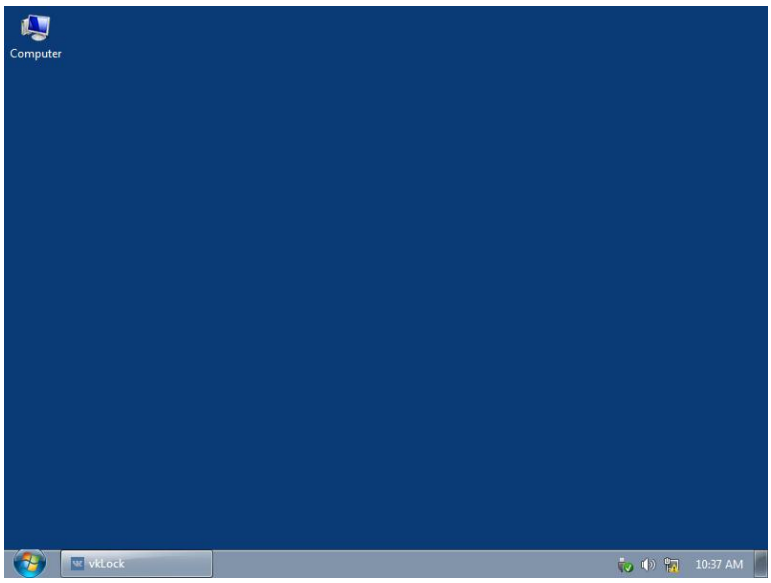

Computer
Network 4
No Internet access
vkLock
10:37 AM


Computer
vkLock
10:38 AM


Computer
vkLock
10:35 AM


Computer
10:35 AM


Computer
vkLock
10:38 AM


Computer
vkLock
10:37 AM