VALKYRIE COMODO

Summary

File Name: captainphillips2013dvdripx264sparksnzb_013-a4a___.exe

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

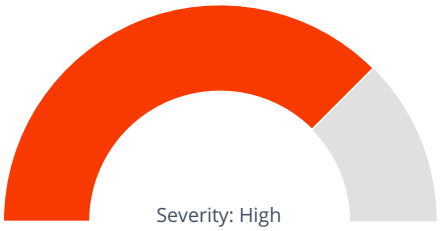
SHA1: 54f7533b1a92b258e7cd1a93f4fcb1a654d121b1

MD5: faa2f790c93c4d05697ca48d374c3364

MALWARE

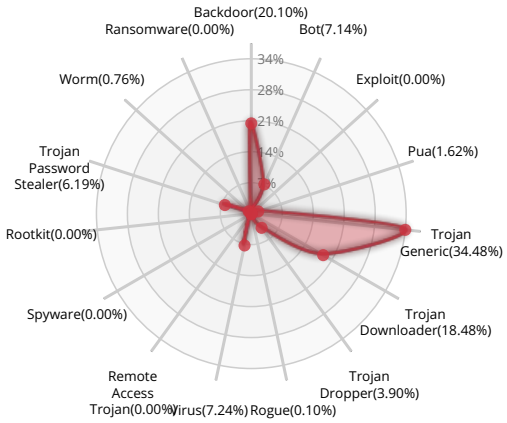
Valkyrie Final Verdict

DETECTION SECTION

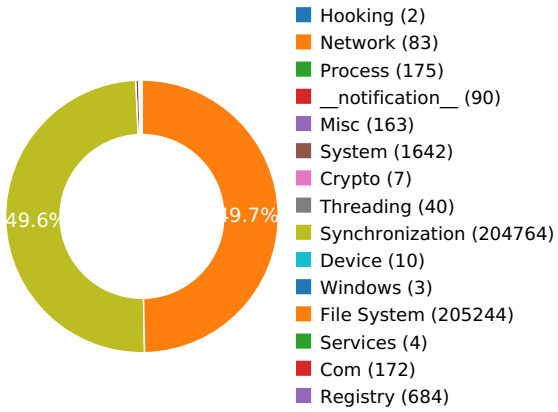


Verdict: Malware

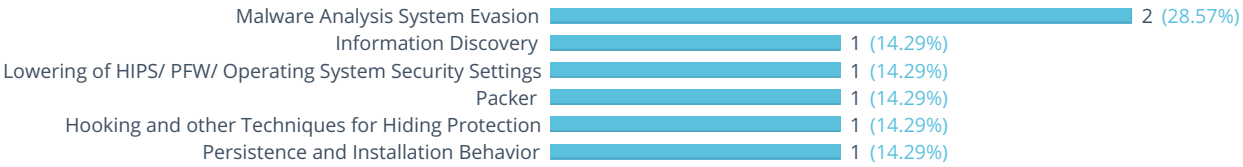
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys — Show sources

PACKER

The binary likely contains encrypted or compressed data. — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Attempts to interact with an Alternate Data Stream (ADS) — Show sources

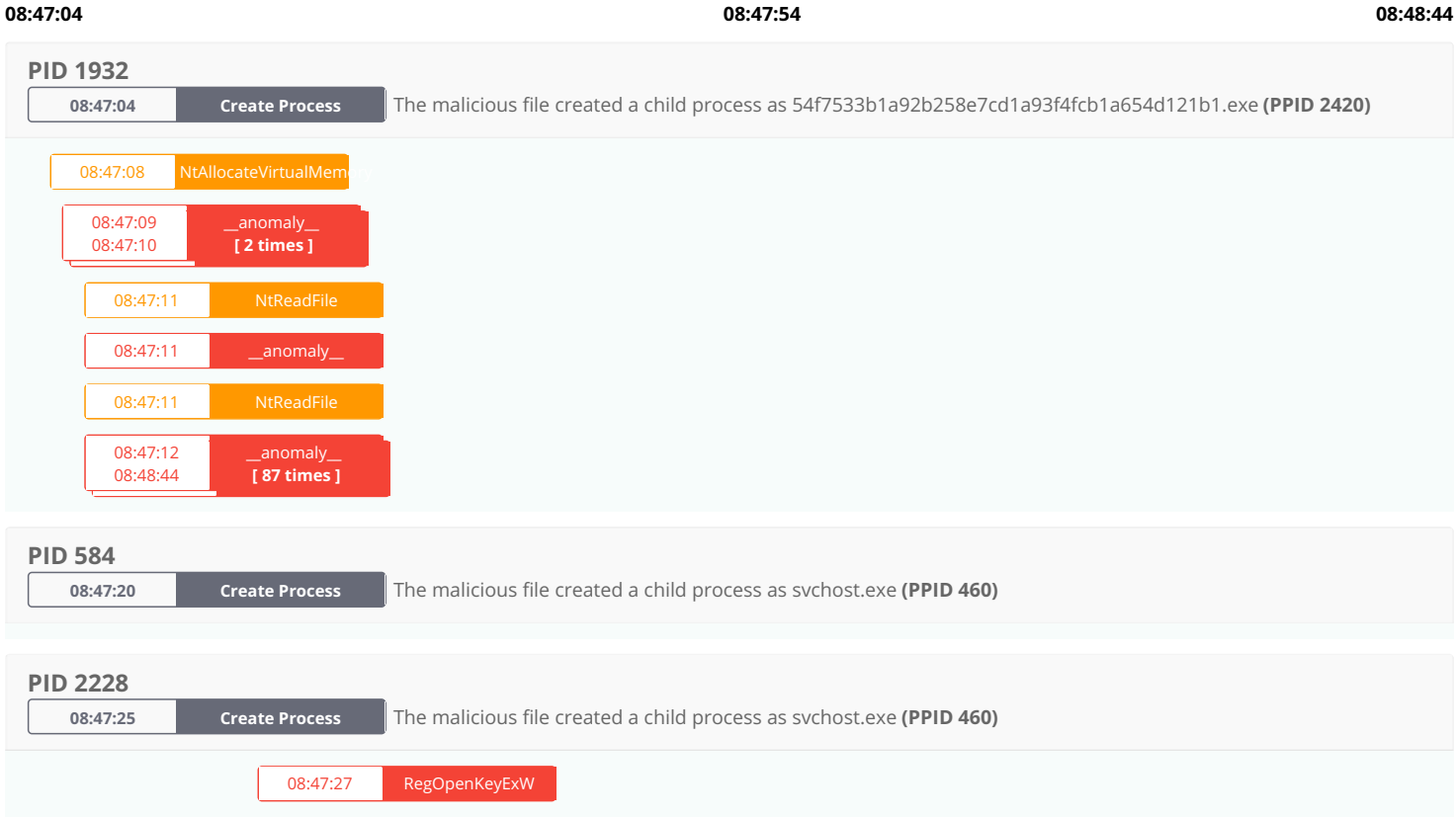
MALWARE ANALYSIS SYSTEM EVASION

Tries to unhook or modify Windows functions monitored by Cuckoo — Show sources

Spoofs its process name and/or associated pathname to appear as a legitimate process — Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\Temp\54f7533b1a92b258e7cd1a93f4fcb1a654d121b1.exe
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\54f7533b1a92b258e7cd1a93f4fcb1a654d121b1.exe:tmp
C:\Users\user\AppData\Local\Temp\54f7533b1a92b258e7cd1a93f4fcb1a654d121b1.exe.tmp
C:\Users\user\AppData\Local\Temp\54f7533b1a92b258e7cd1a93f4fcb1a654d121b1.exe:Zone.Identifier
C:\Windows\System32\en-US\wuapi.dll.mui
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32
C:\Windows\System32\
C:\Windows
C:\Windows\
C:
\??\MountPointManager
C:\
C:\Users\user\AppData\Local\Temp\comres.DLL
C:\Windows\System32\comres.dll
C:\Windows\System32\en-US\comres.DLL.mui
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\imageres.dll
C:\Windows\System32\imageres.dll
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository
C:\Windows\sysnative\wbem\Logs
C:\Windows\sysnative\wbem\AutoRecover
C:\Windows\sysnative\wbem\MOF
C:\Windows\sysnative\wbem\repository\INDEX.BTR
C:\Windows\sysnative\wbem\repository\WRITABLE.TST

C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\WBEM9xUpgd.dat
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Domain
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32\(Default)
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 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\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\Microsoft\WBEM\Tracing\WMI\SessionEnabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\Level
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\AreaFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\Session
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\LogFile
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\BufferSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\MinimumBuffers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\MaximumBuffers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\MaximumFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\LogFileMode
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\FlushTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Tracing\WMI\AgeLimit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress
HKEY_LOCAL_MACHINE\SYSTEM\Setup\UpgradeInProgress
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\VSS\Settings\ActiveWriterStateTimeout
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\VSS\Diag\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\VSS\Settings\TornComponentsMax
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{00000100-0000-0000-C000-000000000046}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{609B9555-4FB6-11D1-9971-00C04FBBB345}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{609B9557-4FB6-11D1-9971-00C04FBBB345}\ProxyStubClsid32\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{F309AD18-D86A-11D0-A075-00C04FB68820}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\InProcServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\InProcServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\IdentifierLimit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\QueryLimit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\PathLimit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ArbThrottlingEnabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ArbSystemHighMaxLimitFactor
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ArbTaskMaxSleep
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ArbSystemHighThreshold1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ArbSystemHighThreshold1Mult
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ArbSystemHighThreshold2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ArbSystemHighThreshold2Mult

MODIFIED FILES

\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\WRITABLE.TST
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.VirtualAlloc

kernel32.dll.GetModuleHandleA
kernel32.dll.LoadLibraryA
kernel32.dll.VirtualProtect
kernel32.dll.ExitProcess
kernel32.dll.Sleep
kernel32.dll.GetTickCount
kernel32.dll.GetProcessHeap
winscard.dll.SCardIntroduceCardTypeA
kernel32.dll.OpenProcess
kernel32.dll.SetLastError
kernel32.dll.CreateProcessW
kernel32.dll.lstrlenW
kernel32.dll.LocalAlloc
kernel32.dll.GetTempPathW
kernel32.dll.QueryDosDeviceW
kernel32.dll.GetFullPathNameW
kernel32.dll.GetLongPathNameW
kernel32.dll.GetModuleFileNameW
kernel32.dll.MoveFileExW
kernel32.dll.ExpandEnvironmentStringsW
kernel32.dll.WideCharToMultiByte
kernel32.dll.MultiByteToWideChar
kernel32.dll.GetFileAttributesW
kernel32.dll.GetVersion
kernel32.dll.GetFileInformationByHandle
kernel32.dll.CopyFileW
kernel32.dll.DeleteFileW
kernel32.dll.IsBadWritePtr
kernel32.dll.SetFilePointer
kernel32.dll.CreateToolhelp32Snapshot
kernel32.dll.Process32FirstW
kernel32.dll.GetProcessTimes
kernel32.dll.Process32NextW
kernel32.dll.GetCurrentProcessId

kernel32.dll.LoadLibraryExW
kernel32.dll.FreeLibrary
kernel32.dll.SetProcessShutdownParameters
kernel32.dll.TlsAlloc
kernel32.dll.TlsGetValue
kernel32.dll.TlsSetValue
kernel32.dll.GlobalAlloc
kernel32.dll.GlobalLock
kernel32.dll.GlobalUnlock
kernel32.dll.GlobalFree
kernel32.dll.GetEnvironmentVariableW
kernel32.dll.GetLocaleInfoW
kernel32.dll.GetComputerNameW
kernel32.dll.ReadProcessMemory
kernel32.dll.FileTimeToLocalFileTime
kernel32.dll.FileTimeToSystemTime
kernel32.dll.TerminateProcess
kernel32.dll.GetCurrentProcess
kernel32.dll.LoadLibraryW
kernel32.dll.TryEnterCriticalSection
kernel32.dll.SetEnvironmentVariableA
kernel32.dll.CompareStringW
kernel32.dll.CompareStringA
kernel32.dll.WriteConsoleW
kernel32.dll.GetConsoleOutputCP
kernel32.dll.WriteConsoleA
kernel32.dll.SetStdHandle
kernel32.dll.GetConsoleMode
kernel32.dll.GetConsoleCP
kernel32.dll.GetStringTypeW
kernel32.dll.GetStringTypeA
kernel32.dll.ReadFile
kernel32.dll.GetLocaleInfoA
kernel32.dll.GetTimeZoneInformation
kernel32.dll.GetStartupInfoA

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\System\DNSclient
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Domain
HKEY_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Classes\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_CURRENT_USER\Software\Classes\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocHandler32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocHandler
HKEY_CURRENT_USER\Software\Classes\Interface\{027947E1-D731-11CE-A357-000000000001}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\Progid

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocHandler32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocHandler
HKEY_CURRENT_USER\Software\Classes\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32\(Default)
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 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\CTF\Compatibility_____
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

READ FILES

C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\Temp\54f7533b1a92b258e7cd1a93f4fcb1a654d121b1.exe
C:\Windows\System32\en-US\wuapi.dll.mui
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\comres.dll
C:\Windows\System32\en-US\comres.DLL.mui
C:\Windows\Fonts\staticcache.dat
C:\Windows\System32\imageres.dll
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM

MUTEXES

IESQMMUTEX_0_208
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

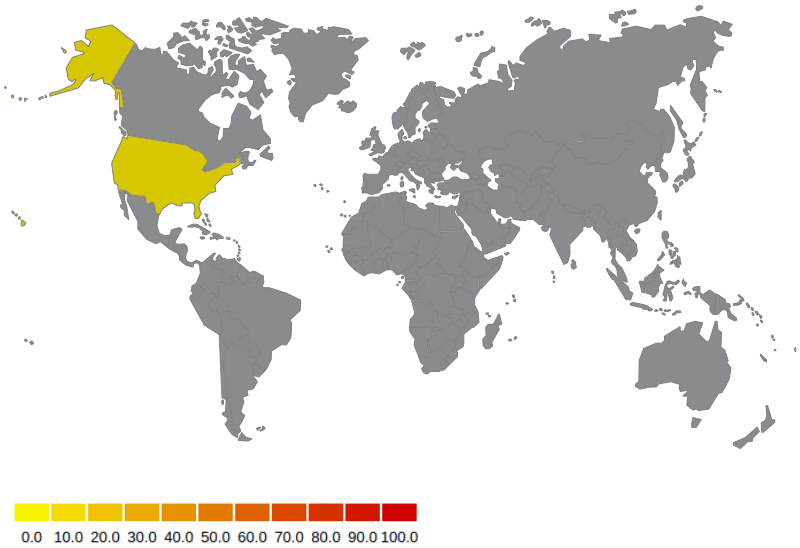
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server

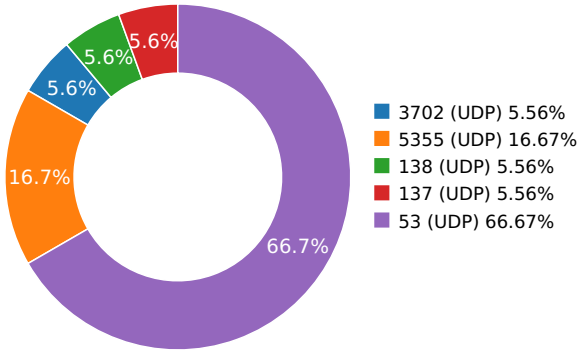
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider

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
dyrjwivnsayi.indeedbranch.ru	52.209.50.254	United States	16509	Amazon Data Services Irelan...	Malware Process

DNS QUERIES

Request	Type
dyrjwivnsayi.indeedbranch.ru	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.09762692451	Sandbox	224.0.0.252	5355
3.11642503738	Sandbox	224.0.0.252	5355
3.1227478981	Sandbox	239.255.255.250	3702
3.16163492203	Sandbox	192.168.56.255	137
5.7707118988	Sandbox	224.0.0.252	5355
9.16138887405	Sandbox	192.168.56.255	138
31.0779459476	Sandbox	8.8.4.4	53
32.066847086	Sandbox	8.8.8.8	53
43.0833399296	Sandbox	8.8.8.8	53
44.0828149319	Sandbox	8.8.4.4	53
55.116642952	Sandbox	8.8.8.8	53
56.1145269871	Sandbox	8.8.4.4	53
73.3020460606	Sandbox	8.8.8.8	53
74.3015139103	Sandbox	8.8.4.4	53
85.302521944	Sandbox	8.8.8.8	53
86.3013319969	Sandbox	8.8.4.4	53
97.3036179543	Sandbox	8.8.8.8	53
98.3012869358	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	captainphillips2013dvdripx264sparksnzb_013-a4a___.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	54f7533b1a92b258e7cd1a93f4fcb1a654d121b1
MD5:	faa2f790c93c4d05697ca48d374c3364
First Seen Date:	2017-10-18 01:33:25.550454 (about a year ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-10-20 08:46:42.556381 (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	5
Compilation Time Stamp	0x59E37EA1 [Sun Oct 15 15:28:33 2017 UTC]
LegalCopyright	Copyright (C) 2017
ProductVersion	3, 2, 23, 4348
FileVersion	3, 2, 23, 4348
ProductName	Anime catron Application
Translation	0x0409 0x04b0
Entry Point	0x40918a (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1586152
Sha256	64cce2ef68063ce8265a52530d776645af9117bc7cd831d76f0e85042d42a169
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x16e48	0x17000	5.80670892908	acc5c8e6031d4a3264d4643887916361
.data	0x18000	0xa0c48	0xa0000	6.41254353129	7ad4bf5fb0191ebb8775f0b2eae13e44
.tls	0xb9000	0x78bc	0x8000	2.04546043	146114093fc8ec6efb435b9e1a5aedea
.rsrc	0xc1000	0xbed70	0xbf000	7.52324801101	454c41705d349a432bc839f3ea367096
.reloc	0x180000	0x20be	0x3000	2.3702076093	1065c69b9cd9d39cc1f8d9915f33ab6f

PE Imports

- KERNEL32.dll
  - SetEvent
  - InterlockedIncrement
  - GetBinaryTypeA
  - GetProcAddress
  - LoadLibraryA
  - GetFileSize
  - GetCurrentThread
  - InterlockedExchange
  - CreateFileA
  - WriteConsoleW
  - GetConsoleOutputCP
  - GetTempPathA
  - Sleep
  - GetSystemDirectoryA
  - SetThreadPriority
  - LockResource

    - GetTickCount
    - WriteConsoleA
    - CloseHandle
    - HeapSize
    - RaiseException
    - GetCommandLineA
    - HeapFree
    - GetVersionExA
    - HeapAlloc
    - GetProcessHeap
    - GetStartupInfoA
    - EnterCriticalSection
    - LeaveCriticalSection
    - TerminateProcess
    - GetCurrentProcess
    - UnhandledExceptionFilter
    - SetUnhandledExceptionFilter
    - IsDebuggerPresent
    - GetModuleHandleA
    - MultiByteToWideChar
    - GetLastError
    - ReadFile
    - ExitProcess
    - WriteFile
    - GetStdHandle
    - GetModuleFileNameA
    - FreeEnvironmentStringsA
    - GetEnvironmentStrings
    - FreeEnvironmentStringsW
    - WideCharToMultiByte
    - GetEnvironmentStringsW
    - SetHandleCount
    - GetFileType
    - DeleteCriticalSection
    - TlsGetValue
    - TlsAlloc
    - TlsSetValue
    - TlsFree
    - SetLastError
    - GetCurrentThreadId
    - InterlockedDecrement
    - HeapDestroy
    - HeapCreate
    - VirtualFree
    - QueryPerformanceCounter
    - GetCurrentProcessId
    - GetSystemTimeAsFileTime
    - GetCPInfo
    - GetACP
    - GetOEMCP
    - RtlUnwind
    - SetFilePointer
    - SetStdHandle
    - InitializeCriticalSection
    - VirtualAlloc
    - HeapReAlloc
    - GetConsoleCP
    - GetConsoleMode
    - FlushFileBuffers
    - LCMapStringA
    - LCMapStringW
    - GetStringTypeA
    - GetStringTypeW
    - GetLocaleInfoA
- USER32.dll
    - GetDC
    - EnableWindow
    - GetClientRect
    - LoadImageW
    - LoadBitmapA
- GDI32.dll
    - SelectObject
    - GetDeviceCaps
    - CreatePen
    - CreateBitmap

- SetPixel
- ole32.dll
  - CoUninitialize
- OLEAUT32.dll
  - VariantInit
- WS2_32.dll
  - recv
  - closesocket

PE Resources

RT_BITMAP
RT_ICON
RT_GROUP_ICON
RT_VERSION
RT_MANIFEST

CERTIFICATE VALIDATION

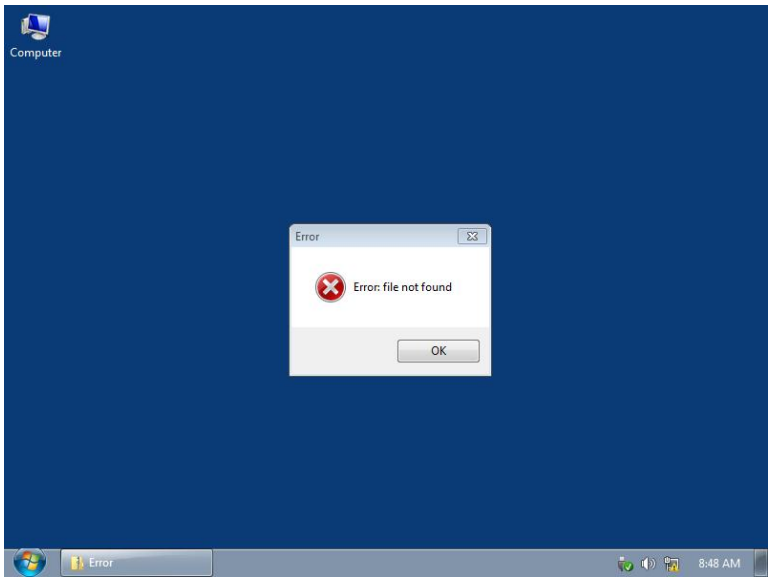
- Success ✔

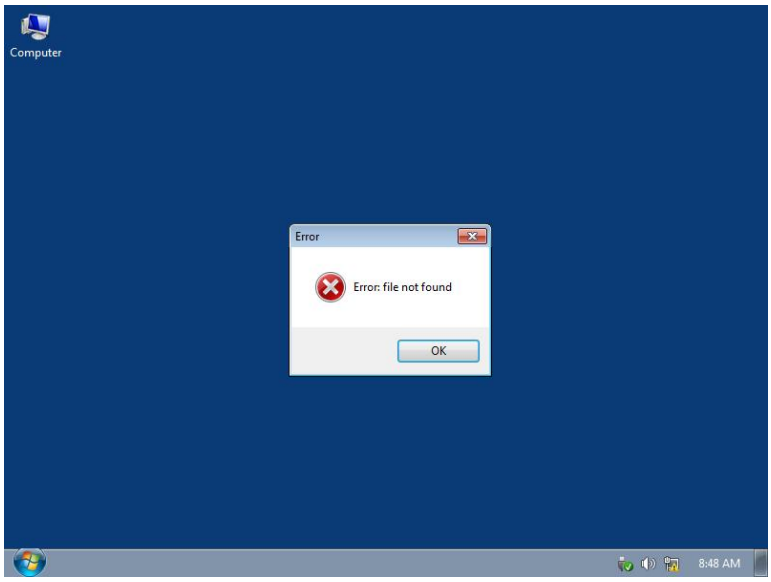
[+] COMODO RSA Certification Authority	
Status	NoError ✔
Start Date	2010-01-19 00:00:00
End Date	2038-01-18 23:59:59
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	null
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

[+] COMODO RSA Code Signing CA	
Status	NoError ✔
Start Date	2013-05-09 00:00:00
End Date	2028-05-08 23:59:59
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	{"Digital Signature","Certificate Signing","Off-line CRL Signing","CRL Signing (86)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

[+] OOO SUNDUS	
Status	NoError ✔
Start Date	2017-10-02 00:00:00
End Date	2018-06-02 23:59:59
Sha256	9f2525d06d1f0a17c612a2eeec44173b04794603a69c29670ba154461c3dc17f
Serial	00B15257A2E6860C26F34383023F5BECD2
Subject Key Identifier	da c5 2f 1e f2 ee 2f ec f9 44 1a 34 64 8a c0 c7 50 cc f1 ad
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.crl
Key Usage	{"Digital Signature (80)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

SCREENSHOTS




Computer
Error
Error: file not found
OK
8:48 AM


Computer
8:47 AM


Computer
8:48 AM


Computer
8:48 AM