VALKYRIE COMODO

Summary

File Name: dio-562-rukovodstvo-po-ekspluatatsii_6d4-06d___.exe

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

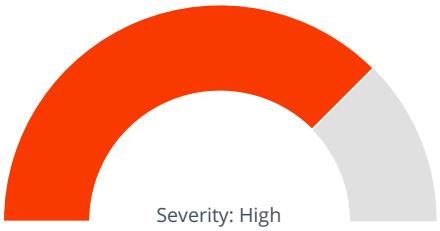
SHA1: 89c0d3c4f1b0d988898e05bb79a67e56848a6b5a

MD5: e8ffa734ea0fa052867dcb4c350ea49b

MALWARE

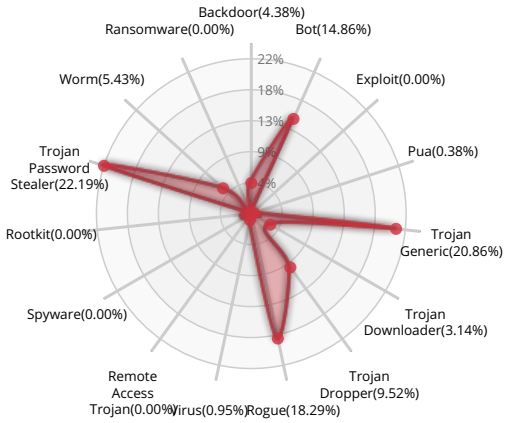
Valkyrie Final Verdict

DETECTION SECTION

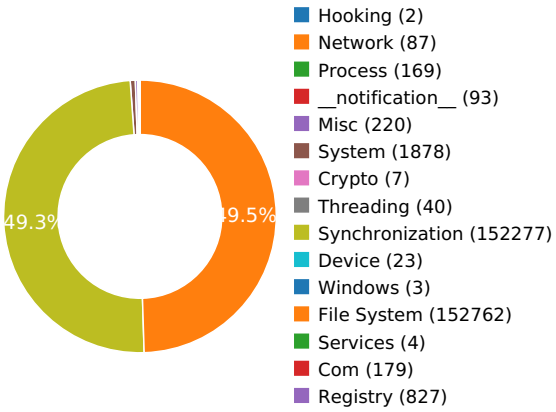


Verdict: Malware

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

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

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

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

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

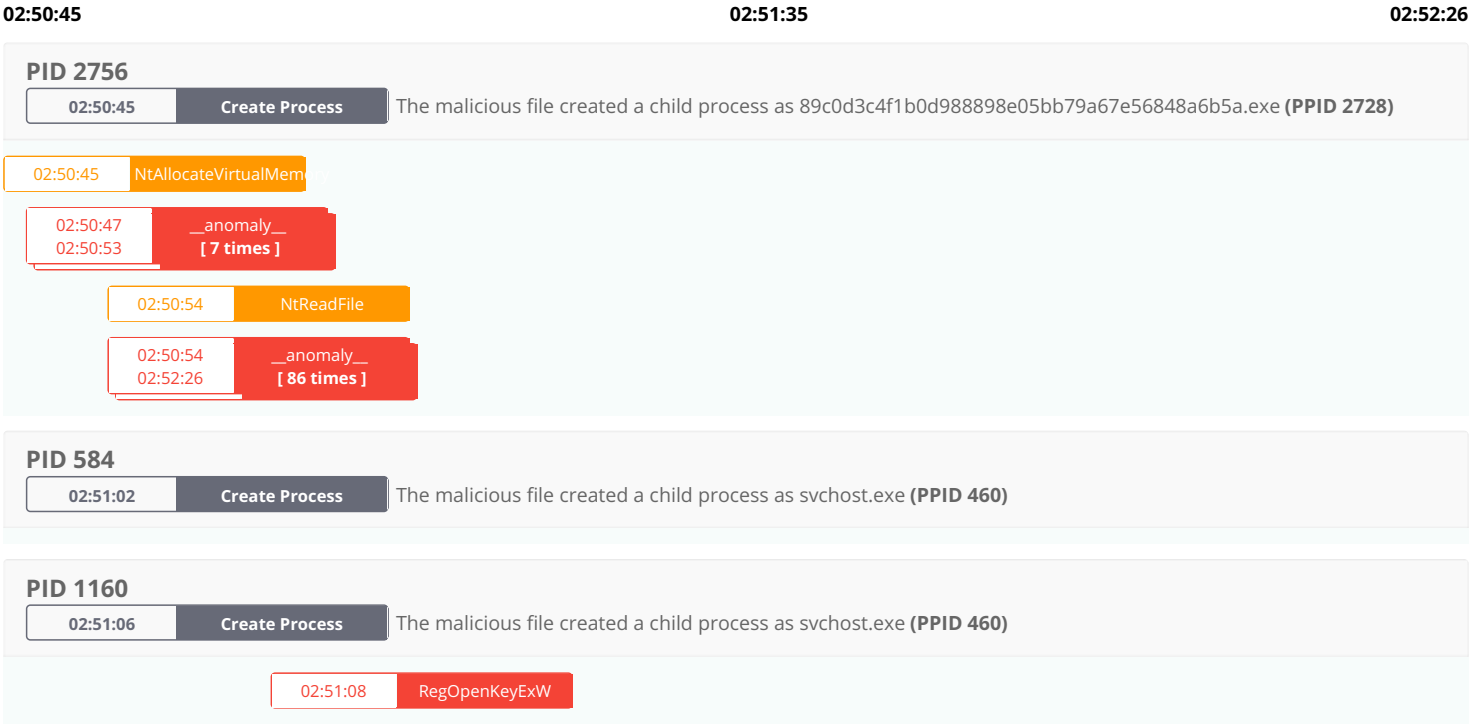
Creates RWX memory — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

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

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\zzkdkd
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\Temp\89c0d3c4f1b0d988898e05bb79a67e56848a6b5a.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\89c0d3c4f1b0d988898e05bb79a67e56848a6b5a.exe:tmp
C:\Users\user\AppData\Local\Temp\89c0d3c4f1b0d988898e05bb79a67e56848a6b5a.exe.tmp
C:\Users\user\AppData\Local\Temp\89c0d3c4f1b0d988898e05bb79a67e56848a6b5a.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:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\ProgramData\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\ras*.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk*.pbk
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\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoProxyDetectType
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
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\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
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

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.GetModuleHandleA

kernel32.dll.VirtualAlloc
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.InitializeCriticalSectionAndSpinCount
kernel32.dll.GetStringTypeW
kernel32.dll.GetStringTypeA
kernel32.dll.ReadFile
kernel32.dll.GetLocaleInfoA
kernel32.dll.GetTimeZoneInformation
kernel32.dll.GetStartupInfoA

kernel32.dll.GetFileType
kernel32.dll.SetHandleCount
kernel32.dll.GetEnvironmentStringsW
kernel32.dll.FreeEnvironmentStringsW
kernel32.dll.IsValidCodePage

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_CURRENT_USER\Software\Classes\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocHandler32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocHandler
HKEY_LOCAL_MACHINE\Software\Microsoft\OleAut
HKEY_CURRENT_USER\Software\Classes\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision

READ FILES

C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\Temp\89c0d3c4f1b0d988898e05bb79a67e56848a6b5a.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

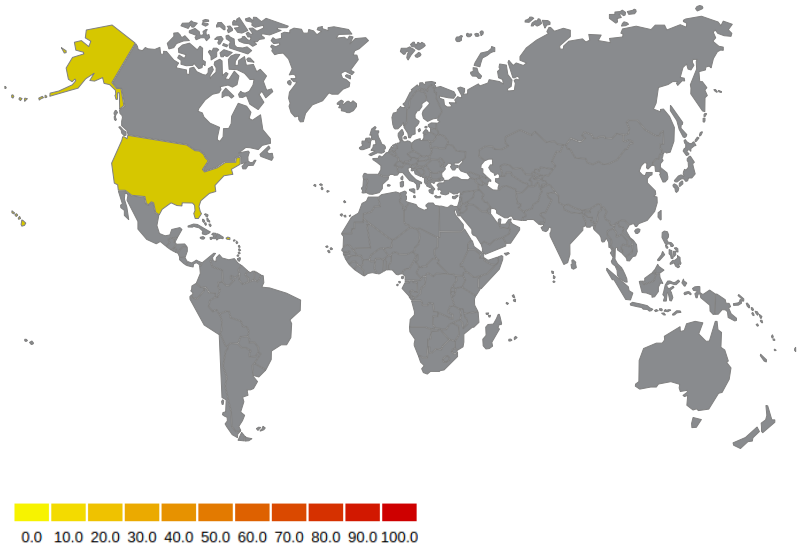
Local\MSCTF.CtfMonitorInstMutexDefault1

MODIFIED REGISTRY KEYS

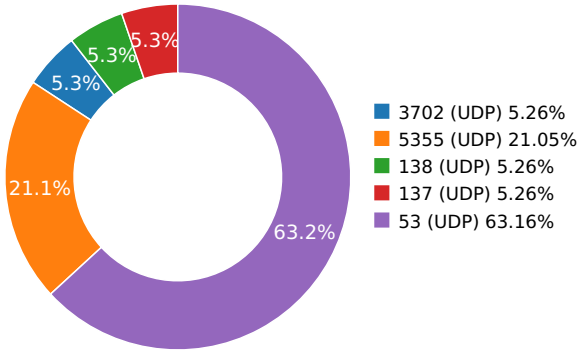
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
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
vtfhmtgqjmnp.awfultoworse.ru	34.241.199.8	United States	16509	Amazon Data Services Irelan...	Malware Process

DNS QUERIES

Request	Type
vtfhmtgqjmnp.awfultoworse.ru	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.03753781319	Sandbox	224.0.0.252	5355
3.03871178627	Sandbox	224.0.0.252	5355
3.04798698425	Sandbox	239.255.255.250	3702
3.08618378639	Sandbox	192.168.56.255	137
5.59580183029	Sandbox	224.0.0.252	5355
9.07922577858	Sandbox	192.168.56.255	138
29.8792529106	Sandbox	224.0.0.252	5355
32.7942388058	Sandbox	8.8.4.4	53
33.7814719677	Sandbox	8.8.8.8	53
44.8158028126	Sandbox	8.8.8.8	53
45.8124299049	Sandbox	8.8.4.4	53
56.8410849571	Sandbox	8.8.8.8	53
57.8278918266	Sandbox	8.8.4.4	53
71.4120008945	Sandbox	8.8.8.8	53
72.406482935	Sandbox	8.8.4.4	53
83.4070668221	Sandbox	8.8.8.8	53
84.4067459106	Sandbox	8.8.4.4	53
95.4235208035	Sandbox	8.8.8.8	53
96.4220399857	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:	dio-562-rukovodstvo-po-ekspluatatsii_6d4-06d___.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	89c0d3c4f1b0d988898e05bb79a67e56848a6b5a
MD5:	e8ffa734ea0fa052867dcb4c350ea49b
First Seen Date:	2017-11-15 16:53:40.895206 (about a year ago)
Number Of Clients Seen:	4
Last Analysis Date:	2017-11-16 21:10:07.508281 (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	3
Compilation Time Stamp	0x5A0C58EC [Wed Nov 15 15:10:36 2017 UTC]
Entry Point	0x56174c (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1582072
Sha256	49b1601b48cb1558aaefc2c9219294e3bfcb3e3bef36a3aea28ad57f7c894bbb
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x160dce	0x161000	6.05168265249	5852ea035134bb142e094dbfc7c3b178
.data	0x162000	0x162d4	0x17000	0.663575259041	fd8c4e12a7d57c10da96e38a44216202
.rsrc	0x179000	0x7d10	0x8000	5.2233483947	de4bc38e8e1b15e5c7bd0ef79077110d

CERTIFICATE VALIDATION

- Success ✔

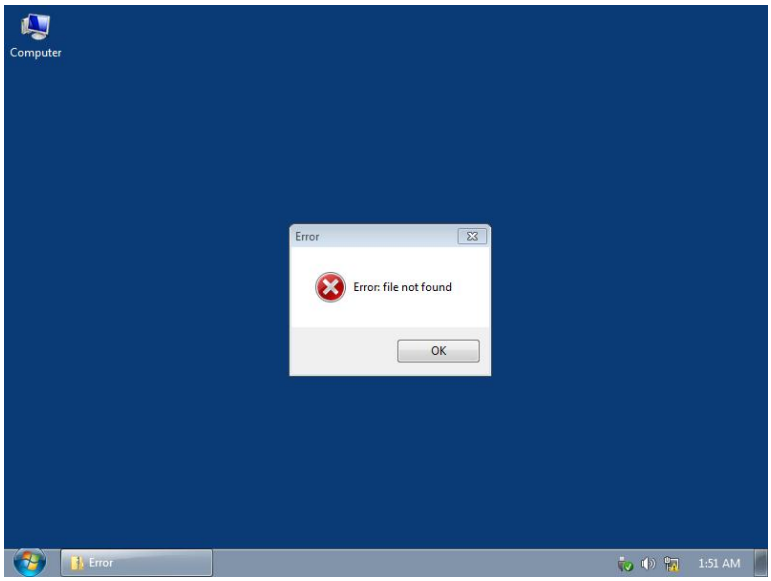
[+] COMODO RSA Certification Authority	
Status	NoError ✔
Start Date	2010-01-19 00:00:00
End Date	2038-01-18 23:59:59
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 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

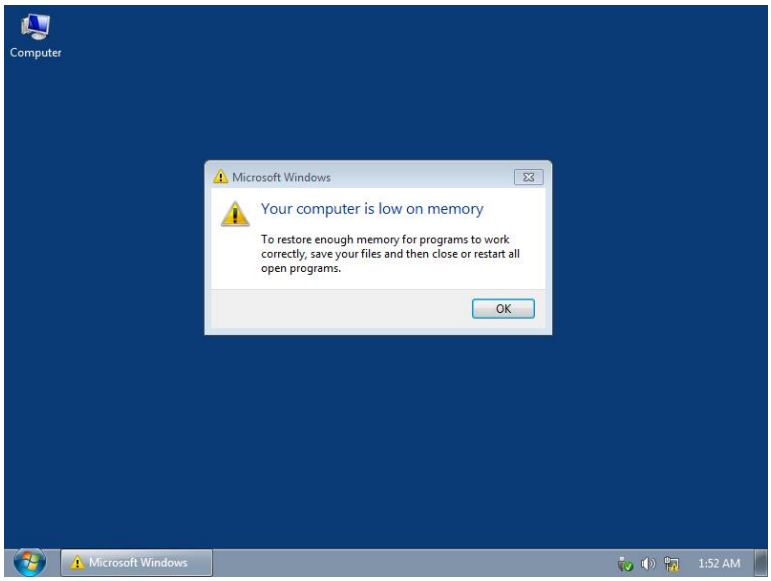
[+] COMODO RSA Code Signing CA	
Status	NoError ✔
Start Date	2013-05-09 00:00:00
End Date	2028-05-08 23:59:59
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 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, Gorko	
Status	NoError ✔
Start Date	2017-11-07 00:00:00
End Date	2018-07-18 23:59:59
Sha256	43f16fee15d8ec52776c09118f52e334801f9db8113a7f2ed22eaaf2b925a899
Serial	4FAB82DAFCDED6B0D22FF95E14C6140C
Subject Key Identifier	6e 5f 50 e8 a7 bd 29 e6 8b 05 a3 94 bf 05 44 34 78 91 5a a4
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)"}

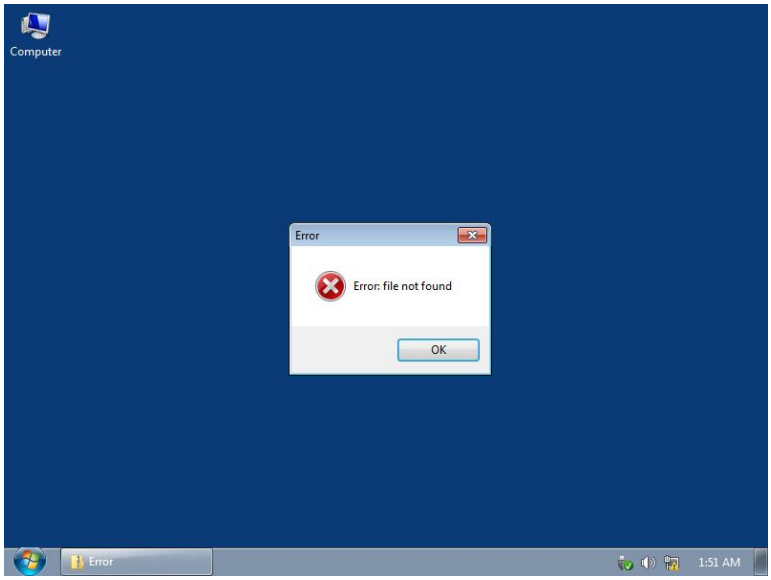
SCREENSHOTS

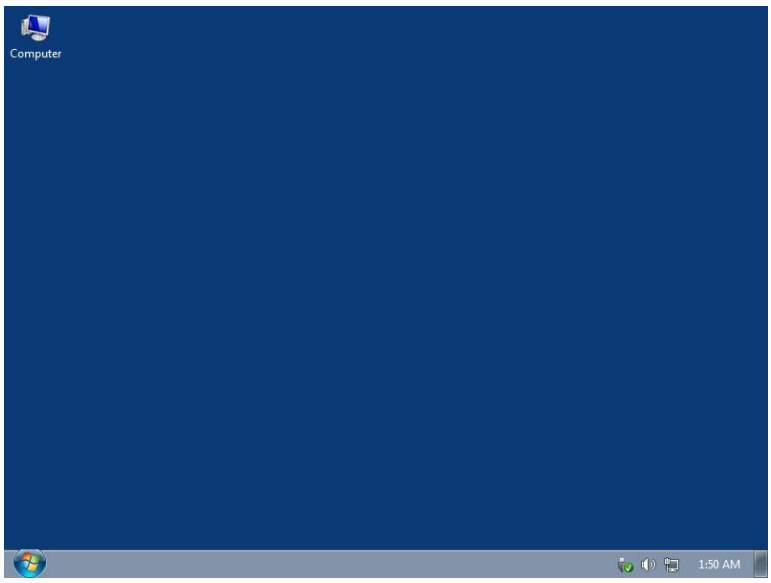

Computer
1:52 AM

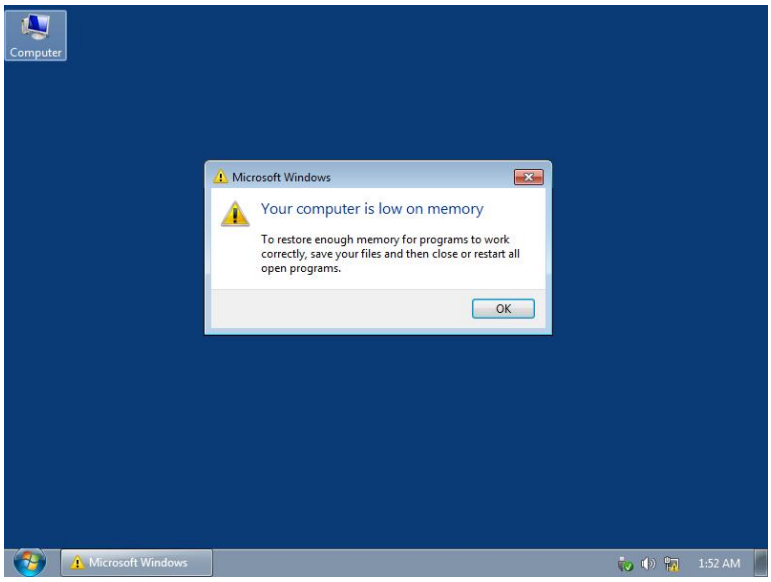

Computer
Error
Error: file not found
OK
Error
1:51 AM


Computer
Microsoft Windows
Your computer is low on memory
To restore enough memory for programs to work correctly, save your files and then close or restart all open programs.
OK
Microsoft Windows
1:52 AM


Computer
1:52 AM


Computer
Error
Error: file not found
OK
Error
1:51 AM


Computer
1:50 AM


Computer
Microsoft Windows
Your computer is low on memory
To restore enough memory for programs to work correctly, save your files and then close or restart all open programs.
OK
Microsoft Windows
1:52 AM


Computer
1:51 AM