now.exe

Is DLL ✗ | Packer ✓ | Anti Debug ✓ | Anti VM ✗ | Signed ✗ | XOR ✗

MalFamily: Nanocore **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
File size:	792.50 KB (811520 bytes)
Compile time:	1992-04-29 10:21:53
MD5:	1ed9d00252dead6ea2256a0e1af1aafd
SHA1:	bf341ad7e08f99134b09a160deede74ca0162072
Import hash:	b2dd322e598d313486710f40e7d0f709
Submitted:	2019-01-25 02:09:16

URL(s) file hosting

http://7bwh.com/wp-content/plugins/Ultimate_VC_Addons/admin/ifeanyi/now.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2019-01-23 21:43:13	50/69	

Import library

comdlg32.dll
VERSION.dll
GDI32.dll
KERNEL32.dll

OLEAUT32.dll
ADVAPI32.dll
USER32.dll
comctl32.dll

18 Behaviors detected by system signatures

Domain Sinkholed or blacklisted

- Alert: Honeypot blocked domain: 99grams.ddns.net

Anomalous binary characteristics

- anomaly: Timestamp on binary predates the release date of the OS version it requires by at least a year

Collects information to fingerprint the system

Creates a copy of itself

- copy: C:\Program Files (x86)\UPNP Subsystem\upnpss.exe

Exhibits behavior characteristic of Nanocore RAT

Installs itself for autorun at Windows startup

- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\UPNP Subsystem
- data: C:\Program Files (x86)\UPNP Subsystem\upnpss.exe

Tries to unhook or modify Windows functions monitored by Cuckoo

- unhook: function_name: NtCreateSection, type: modification

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Local\Temp\now.exe:Zone.Identifier

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

- Injection: now.exe(2072) -> now.exe(2332)

The binary likely contains encrypted or compressed data.

- section: name: .rsrc, entropy: 7.35, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_SHARED|IMAGE_SCN_MEM_READ, raw_size: 0x0003d000, virtual_size: 0x0003ce68

Reads data out of its own binary image

- self_read: process: now.exe, pid: 2332, offset: 0x00000000, length: 0x00001000
- self_read: process: now.exe, pid: 2332, offset: 0x00000100, length: 0x00000200

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: v2.0.50727

Dynamic (imported) function loading detected

- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled

- DynamicLoader: GDI32.dll/GetLayout
- DynamicLoader: GDI32.dll/GdiRealizationInfo
- DynamicLoader: GDI32.dll/FontIsLinked
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: GDI32.dll/GetFontAssocStatus
- DynamicLoader: ADVAPI32.dll/RegQueryValueExA
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: GDI32.dll/GetTextFaceAliasW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: user32.dll/AnimateWindow
- DynamicLoader: comctl32.dll/InitializeFlatSB
- DynamicLoader: comctl32.dll/UninitializeFlatSB
- DynamicLoader: comctl32.dll/FlatSB_GetScrollProp
- DynamicLoader: comctl32.dll/FlatSB_SetScrollProp
- DynamicLoader: comctl32.dll/FlatSB_EnableScrollBar
- DynamicLoader: comctl32.dll/FlatSB_ShowScrollBar
- DynamicLoader: comctl32.dll/FlatSB_GetScrollRange
- DynamicLoader: comctl32.dll/FlatSB_GetScrollInfo
- DynamicLoader: comctl32.dll/FlatSB_GetScrollPos
- DynamicLoader: comctl32.dll/FlatSB_SetScrollPos
- DynamicLoader: comctl32.dll/FlatSB_SetScrollInfo
- DynamicLoader: comctl32.dll/FlatSB_SetScrollRange
- DynamicLoader: user32.dll/SetLayeredWindowAttributes
- DynamicLoader: now.exe/K36D1bUhrrXbjTOfBXfWIc
- DynamicLoader: kernel32.dll/GetModuleHandleW
- DynamicLoader: kernel32.dll/VirtualFree
- DynamicLoader: kernel32.dll/LoadLibraryW
- DynamicLoader: kernel32.dll/SizeofResource
- DynamicLoader: kernel32.dll/GetModuleFileNameW
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/MultiByteToWideChar
- DynamicLoader: kernel32.dll/FlushInstructionCache
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: kernel32.dll/VirtualAlloc
- DynamicLoader: kernel32.dll/LoadLibraryA
- DynamicLoader: kernel32.dll/GetModuleFileNameA
- DynamicLoader: kernel32.dll/GetModuleHandleA
- DynamicLoader: kernel32.dll/VirtualProtect
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/LoadResource
- DynamicLoader: kernel32.dll/FindResourceW
- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/GetFileSize
- DynamicLoader: kernel32.dll/LCMapStringW
- DynamicLoader: kernel32.dll/LCMapStringA
- DynamicLoader: kernel32.dll/GetStringTypeW
- DynamicLoader: kernel32.dll/GetStringTypeA
- DynamicLoader: kernel32.dll/HeapAlloc
- DynamicLoader: kernel32.dll/GetStartupInfoW
- DynamicLoader: kernel32.dll/DeleteCriticalSection
- DynamicLoader: kernel32.dll/LeaveCriticalSection
- DynamicLoader: kernel32.dll/EnterCriticalSection
- DynamicLoader: kernel32.dll/HeapFree
- DynamicLoader: kernel32.dll/HeapReAlloc
- DynamicLoader: kernel32.dll/HeapCreate
- DynamicLoader: kernel32.dll/Sleep
- DynamicLoader: kernel32.dll/ExitProcess

- DynamicLoader: kernel32.dll/WriteFile
- DynamicLoader: kernel32.dll/GetStdHandle
- DynamicLoader: kernel32.dll/SetUnhandledExceptionFilter
- DynamicLoader: kernel32.dll/FreeEnvironmentStringsW
- DynamicLoader: kernel32.dll/GetEnvironmentStringsW
- DynamicLoader: kernel32.dll/GetCommandLineW
- DynamicLoader: kernel32.dll/SetHandleCount
- DynamicLoader: kernel32.dll/GetFileType
- DynamicLoader: kernel32.dll/GetStartupInfoA
- DynamicLoader: kernel32.dll/TlsGetValue
- DynamicLoader: kernel32.dll/TlsAlloc
- DynamicLoader: kernel32.dll/TlsSetValue
- DynamicLoader: kernel32.dll/TlsFree
- DynamicLoader: kernel32.dll/InterlockedIncrement
- DynamicLoader: kernel32.dll/SetLastError
- DynamicLoader: kernel32.dll/GetCurrentThreadId
- DynamicLoader: kernel32.dll/GetLastError
- DynamicLoader: kernel32.dll/InterlockedDecrement
- DynamicLoader: kernel32.dll/QueryPerformanceCounter
- DynamicLoader: kernel32.dll/GetTickCount
- DynamicLoader: kernel32.dll/GetCurrentProcessId
- DynamicLoader: kernel32.dll/GetSystemTimeAsFileTime
- DynamicLoader: kernel32.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: kernel32.dll/TerminateProcess
- DynamicLoader: kernel32.dll/UnhandledExceptionFilter
- DynamicLoader: kernel32.dll/IsDebuggerPresent
- DynamicLoader: kernel32.dll/RtlUnwind
- DynamicLoader: kernel32.dll/GetCPInfo
- DynamicLoader: kernel32.dll/GetACP
- DynamicLoader: kernel32.dll/GetOEMCP
- DynamicLoader: kernel32.dll/IsValidCodePage
- DynamicLoader: kernel32.dll/HeapSize
- DynamicLoader: kernel32.dll/GetLocaleInfoA
- DynamicLoader: kernel32.dll/WideCharToMultiByte
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: PSAPI.DLL/GetModuleInformation
- DynamicLoader: PSAPI.DLL/GetModuleBaseNameW
- DynamicLoader: PSAPI.DLL/EnumProcessModules
- DynamicLoader: SHLWAPI.dll/StrStrIW
- DynamicLoader: SHLWAPI.dll/PathFileExistsW
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: mscoree.dll/_CorExeMain
- DynamicLoader: mscoree.dll/_CorExeMain
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: kernel32.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: kernel32.dll/IsProcessorFeaturePresent
- DynamicLoader: msvcrt.dll/_set_error_mode
- DynamicLoader: msvcrt.dll/?set_terminate@@YAP6AXXZP6AXXZ@Z
- DynamicLoader: msvcrt.dll/_get_terminate
- DynamicLoader: kernel32.dll/FindActCtxSectionStringW
- DynamicLoader: kernel32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: mscoree.dll/GetProcessExecutableHeap
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW

- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/InitializeCriticalSectionEx
- DynamicLoader: kernel32.dll/CreateEventExW
- DynamicLoader: kernel32.dll/CreateSemaphoreExW
- DynamicLoader: kernel32.dll/SetThreadStackGuarantee
- DynamicLoader: kernel32.dll/CreateThreadpoolTimer
- DynamicLoader: kernel32.dll/SetThreadpoolTimer
- DynamicLoader: kernel32.dll/WaitForThreadpoolTimerCallbacks
- DynamicLoader: kernel32.dll/CloseThreadpoolTimer
- DynamicLoader: kernel32.dll/CreateThreadpoolWait
- DynamicLoader: kernel32.dll/SetThreadpoolWait
- DynamicLoader: kernel32.dll/CloseThreadpoolWait
- DynamicLoader: kernel32.dll/FlushProcessWriteBuffers
- DynamicLoader: kernel32.dll/FreeLibraryWhenCallbackReturns
- DynamicLoader: kernel32.dll/GetCurrentProcessorNumber
- DynamicLoader: kernel32.dll/GetLogicalProcessorInformation
- DynamicLoader: kernel32.dll/CreateSymbolicLinkW
- DynamicLoader: kernel32.dll/SetDefaultDllDirectories
- DynamicLoader: kernel32.dll/EnumSystemLocalesEx
- DynamicLoader: kernel32.dll/CompareStringEx
- DynamicLoader: kernel32.dll/GetDateFormatEx
- DynamicLoader: kernel32.dll/GetLocaleInfoEx
- DynamicLoader: kernel32.dll/GetTimeFormatEx
- DynamicLoader: kernel32.dll/GetUserDefaultLocaleName
- DynamicLoader: kernel32.dll/IsValidLocaleName
- DynamicLoader: kernel32.dll/LCMapStringEx
- DynamicLoader: kernel32.dll/GetCurrentPackageId
- DynamicLoader: kernel32.dll/GetTickCount64
- DynamicLoader: kernel32.dll/GetFileInformationByHandleExW
- DynamicLoader: kernel32.dll/SetFileInformationByHandleW
- DynamicLoader: ADVAPI32.dll/EventRegister
- DynamicLoader: ADVAPI32.dll/EventSetInformation
- DynamicLoader: mscoree.dll/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: mscoreei.dll/RegisterShimImplCallback
- DynamicLoader: mscoreei.dll/RegisterShimImplCleanupCallback
- DynamicLoader: mscoreei.dll/SetShellShimInstance
- DynamicLoader: mscoreei.dll/OnShimDllMainCalled
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: KERNELBASE.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: kernel32.dll/ProcessIdToSessionId
- DynamicLoader: IMM32.DLL/ImmCreateContext
- DynamicLoader: IMM32.DLL/ImmDestroyContext
- DynamicLoader: IMM32.DLL/ImmNotifyIME
- DynamicLoader: IMM32.DLL/ImmAssociateContext
- DynamicLoader: IMM32.DLL/ImmReleaseContext
- DynamicLoader: IMM32.DLL/ImmGetContext
- DynamicLoader: IMM32.DLL/ImmGetCompositionStringA
- DynamicLoader: IMM32.DLL/ImmSetCompositionStringA

- DynamicLoader: IMM32.DLL/ImmGetCompositionStringW
- DynamicLoader: IMM32.DLL/ImmSetCompositionStringW
- DynamicLoader: IMM32.DLL/ImmSetCandidateWindow
- DynamicLoader: mscorwks.dll/GetCLRFunction
- DynamicLoader: mscoree.dll/IEE
- DynamicLoader: mscoreei.dll/IEE_RetAddr
- DynamicLoader: mscoreei.dll/IEE
- DynamicLoader: SHLWAPI.dll/UrlIsW
- DynamicLoader: ADVAPI32.dll/RegQueryInfoKeyW
- DynamicLoader: ADVAPI32.dll/RegEnumKeyExW
- DynamicLoader: ADVAPI32.dll/RegEnumValueW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: mscorwks.dll/SetLoadedByMscoree
- DynamicLoader: mscorwks.dll/IEE
- DynamicLoader: mscorwks.dll/GetCLRFunction
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: kernel32.dll/InitializeCriticalSectionAndSpinCount
- DynamicLoader: kernel32.dll/IsProcessorFeaturePresent
- DynamicLoader: kernel32.dll/GetModuleHandleA
- DynamicLoader: kernel32.dll/GetModuleHandleW
- DynamicLoader: kernel32.dll/GetModuleFileNameW
- DynamicLoader: kernel32.dll/GetModuleFileNameA
- DynamicLoader: ntdll.dll/ZwCreateSection
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/GetFileSize
- DynamicLoader: kernel32.dll/MapViewOfFile
- DynamicLoader: kernel32.dll/LoadLibraryExW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: mscoreei.dll/_CorExeMain_RetAddr
- DynamicLoader: mscoreei.dll/_CorExeMain
- DynamicLoader: mscorwks.dll/_CorExeMain
- DynamicLoader: ADVAPI32.dll/RegisterTraceGuidsW
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: ADVAPI32.dll/GetTraceLoggerHandle
- DynamicLoader: ADVAPI32.dll/GetTraceEnableLevel
- DynamicLoader: ADVAPI32.dll/GetTraceEnableFlags
- DynamicLoader: ADVAPI32.dll/TraceEvent
- DynamicLoader: mscoree.dll/IEE
- DynamicLoader: mscoree.dll/GetStartupFlags
- DynamicLoader: mscoreei.dll/GetStartupFlags_RetAddr
- DynamicLoader: mscoreei.dll/GetStartupFlags
- DynamicLoader: mscoree.dll/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile_RetAddr
- DynamicLoader: mscoreei.dll/GetHostConfigurationFile
- DynamicLoader: mscoreei.dll/GetCORVersion_RetAddr
- DynamicLoader: mscoreei.dll/GetCORVersion
- DynamicLoader: mscoree.dll/GetCORSystemDirectory
- DynamicLoader: mscoreei.dll/GetCORSystemDirectory_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: ntdll.dll/RtlUnwind
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: kernel32.dll/GetSystemWindowsDirectoryW
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce

- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/InitializeAcl
- DynamicLoader: ADVAPI32.dll/AddAccessAllowedAce
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: kernel32.dll/SetThreadStackGuarantee
- DynamicLoader: kernel32.dll/FlsSetValue
- DynamicLoader: kernel32.dll/FlsGetValue
- DynamicLoader: kernel32.dll/FlsAlloc
- DynamicLoader: kernel32.dll/FlsFree
- DynamicLoader: kernel32.dll/AddVectoredContinueHandler
- DynamicLoader: kernel32.dll/RemoveVectoredContinueHandler
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidW
- DynamicLoader: SHELL32.dll/SHGetFolderPathW
- DynamicLoader: kernel32.dll/FlushProcessWriteBuffers
- DynamicLoader: kernel32.dll/GetWriteWatch
- DynamicLoader: kernel32.dll/ResetWriteWatch
- DynamicLoader: kernel32.dll/CreateMemoryResourceNotification
- DynamicLoader: kernel32.dll/QueryMemoryResourceNotification
- DynamicLoader: mscoree.dll/_CorExeMain
- DynamicLoader: mscoree.dll/_CorImageUnloading
- DynamicLoader: mscoree.dll/_CorValidateImage
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: kernel32.dll/QueryActCtxW
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: kernel32.dll/GetVersionEx
- DynamicLoader: kernel32.dll/GetVersionExW
- DynamicLoader: kernel32.dll/GetVersionEx
- DynamicLoader: kernel32.dll/GetVersionExW
- DynamicLoader: kernel32.dll/GetFullPathName
- DynamicLoader: kernel32.dll/GetFullPathNameW
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextA
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptGetHashParam
- DynamicLoader: ADVAPI32.dll/CryptImportKey
- DynamicLoader: ADVAPI32.dll/CryptExportKey
- DynamicLoader: ADVAPI32.dll/CryptGenKey
- DynamicLoader: ADVAPI32.dll/CryptGetKeyParam
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptVerifySignatureA
- DynamicLoader: ADVAPI32.dll/CryptSignHashA
- DynamicLoader: ADVAPI32.dll/CryptGetProvParam
- DynamicLoader: ADVAPI32.dll/CryptGetUserKey
- DynamicLoader: ADVAPI32.dll/CryptEnumProvidersA
- DynamicLoader: mscoree.dll/GetMetaDataInternalInterface
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface_RetAddr
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorwks.dll/GetMetaDataInternalInterface
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureA
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey

- DynamicLoader: mscorjit.dll/getJit
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: kernel32.dll/GetUserDefaultUILanguage
- DynamicLoader: USER32.dll/RegisterWindowMessage
- DynamicLoader: USER32.dll/RegisterWindowMessageW
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/AdjustWindowRectEx
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: kernel32.dll/GetCurrentThread
- DynamicLoader: kernel32.dll/DuplicateHandle
- DynamicLoader: kernel32.dll/GetCurrentThreadId
- DynamicLoader: kernel32.dll/lstrlen
- DynamicLoader: kernel32.dll/lstrlenW
- DynamicLoader: kernel32.dll/GetModuleHandle
- DynamicLoader: kernel32.dll/GetModuleHandleW
- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: GDI32.dll/GetStockObject
- DynamicLoader: USER32.dll/RegisterClass
- DynamicLoader: USER32.dll/RegisterClassW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: USER32.dll/CreateWindowEx
- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/GetWindowLong
- DynamicLoader: USER32.dll/GetWindowLongW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: USER32.dll/SetWindowLong
- DynamicLoader: USER32.dll/SetWindowLongW
- DynamicLoader: USER32.dll/CallWindowProc
- DynamicLoader: USER32.dll/CallWindowProcW
- DynamicLoader: USER32.dll/GetClientRect
- DynamicLoader: USER32.dll/GetWindowRect
- DynamicLoader: USER32.dll/GetParent
- DynamicLoader: uxtheme.dll/IsAppThemed
- DynamicLoader: uxtheme.dll/IsAppThemedW
- DynamicLoader: kernel32.dll/CreateActCtx
- DynamicLoader: kernel32.dll/CreateActCtxA
- DynamicLoader: kernel32.dll/GetCurrentActCtx
- DynamicLoader: kernel32.dll/ActivateActCtx
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: USER32.dll/GetWindowTextLength
- DynamicLoader: USER32.dll/GetWindowTextLengthW
- DynamicLoader: USER32.dll/GetWindowText
- DynamicLoader: USER32.dll/GetWindowTextW
- DynamicLoader: USER32.dll/GetProcessWindowStation
- DynamicLoader: USER32.dll/GetUserObjectInformation
- DynamicLoader: USER32.dll/GetUserObjectInformationA
- DynamicLoader: kernel32.dll/SetConsoleCtrlHandler
- DynamicLoader: kernel32.dll/SetConsoleCtrlHandlerW
- DynamicLoader: kernel32.dll/GetModuleHandle
- DynamicLoader: kernel32.dll/GetModuleHandleW
- DynamicLoader: USER32.dll/GetClassInfo
- DynamicLoader: USER32.dll/GetClassInfoW
- DynamicLoader: USER32.dll/RegisterClass
- DynamicLoader: USER32.dll/RegisterClassW
- DynamicLoader: USER32.dll/CreateWindowEx

- DynamicLoader: USER32.dll/CreateWindowExW
- DynamicLoader: USER32.dll/DefWindowProc
- DynamicLoader: USER32.dll/DefWindowProcW
- DynamicLoader: kernel32.dll/GetStartupInfo
- DynamicLoader: kernel32.dll/GetStartupInfoW
- DynamicLoader: USER32.dll/GetWindowPlacement
- DynamicLoader: USER32.dll/GetSystemMetrics
- DynamicLoader: USER32.dll/GetDC
- DynamicLoader: GDI32.dll/GetDeviceCaps
- DynamicLoader: USER32.dll/ReleaseDC
- DynamicLoader: USER32.dll/CreateIconFromResourceEx
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/GetSystemMenu
- DynamicLoader: USER32.dll/EnableMenuItem
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/SetWindowPos
- DynamicLoader: USER32.dll/RedrawWindow
- DynamicLoader: USER32.dll/ShowWindow
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageW
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: USER32.dll/PostMessage
- DynamicLoader: USER32.dll/PostMessageW
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: ole32.dll/CoRegisterMessageFilter
- DynamicLoader: USER32.dll/PeekMessage
- DynamicLoader: USER32.dll/PeekMessageW
- DynamicLoader: USER32.dll/IsWindowUnicode
- DynamicLoader: USER32.dll/GetMessageW
- DynamicLoader: USER32.dll/TranslateMessage
- DynamicLoader: USER32.dll/DispatchMessageW
- DynamicLoader: USER32.dll/GetFocus
- DynamicLoader: kernel32.dll/GetModuleFileName
- DynamicLoader: kernel32.dll/GetModuleFileNameW
- DynamicLoader: kernel32.dll/SetCurrentDirectory
- DynamicLoader: kernel32.dll/SetCurrentDirectoryW
- DynamicLoader: kernel32.dll/FindResourceEx
- DynamicLoader: kernel32.dll/FindResourceExA
- DynamicLoader: kernel32.dll/LoadResource
- DynamicLoader: kernel32.dll/SizeofResource
- DynamicLoader: kernel32.dll/LockResource
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptGetProvParam
- DynamicLoader: CRYPTSP.dll/CryptSetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptDecrypt
- DynamicLoader: CRYPTSP.dll/CryptEncrypt
- DynamicLoader: kernel32.dll/ReleaseMutex
- DynamicLoader: kernel32.dll/CreateMutex
- DynamicLoader: kernel32.dll/CreateMutexW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: ADVAPI32.dll/RegOpenKeyEx
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExA
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExA
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: shfolder.dll/SHGetFolderPath

- DynamicLoader: shfolder.dll/SHGetFolderPathW
- DynamicLoader: kernel32.dll/SetErrorMode
- DynamicLoader: kernel32.dll/GetFileAttributesEx
- DynamicLoader: kernel32.dll/GetFileAttributesExW
- DynamicLoader: kernel32.dll/CreateDirectory
- DynamicLoader: kernel32.dll/CreateDirectoryW
- DynamicLoader: kernel32.dll/CreateFile
- DynamicLoader: kernel32.dll/CreateFileW
- DynamicLoader: kernel32.dll/GetFileType
- DynamicLoader: kernel32.dll/WriteFile
- DynamicLoader: kernel32.dll/DeleteFile
- DynamicLoader: kernel32.dll/DeleteFileW
- DynamicLoader: kernel32.dll/CopyFile
- DynamicLoader: kernel32.dll/CopyFileW
- DynamicLoader: ADVAPI32.dll/RegSetValueEx
- DynamicLoader: ADVAPI32.dll/RegSetValueExW
- DynamicLoader: mscoreei.dll/LoadLibraryShim_RetAddr
- DynamicLoader: mscoreei.dll/LoadLibraryShim
- DynamicLoader: Culture.dll/ConvertLangIdToCultureName
- DynamicLoader: mscoree.dll/DllGetClassObject
- DynamicLoader: mscoreei.dll/DllGetClassObject_RetAddr
- DynamicLoader: mscoreei.dll/DllGetClassObject
- DynamicLoader: diasymreader.dll/DllGetClassObjectInternal
- DynamicLoader: mscoree.dll/DllGetClassObject
- DynamicLoader: kernel32.dll/DeleteFile
- DynamicLoader: kernel32.dll/DeleteFileA
- DynamicLoader: kernel32.dll/GetSystemInfo
- DynamicLoader: kernel32.dll/CreateIoCompletionPort
- DynamicLoader: kernel32.dll/PostQueuedCompletionStatus
- DynamicLoader: ntdll.dll/NtQueryInformationThread
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtGetCurrentProcessorNumber
- DynamicLoader: ADVAPI32.dll/GetUserName
- DynamicLoader: ADVAPI32.dll/GetUserNameW
- DynamicLoader: USER32.dll/GetForegroundWindow
- DynamicLoader: USER32.dll/GetWindowThreadProcessId
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValue
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueW
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivilegesW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: PSAPI.DLL/EnumProcesses
- DynamicLoader: PSAPI.DLL/EnumProcessesW
- DynamicLoader: ntdll.dll/NtQuerySystemInformation
- DynamicLoader: ntdll.dll/NtQuerySystemInformationW
- DynamicLoader: USER32.dll/GetKeyboardLayout
- DynamicLoader: USER32.dll/GetWindowText
- DynamicLoader: USER32.dll/GetWindowTextW
- DynamicLoader: kernel32.dll/GlobalMemoryStatusEx
- DynamicLoader: USER32.dll/RegisterRawInputDevices
- DynamicLoader: USER32.dll/SetClipboardViewer
- DynamicLoader: USER32.dll/SendMessage
- DynamicLoader: USER32.dll/SendMessageA
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: ws2_32.dll/WSAStartup
- DynamicLoader: ADVAPI32.dll/RegQueryValueEx
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: ws2_32.dll/WSASocket
- DynamicLoader: ws2_32.dll/WSASocketW
- DynamicLoader: ws2_32.dll/setsockopt

- DynamicLoader: ws2_32.dll/WSAEventSelect
- DynamicLoader: ws2_32.dll/ioctlsocket
- DynamicLoader: ws2_32.dll/closesocket
- DynamicLoader: kernel32.dll/GetCurrentProcess
- DynamicLoader: kernel32.dll/GetCurrentProcessW
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/OpenProcessTokenW
- DynamicLoader: kernel32.dll/GetFileAttributesEx
- DynamicLoader: kernel32.dll/GetFileAttributesExW
- DynamicLoader: kernel32.dll/GetFileSize
- DynamicLoader: kernel32.dll/ReadFile
- DynamicLoader: mscoree.dll/ND_RI2
- DynamicLoader: mscoreei.dll/ND_RI2_RetAddr
- DynamicLoader: mscoreei.dll/ND_RI2
- DynamicLoader: kernel32.dll/GetCurrentProcessId
- DynamicLoader: kernel32.dll/GetCurrentProcessIdW
- DynamicLoader: kernel32.dll/GetComputerName
- DynamicLoader: kernel32.dll/GetComputerNameW
- DynamicLoader: ADVAPI32.dll/ConvertStringSecurityDescriptorToSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/ConvertStringSecurityDescriptorToSecurityDescriptorW
- DynamicLoader: kernel32.dll/LocalFree
- DynamicLoader: kernel32.dll/CreateFileMapping
- DynamicLoader: kernel32.dll/CreateFileMappingW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/MapViewOfFile
- DynamicLoader: kernel32.dll/UnmapViewOfFile
- DynamicLoader: kernel32.dll/VirtualQuery
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSid
- DynamicLoader: ADVAPI32.dll/CreateWellKnownSidW
- DynamicLoader: kernel32.dll/WaitForSingleObject
- DynamicLoader: kernel32.dll/OpenMutex
- DynamicLoader: kernel32.dll/OpenMutexW
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/OpenProcess
- DynamicLoader: kernel32.dll/OpenProcessW
- DynamicLoader: kernel32.dll/GetProcessTimes
- DynamicLoader: kernel32.dll/GetProcessTimesW
- DynamicLoader: ws2_32.dll/inet_addr
- DynamicLoader: USER32.dll/WaitMessage
- DynamicLoader: dnsapi.dll/DnsQuery_A
- DynamicLoader: ws2_32.dll/getaddrinfo
- DynamicLoader: ws2_32.dll/freeaddrinfo
- DynamicLoader: ws2_32.dll/setsockopt
- DynamicLoader: ws2_32.dll/bind
- DynamicLoader: ws2_32.dll/WSAIoctl
- DynamicLoader: ws2_32.dll/WSAGetOverlappedResult
- DynamicLoader: kernel32.dll/FormatMessage
- DynamicLoader: kernel32.dll/FormatMessageW
- DynamicLoader: kernel32.dll/SwitchToThread
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: kernel32.dll/SetThreadExecutionState

A process attempted to delay the analysis task.

- Process: now.exe tried to sleep 466 seconds, actually delayed analysis time by 0 seconds

Guard pages use detected - possible anti-debugging.

Creates RWX memory

Attempts to connect to a dead IP:Port (1 unique times)

- IP: 192.168.56.1:2556

SetUnhandledExceptionFilter detected (possible anti-debug)

2 Host(s) detected

IP Address	Hostname	Reverse DNS
8.8.8.8		google-public-dns-a.google.com.
8.8.4.4		google-public-dns-b.google.com.

1 Countr(y|ies) detected

Hosts	Country
2	United States