

## Gwardrfd.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

**MalFamily: Lokibot**


**MalScore: 100**

<b>File type:</b>	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
<b>File size:</b>	256.50 KB (262656 bytes)
<b>Compile time:</b>	2019-08-09 10:13:16
<b>MD5:</b>	7fbd2b160120ce8f05103836afd8fd78
<b>SHA1:</b>	3495af2d60e4cca2cdc5627fbb57a56b53c11b99
<b>Import hash:</b>	f34d5f2d4577ed6d9ceec516c1f5a744
<b>Submitted:</b>	2019-09-26 13:30:07

### URL(s) file hosting

<http://www.altoimpactoperu.com/dinopl/Gwardrfd.exe>

### Antivirus Report

Report date	Detection Ratio	Permalink
2019-09-26 09:17:45	19/69	

### Import library

mscoree.dll

**16**

## Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN LokiBot User-Agent (Charon/Inferno)

- signature: ET TROJAN LokiBot Checkin
- signature: ET TROJAN LokiBot Request for C2 Commands Detected M2
- signature: ET TROJAN LokiBot Request for C2 Commands Detected M1
- signature: ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1
- signature: ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2

Collects information to fingerprint the system

Harvests information related to installed mail clients

- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c00000000000046\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7d19c9e894f20d4780a31c9a9f17da11
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd4111
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{f86ed2903a4a11cfb57e524153480001}\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\32a3dc9c400a4b448b60ab7fe553a392\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\32a3dc9c400a4b448b60ab7fe553a392
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c00000000000046
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Email
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7760e21103136b47946c9c80fa097f15
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows



Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\0a0d020000000000c00000000000046\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\0a0d020000000000c00000000000046  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\7d19c9e894f20d4780a31c9a9f17da11\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\7760e21103136b47946c9c80fa097f15\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar  
Summary\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd4111\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows  
Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook  
- key: HKEY\_CURRENT\_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook

Harvests information related to installed instant messenger clients

- file: C:\Users\Seven01\AppData\Roaming\purple\accounts.xml

Harvests credentials from local FTP client softwares

- file: C:\Users\Seven01\AppData\Roaming\FileZilla\sitemanager.xml  
- file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentsservers.xml  
- file: C:\Users\Seven01\AppData\Roaming\Far  
Manager\Profile\PluginsData\42E4AEB1-A230-44F4-B33C-F195BB654931.db  
- file: C:\Program Files (x86)\FTPGetter\Profile\servers.xml  
- file: C:\Users\Seven01\AppData\Roaming\FTPGetter\servers.xml  
- file: C:\Users\Seven01\AppData\Roaming\Estsoft\ALFTP\ESTdb2.dat  
- key: HKEY\_CURRENT\_USER\Software\Far\Plugins\FTP\Hosts  
- key: HKEY\_CURRENT\_USER\Software\Far2\Plugins\FTP\Hosts  
- key: HKEY\_CURRENT\_USER\Software\Ghisler\Total Commander  
- key: HKEY\_CURRENT\_USER\Software\LinasFTP\Site Manager

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\E62877\73E4A9.exe  
- file: C:\Users\Seven01\AppData\Roaming\E62877

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

- Spam: services.exe (480) called API GetSystemTimeAsFileTime 3663048 times

## Anomalous .NET characteristics

- anomalous\_version: Assembly version is set to 0

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.94, characteristics:  
IMAGE\_SCN\_CNT\_CODE|IMAGE\_SCN\_MEM\_EXECUTE|IMAGE\_SCN\_MEM\_READ, raw\_size:  
0x0003f800, virtual\_size: 0x0003f674

Performs some HTTP requests

- url: http://himmgihsddbif.myftp.biz/BILLIHF/Panel/five/fre.php

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

- post\_no\_referer: HTTP traffic contains a POST request with no referer header  
- http\_version\_old: HTTP traffic uses version 1.0  
- suspicious\_request: http://himmgihsddbif.myftp.biz/BILLIHF/Panel/five/fre.php

Dynamic (imported) function loading detected

- 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/\_CorExeMain\_RetAddr
- DynamicLoader: mscoreei.dll/\_CorExeMain
- DynamicLoader: SHLWAPI.dll/UrllsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsSetValue
- 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/EventSetInformation
- DynamicLoader: clr.dll/SetRuntimeInfo
- DynamicLoader: clr.dll/\_CorExeMain
- DynamicLoader: MSCOREE.DLL/CreateConfigStream
- DynamicLoader: mscoreei.dll/CreateConfigStream\_RetAddr
- DynamicLoader: mscoreei.dll/CreateConfigStream
- DynamicLoader: KERNEL32.dll/GetNumaHighestNodeNumber
- DynamicLoader: KERNEL32.dll/FIsSetValue
- DynamicLoader: KERNEL32.dll/FIsGetValue
- DynamicLoader: KERNEL32.dll/FIsAlloc
- DynamicLoader: KERNEL32.dll/FIsFree
- 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/AddSIDToBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/CreateBoundaryDescriptorW
- DynamicLoader: KERNEL32.dll/CreatePrivateNamespaceW
- DynamicLoader: KERNEL32.dll/OpenPrivateNamespaceW
- 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/DeleteBoundaryDescriptor
- DynamicLoader: KERNEL32.dll/WerRegisterRuntimeExceptionModule
- DynamicLoader: KERNEL32.dll/RaiseException
- DynamicLoader: MSCOREE.DLL/
- DynamicLoader: mscoreei.dll/
- DynamicLoader: KERNELBASE.dll/SetSystemFileCacheSize
- DynamicLoader: ntdll.dll/NtSetSystemInformation
- DynamicLoader: KERNELBASE.dll/PrivIsDllSynchronizationHeld
- DynamicLoader: KERNEL32.dll/AddDllDirectory
- DynamicLoader: KERNEL32.dll/SortGetHandle
- DynamicLoader: KERNEL32.dll/SortCloseHandle
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: clrjit.dll/sxsJitStartup
- DynamicLoader: clrjit.dll/getJit
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetNativeSystemInfo
- DynamicLoader: KERNEL32.dll/GetLocaleInfoEx
- DynamicLoader: KERNEL32.dll/LocaleNameToLCID
- DynamicLoader: gdiplus.dll/GdiplusStartup
- DynamicLoader: KERNEL32.dll/IsProcessorFeaturePresent
- DynamicLoader: USER32.dll/GetWindowInfo
- DynamicLoader: USER32.dll/GetAncestor
- DynamicLoader: USER32.dll/GetMonitorInfoA
- DynamicLoader: USER32.dll/EnumDisplayMonitors
- DynamicLoader: USER32.dll/EnumDisplayDevicesA
- DynamicLoader: GDI32.dll/ExtTextOutW
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: gdiplus.dll/GdiLoadImageFromStream
- DynamicLoader: MSCOREE.DLL/GetProcessExecutableHeap
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap\_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: WindowsCodecs.dll/DllGetClassObject
- DynamicLoader: KERNEL32.dll/WerRegisterMemoryBlock
- DynamicLoader: gdiplus.dll/GdiImageForceValidation
- DynamicLoader: gdiplus.dll/GdiGetImageType
- DynamicLoader: gdiplus.dll/GdiGetImageRawFormat
- DynamicLoader: gdiplus.dll/GdiGetImageWidth
- DynamicLoader: gdiplus.dll/GdiGetImageHeight
- DynamicLoader: gdiplus.dll/GdiBitmapGetPixel



- DynamicLoader: KERNEL32.dll/LCIDToLocaleName
- DynamicLoader: KERNEL32.dll/GetUserDefaultLocaleName
- DynamicLoader: KERNEL32.dll/GetUserPreferredUILanguages
- DynamicLoader: shell32.dll/SHGetFolderPath
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: KERNEL32.dll/GetFullPathName
- DynamicLoader: KERNEL32.dll/GetFullPathNameW
- DynamicLoader: KERNEL32.dll/SetThreadErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: KERNEL32.dll/VirtualAlloc
- DynamicLoader: KERNEL32.dll/LocalAlloc
- DynamicLoader: KERNEL32.dll/WideCharToMultiByte
- DynamicLoader: ADVAPI32.dll/CryptAcquireContextW
- DynamicLoader: ADVAPI32.dll/CryptCreateHash
- DynamicLoader: ADVAPI32.dll/CryptDecrypt
- DynamicLoader: ADVAPI32.dll/CryptDeriveKey
- DynamicLoader: ADVAPI32.dll/CryptDestroyHash
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptHashData
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: USER32.dll/MessageBoxA
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: apphelp.dll/ApphelpCheckRunAppEx
- DynamicLoader: apphelp.dll/ApphelpQueryModuleDataEx
- DynamicLoader: apphelp.dll/ApphelpParseModuleData
- DynamicLoader: apphelp.dll/ApphelpCreateAppcompatData
- DynamicLoader: apphelp.dll/SdbInitDatabaseEx
- DynamicLoader: apphelp.dll/SdbReleaseDatabase
- DynamicLoader: apphelp.dll/SdbUnpackAppCompatData
- DynamicLoader: apphelp.dll/SdbQueryContext
- DynamicLoader: ole32.dll/CoGetContextToken
- DynamicLoader: gdiplus.dll/GdiplusDisposeImage
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: KERNEL32.dll/CreateActCtxW
- DynamicLoader: KERNEL32.dll/AddRefActCtx
- DynamicLoader: KERNEL32.dll/ReleaseActCtx
- DynamicLoader: KERNEL32.dll/ActivateActCtx
- DynamicLoader: KERNEL32.dll/DeactivateActCtx
- DynamicLoader: KERNEL32.dll/GetCurrentActCtx
- DynamicLoader: KERNEL32.dll/QueryActCtxW
- DynamicLoader: ADVAPI32.dll/EventUnregister
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: vaultcli.dll/VaultEnumerateItems
- DynamicLoader: vaultcli.dll/VaultEnumerateVaults
- DynamicLoader: vaultcli.dll/VaultFree
- DynamicLoader: vaultcli.dll/VaultGetItem
- DynamicLoader: vaultcli.dll/VaultOpenVault
- DynamicLoader: vaultcli.dll/VaultCloseVault
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: NETAPI32.DLL/NetUserGetInfo
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptSetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptDecrypt

- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: NETAPI32.DLL/NetUserGetInfo
- DynamicLoader: NETAPI32.DLL/NetUserGetInfo
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: ole32.dll/CoInitializeSecurity
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: fntcache.dll/ServiceMain
- DynamicLoader: fntcache.dll/SvchostPushServiceGlobals
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: wkscli.dll/NetGetJoinInformation
- DynamicLoader: netutils.dll/NetApiBufferFree
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: RPCRT4.dll/UuidFromStringW
- DynamicLoader: radarrs.dll/WdiDiagnosticModuleMain
- DynamicLoader: radarrs.dll/WdiHandleInstance
- DynamicLoader: radarrs.dll/WdiGetDiagnosticModuleInterfaceVersion

A process attempted to delay the analysis task.

- Process: vbc.exe tried to sleep 720 seconds, actually delayed analysis time by 0 seconds

Guard pages use detected - possible anti-debugging.

Creates RWX memory

SetUnhandledExceptionFilter detected (possible anti-debug)

**2**

## HTTP Request(s) detected

<http://himmgihsddbif.myftp.biz/BILLIHF/Panel/five/fre.php>

Hostname: himmgihsddbif.myftp.biz

IP Address: 154.118.124.205

Port: 80

Count: 2

<http://himmgihsddbif.myftp.biz/BILLIHF/Panel/five/fre.php>

Hostname: himmgihsddbif.myftp.biz

IP Address: 154.118.124.205

Port: 80

Count: 12