cfgb.scr

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

MalFamily: Powershell **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	425.00 KB (435200 bytes)
Compile time:	2018-09-16 16:32:21
MD5:	10d9300bbb67ca1f82c5f2b027e83f37
SHA1:	9db3d09c63e5c1cb4528b8935a2b7cdaed7de038
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-10-30 22:27:07

URL(s) file hosting

http://ysxdfrtzg.000webhostapp.com/cfgb.scr

Antivirus Report

Report date	Detection Ratio	Permalink
2018-10-30 09:58:39	33/66	

Import library

mscoree.dll

5 Behaviors detected by system signatures

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

- Spam: services.exe (480) called API GetSystemTimeAsFileTime 2551729 times

Harvests information related to installed mail clients

- key: HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook\Capabilities\Hidden
- key: HKEY_LOCAL_MACHINE\Software\Clients\Mail\Microsoft Outlook\Capabilities
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook\Capabilities\FileAssociations

Guard pages use detected - possible anti-debugging.

Dynamic (imported) function loading detected

- DynamicLoader: SHELL32.dll/ShellExecuteExW
- DynamicLoader: ole32.dll/OleInitialize
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: PROPSYS.dll/PSCreateMemoryPropertyStore
- DynamicLoader: PROPSYS.dll/PSPropertyBag_WriteDWORD
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: PROPSYS.dll/PSPropertyBag_ReadDWORD
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: PROPSYS.dll/PSPropertyBag_ReadBSTR
- DynamicLoader: PROPSYS.dll/PSPropertyBag_ReadStrAlloc
- DynamicLoader: SHELL32.dll/
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor
- DynamicLoader: ADVAPI32.dll/SetEntriesInAclW
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: ADVAPI32.dll/IsTextUnicode
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: profapi.dll/
- DynamicLoader: PROPSYS.dll/
- DynamicLoader: ole32.dll/PropVariantClear
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: apphelp.dll/ApphelpCheckShellObject
- DynamicLoader: PROPSYS.dll/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW

- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ole32.dll/CoTaskMemRealloc
- DynamicLoader: ole32.dll/CoAllowSetForegroundWindow
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ADVAPI32.dll/InstallApplication
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: kernel32.dll/InitializeSRWLock
- DynamicLoader: kernel32.dll/AcquireSRWLockExclusive
- DynamicLoader: kernel32.dll/AcquireSRWLockShared
- DynamicLoader: kernel32.dll/ReleaseSRWLockExclusive
- DynamicLoader: kernel32.dll/ReleaseSRWLockShared
- DynamicLoader: SHELL32.dll/SHGetFolderPathW
- DynamicLoader: ADVAPI32.dll/SaferGetPolicyInformation
- DynamicLoader: sfc.dll/SfcIsFileProtected
- DynamicLoader: ntdll.dll/RtlDllShutdownInProgress
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/OleUninitialize
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: KERNELBASE.dll/SetThreadStackGuarantee
- DynamicLoader: KERNELBASE.dll/SetThreadStackGuarantee
- DynamicLoader: KERNELBASE.dll/SetThreadStackGuarantee
- 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: 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: appmgmts.dll/ServiceMain
- DynamicLoader: appmgmts.dll/SvchostPushServiceGlobals
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: SHELL32.dll/OpenAs_RunDLLW
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: dwmapi.dll/DwmIsCompositionEnabled
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: comctl32.dll/InitCommonControlsEx
- DynamicLoader: uxtheme.dll/EnableThemeDialogTexture
- DynamicLoader: comctl32.dll/RegisterClassNameW
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: uxtheme.dll/OpenThemeData
- DynamicLoader: uxtheme.dll/GetThemeBool
- DynamicLoader: uxtheme.dll/IsThemePartDefined

- DynamicLoader: comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/GetThemePartSize
- DynamicLoader: uxtheme.dll/GetThemeFont
- DynamicLoader: uxtheme.dll/GetThemeColor
- DynamicLoader: IMM32.DLL/ImmIsIME
- DynamicLoader: uxtheme.dll/CloseThemeData
- DynamicLoader: uxtheme.dll/GetThemeTextExtent
- 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: comctl32.dll/RegisterClassNameW
- DynamicLoader: uxtheme.dll/GetThemeMargins
- DynamicLoader: GDI32.dll/GetTextExtentExPointWPri
- DynamicLoader: ole32.dll/CreateBindCtx
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetApartmentType
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoGetMalloc
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/StringFromGUID2
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: ADVAPI32.dll/OpenThreadToken
- DynamicLoader: SHELL32.dll/
- DynamicLoader: PROPSYS.dll/
- DynamicLoader: ADVAPI32.dll/RegOpenKeyExW
- DynamicLoader: ADVAPI32.dll/RegGetValueW
- DynamicLoader: ADVAPI32.dll/RegCloseKey
- DynamicLoader: ole32.dll/CoTaskMemRealloc
- DynamicLoader: comctl32.dll/ImageList_CoCreateInstance
- DynamicLoader: WindowsCodecs.dll/WICCreateImagingFactory_Proxy
- DynamicLoader: ADVAPI32.dll/RegQueryValueW
- DynamicLoader: apphelp.dll/ApphelpCheckShellObject
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: uxtheme.dll/SetWindowTheme
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: ADVAPI32.dll/RegEnumKeyW
- DynamicLoader: comctl32.dll/
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: ADVAPI32.dll/InitializeSecurityDescriptor

- DynamicLoader: ADVAPI32.dll/SetEntriesInAclW
- DynamicLoader: ntmarta.dll/GetMartaExtensionInterface
- DynamicLoader: ADVAPI32.dll/SetSecurityDescriptorDacl
- DynamicLoader: ADVAPI32.dll/IsTextUnicode
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_Size_ExW
- DynamicLoader: comctl32.dll/
- DynamicLoader: SETUPAPI.dll/CM_Get_Device_Interface_List_ExW
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: profapi.dll/
- DynamicLoader: PROPSYS.dll/PSLookupPropertyHandlerCLSID
- DynamicLoader: ADVAPI32.dll/RegQueryValueExW
- DynamicLoader: PROPSYS.dll/PSCreateDelayedMultiplexPropertyStore
- DynamicLoader: PROPSYS.dll/PSCreatePropertyStoreFromObject
- DynamicLoader: SHELL32.dll/
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeExW
- DynamicLoader: VERSION.dll/GetFileVersionInfoExW
- DynamicLoader: PROPSYS.dll/
- DynamicLoader: VERSION.dll/VerQueryValueW
- DynamicLoader: PROPSYS.dll/PSCoerceToCanonicalValue
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: PROPSYS.dll/PropVariantToVariant
- DynamicLoader: ole32.dll/PropVariantClear
- DynamicLoader: PROPSYS.dll/VariantToString
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: comctl32.dll/
- DynamicLoader: GDI32.dll/GdiIsMetaPrintDC
- DynamicLoader: ole32.dll/CoInitializeEx
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: ole32.dll/CoRegisterInitializeSpy
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: uxtheme.dll/GetThemeInt
- DynamicLoader: uxtheme.dll/DrawThemeBackground
- DynamicLoader: uxtheme.dll/BufferedPaintInit
- DynamicLoader: uxtheme.dll/BufferedPaintRenderAnimation
- DynamicLoader: uxtheme.dll/BeginBufferedAnimation
- DynamicLoader: uxtheme.dll/IsThemeBackgroundPartiallyTransparent
- DynamicLoader: uxtheme.dll/DrawThemeParentBackground
- DynamicLoader: uxtheme.dll/GetThemeBackgroundContentRect
- DynamicLoader: uxtheme.dll/DrawThemeText
- DynamicLoader: uxtheme.dll/EndBufferedAnimation
- DynamicLoader: uxtheme.dll/GetThemeTransitionDuration
- DynamicLoader: OLEAUT32.dll/SysAllocString
- DynamicLoader: OLEAUT32.dll/SysStringLen
- DynamicLoader: OLEAUT32.dll/SysFreeString
- 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

SetUnhandledExceptionFilter detected (possible anti-debug)