eyu.exe

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

MalFamily: Lokibot **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	504.00 KB (516096 bytes)
Compile time:	2018-10-28 13:46:20
MD5:	32ffae9524a6321051248e4313c91852
SHA1:	5e28c29f740842a5eee6f2717d25f86dd3b0f752
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2019-03-01 15:03:04

URL(s) file hosting

http://sileoturkiye.com/wp-admin/inv/eyu.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2019-02-25 01:07:27	48/67	

Import library

mscoree.dll

24 Behaviors detected by system signatures

Domain Sinkholed or blacklisted

- Alert: Honeypot blocked domain: dresson1.com

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

- Injection: eyu.exe(2604) -> RegAsm.exe(2112)

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

- Spam: services.exe (476) called API GetSystemTimeAsFileTime 2471454 times

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Avast
- data: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{S1YW3N6D-63QW-Q0JP-6OXC-I031YLN58GL4}\StubPath
- data: "C:\Users\Seven01\AppData\Roaming\Install\Host.exe"
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{S1YW3N6D-63QW-Q0JP-6OXC-I031YLN58GL4}
- data: unknown

Creates a hidden or system file

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

Attempts to identify installed AV products by registry key

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Avast

Harvests credentials from local FTP client softwares

- file: C:\Users\Seven01\AppData\Roaming\FileZilla\sitemanager.xml
- file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentservers.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

Harvests information related to installed instant messenger clients

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

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\8503020000000000c000000000000046\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\8503020000000000c000000000000046
- 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\0a0d020000000000c000000000000046\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\0a0d020000000000c000000000000046
- 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

Collects information to fingerprint the system

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

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.68, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00025000, virtual_size: 0x000248bc

Performs some HTTP requests

- url: http://dresson1.com/wip-admin/js/Panel/five/fre.php

Creates RWX memory

Anomalous file deletion behavior detected (10+)

- DeletedFile: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2604.26534453
- DeletedFile: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2604.26534453
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2604.26534515
- DeletedFile: C:\Users\Seven01\AppData\Roaming\E62877\73E4A9.lck
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- DeletedFile: C:\Users\Seven01\AppData\Roaming\Install\Host.exe

Guard pages use detected - possible anti-debugging.

A process attempted to delay the analysis task.

- Process: build.exe tried to sleep 720 seconds, actually delayed analysis time by 0 seconds
- Process: Host.exe tried to sleep 1050 seconds, actually delayed analysis time by 0 seconds

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/UrlIsW
- DynamicLoader: VERSION.dll/GetFileVersionInfoSizeW
- DynamicLoader: VERSION.dll/GetFileVersionInfoW
- DynamicLoader: VERSION.dll/VerQueryValueW
- 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: mscoreei.dll/GetProcessExecutableHeap_RetAddr
- DynamicLoader: mscoreei.dll/GetProcessExecutableHeap
- DynamicLoader: mscorwks.dll/SetLoadedByMscoree
- DynamicLoader: mscorwks.dll/_CorExeMain
- DynamicLoader: mscorwks.dll/GetCLRFunction
- 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: mscoreei.dll/IEE_RetAddr
- DynamicLoader: mscoreei.dll/IEE
- DynamicLoader: mscorwks.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: 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: CRYPTSP.dll/CryptAcquireContextA
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptExportKey
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptHashData
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: CRYPTSP.dll/CryptDestroyKey
- DynamicLoader: mscorjit.dll/getJit
- DynamicLoader: KERNEL32.dll/IsWow64Process
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationEx
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationExW
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface_RetAddr
- DynamicLoader: mscoreei.dll/GetMetaDataInternalInterface
- DynamicLoader: mscorwks.dll/GetMetaDataInternalInterface
- DynamicLoader: CRYPTSP.dll/CryptVerifySignatureA
- DynamicLoader: KERNEL32.dll/GetUserDefaultUILanguage
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariable
- DynamicLoader: KERNEL32.dll/GetEnvironmentVariableW
- DynamicLoader: KERNEL32.dll/SetErrorMode
- DynamicLoader: KERNEL32.dll/GetFileAttributesEx
- DynamicLoader: KERNEL32.dll/GetFileAttributesExW
- DynamicLoader: mscoreei.dll/LoadLibraryShim_RetAddr
- DynamicLoader: mscoreei.dll/LoadLibraryShim
- DynamicLoader: culture.dll/ConvertLangIdToCultureName
- DynamicLoader: KERNEL32.dll/lstrlen
- DynamicLoader: KERNEL32.dll/lstrlenW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGetProvParam
- DynamicLoader: CRYPTSP.dll/CryptSetKeyParam
- DynamicLoader: CRYPTSP.dll/CryptDecrypt
- DynamicLoader: CRYPTSP.dll/CryptEncrypt
- DynamicLoader: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: KERNEL32.dll/GetACP
- DynamicLoader: KERNEL32.dll/UnmapViewOfFile
- DynamicLoader: KERNEL32.dll/CloseHandle
- DynamicLoader: bcrypt.dll/BCryptGetFipsAlgorithmMode
- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationEx

- DynamicLoader: mscorwks.dll/StrongNameSignatureVerificationExW
- DynamicLoader: MSCOREE.DLL/GetMetaDataInternalInterface
- DynamicLoader: mscoreei.dll/_CorDllMain_RetAddr
- DynamicLoader: mscoreei.dll/_CorDllMain
- DynamicLoader: MSCOREE.DLL/GetTokenForVTableEntry
- DynamicLoader: MSCOREE.DLL/SetTargetForVTableEntry
- DynamicLoader: MSCOREE.DLL/GetTargetForVTableEntry
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry_RetAddr
- DynamicLoader: mscoreei.dll/GetTokenForVTableEntry
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry_RetAddr
- DynamicLoader: mscoreei.dll/SetTargetForVTableEntry
- DynamicLoader: mscoreei.dll/GetTargetForVTableEntry_RetAddr
- DynamicLoader: mscoreei.dll/GetTargetForVTableEntry
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: KERNEL32.dll/CreateFile
- DynamicLoader: KERNEL32.dll/CreateFileW
- DynamicLoader: rtm.dll/MgmGetNextMfeStats
- DynamicLoader: KERNEL32.dll/LoadLibraryA
- DynamicLoader: KERNEL32.dll/GetProcAddress
- DynamicLoader: KERNEL32.dll/ReadProcessMemory
- DynamicLoader: KERNEL32.dll/CreateProcessA
- DynamicLoader: KERNEL32.dll/WriteProcessMemory
- DynamicLoader: KERNEL32.dll/GetThreadContext
- DynamicLoader: ntdll.dll/ZwUnmapViewOfSection
- DynamicLoader: KERNEL32.dll/VirtualAllocEx
- DynamicLoader: KERNEL32.dll/SetThreadContext
- DynamicLoader: KERNEL32.dll/ResumeThread
- DynamicLoader: ole32.dll/CoWaitForMultipleHandles
- DynamicLoader: sechost.dll/LookupAccountNameLocalW
- DynamicLoader: ADVAPI32.dll/LookupAccountSidW
- DynamicLoader: sechost.dll/LookupAccountSidLocalW
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptGenRandom
- DynamicLoader: ole32.dll/NdrOleInitializeExtension
- DynamicLoader: ole32.dll/CoGetClassObject
- DynamicLoader: ole32.dll/CoGetMarshalSizeMax
- DynamicLoader: ole32.dll/CoMarshalInterface
- DynamicLoader: ole32.dll/CoUnmarshalInterface
- DynamicLoader: ole32.dll/StringFromIID
- DynamicLoader: ole32.dll/CoGetPSClsid
- DynamicLoader: ole32.dll/CoTaskMemAlloc
- DynamicLoader: ole32.dll/CoTaskMemFree
- DynamicLoader: ole32.dll/CoCreateInstance
- DynamicLoader: ole32.dll/CoReleaseMarshalData
- DynamicLoader: ole32.dll/DcomChannelSetHResult
- DynamicLoader: RpcRtRemote.dll/I_RpcExtInitializeExtensionPoint
- DynamicLoader: mscorwks.dll/_CorDllMain
- 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: CRYPTSP.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/EventUnregister
- 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: comctl32.dll/
- DynamicLoader: ole32.dll/CoUninitialize
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: profapi.dll/
- DynamicLoader: PROPSYS.dll/
- DynamicLoader: ole32.dll/PropVariantClear
- DynamicLoader: OLEAUT32.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: PROPSYS.dll/InitPropVariantFromStringAsVector
- DynamicLoader: PROPSYS.dll/PSCoerceToCanonicalValue
- DynamicLoader: PROPSYS.dll/PropVariantToStringAlloc
- DynamicLoader: ole32.dll/CoAllowSetForegroundWindow
- 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: SETUPAPI.dll/PnpIsFilePnpDriver
- DynamicLoader: kernel32.dll/RegOpenKeyExW

- DynamicLoader: kernel32.dll/RegCloseKey
- DynamicLoader: DEVRTL.dll/DevRtlGetThreadLogToken
- DynamicLoader: apphelp.dll/AllowPermLayer
- DynamicLoader: kernel32.dll/BaseIsAppcompatInfrastructureDisabled
- DynamicLoader: apphelp.dll/SdbInitDatabase
- DynamicLoader: apphelp.dll/SdbGetMatchingExe
- DynamicLoader: apphelp.dll/SdbReleaseDatabase
- DynamicLoader: MPR.dll/WNetGetConnectionW
- DynamicLoader: ole32.dll/CoCreateGuid
- DynamicLoader: RPCRT4.dll/RpcStringBindingComposeW
- DynamicLoader: RPCRT4.dll/RpcBindingFromStringBindingW
- DynamicLoader: RPCRT4.dll/RpcStringFreeW
- DynamicLoader: RPCRT4.dll/RpcBindingSetAuthInfoExW
- DynamicLoader: RPCRT4.dll/NdrClientCall2
- DynamicLoader: ntdll.dll/RtlDllShutdownInProgress
- DynamicLoader: comctl32.dll/
- DynamicLoader: ole32.dll/OleUninitialize
- DynamicLoader: ole32.dll/CoRevokeInitializeSpy
- DynamicLoader: comctl32.dll/
- DynamicLoader: OLEAUT32.dll/
- DynamicLoader: sfc.dll/SfcIsFileProtected
- DynamicLoader: apphelp.dll/AllowPermLayer
- DynamicLoader: kernel32.dll/BaseIsAppcompatInfrastructureDisabled
- DynamicLoader: ADVAPI32.dll/UnregisterTraceGuids
- DynamicLoader: comctl32.dll/
- 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: USER32.dll/RegisterRawInputDevices
- DynamicLoader: USER32.dll/GetRawInputData
- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- 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: 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
- DynamicLoader: wkscli.dll/NetGetJoinInformation
- DynamicLoader: netutils.dll/NetApiBufferFree

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

- ioc: v2.0.50727

Reads data out of its own binary image

- self_read: process: StartUpHost.exe, pid: 2172, offset: 0x00000000, length: 0x00020000

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\Install\Host.exe
- binary: C:\Users\Seven01\AppData\Local\Temp\StartUpHost.exe

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://dresson1.com/wip-admin/js/Panel/five/fre.php

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

- IP: 91.192.100.3:1199 (Switzerland)

SetUnhandledExceptionFilter detected (possible anti-debug)

2 HTTP Request(s) detected

http://dresson1.com/wip-admin/js/Panel/five/fre.php
Hostname: dresson1.com
IP Address: 0.0.0.0
Port: 80
Count: 2

http://dresson1.com/wip-admin/js/Panel/five/fre.php
Hostname: dresson1.com
IP Address: 0.0.0.0
Port: 80
Count: 12

1 Host(s) detected

IP Address	Hostname	Reverse DNS
91.192.100.3		91-192-100-3.gerber.non-logging.vpn.

1 Countr(y|ies) detected

Hosts	Country
1	Switzerland