Report #13639

Creation Date: Sept. 11, 2021, 9:22 p.m.
Last Update: Sept. 11, 2021, 9:27 p.m.
File:
NewHello.exe
Results:

Binary

DLL	**False**
Size	5.00KB
trid	**81.0%** Generic CIL Executable **7.2%** Win32 Dynamic Link Library **4.9%** Win32 Executable **2.2%** OS/2 Executable **2.2%** Generic Win/DOS Executable
type	PE
wordsize	32
Subsystem	Windows CLI

Hashes

md5	62d2761bd5c33184f5f394b8a5232af6
sha1	ae8f31dad61e272b84048dc896318982e619a901
crc32	0xb335d9
sha224	fbf080dd05761d6a60c896b5335779d923c399159e06be6e3c85d34e
sha256	cb722390fb9e87f12974af6f8a5c458b46335631adb9e486fc3bdb012d9188a4
sha384	d435e476aeaab489c3b0bf3c05d387560ffab0bb9d7f9b1a8ac7068062d24a8161f986e307591fc2dc2e023b3fe3570b
sha512	f938e757eb84b782e54282616518097270118 82f440816353c2f6239671391e5306ccd9cf6e77954d3bedb100e3e3005a5d3b72700a2eca9c4ee00dfe6672f6f
ssdeep	48:60FMtHYxdZ6BWuJLiAOtPgI66LCDMlYol34mgFWSfbNtm:tv+Otos6t9ozNt

Community

Google	**False**
HashLib	**False**

YARA

Matches	NET_executable, contentis_base64, Microsoft_Visual_C_v70_Basic_NET, Microsoft_Visual_Studio_NET_additional, IP, IsNET_EXE, NETexecutableMicrosoft, Microsoft_Visual_C_Basic_NET, Microsoft_Visual_Studio_NET, HasDebugData, IsConsole, NET_executable_, domain, IsPE32, Microsoft_Visual_C_v70_Basic_NET_additional
Suspicious	**True**

Imports

mscoree.dll	_CorExeMain

Strings

List

c:\Users\Win\Documents\Visual Studio 2012\Projects\NewHello\NewHello\obj\Release\NewHello.pdb
<assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
1.0.0.0
1.0.0.0
1.0.0.0
1.0.0.0
NewHello.exe
NewHello.exe
NewHello.exe
mscoree.dll
DebuggableAttribute
DebuggingModes
$ec4a2ec5-9dd8-4a3f-9a0a-149ae8e7beab
<requestedExecutionLevel level="asInvoker" uiAccess="false"/>
_CorExeMain
#Strings
RuntimeCompatibilityAttribute
ComVisibleAttribute
<Module>
</assembly>
ProductName
TargetFrameworkAttribute
AssemblyCultureAttribute
GuidAttribute
AssemblyTitleAttribute
InternalName
OriginalFilename
FileDescription
WriteLine

VarFileInfo
StringFileInfo
FileVersion
mscorlib
Hello, world!
Translation
NewHello
NewHello
NewHello
NewHello
#GUID
Program
Copyright
Copyright
Assembly Version
Console
.ctor
Object
`.rsrc
System
Main
<security>
args
2021
2021
</security>
RSDS
!This program cannot be run in DOS mode.
VS_VERSION_INFO
.NETFramework,Version=v4.5
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
AssemblyCopyrightAttribute
System.Runtime.InteropServices
AssemblyProductAttribute
AssemblyCompanyAttribute
System.Runtime.Versioning
System.Runtime.CompilerServices
System.Reflection
CompilationRelaxationsAttribute
AssemblyVersionAttribute
AssemblyTrademarkAttribute
AssemblyFileVersionAttribute
AssemblyDescriptionAttribute
AssemblyConfigurationAttribute
</requestedPrivileges>
LegalCopyright
System.Diagnostics
.NET Framework 4.5
WrapNonExceptionThrows
FrameworkDisplayName
</trustInfo>
@.reloc
ProductVersion
<requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
000004b0
#Blob
.text
v4.0.30319
*BSJB

vyfF
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
.3x.;
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">

Foremost

Matches	0.exe, 5 KB
Suspicious	**True** ✅

Heuristics

IPs	**hasIPs**: **False** ❌ **Allowed** **Suspicious** **hasAllowed**: **False** ❌ **hasSuspicious**: **False** ❌
URLs	**Allowed** **hasURLs**: **False** ❌ **Suspicious** **hasAllowed**: **False** ❌ **hasSuspicious**: **False** ❌
Files	**Allowed**: mscoree.dll **hasFiles**: **True** ✅ **Suspicious** **hasAllowed**: **True** ✅ **hasSuspicious**: **False** ❌

Binary

Sizes	**RVA** **RVA:** 16 **Suspicious:** **False** ❌ **Code** **Size:** 2048 **Suspicious:** **False** ❌ **Image** **Address:** 4194304 **Suspicious:** **False** ❌ **Stack** **Stack:** 4096 **Suspicious:** **False** ❌ **Headers** **Headers:** 512 **Suspicious:** **False** ❌ **Suspicious**: **False** ❌

Symbols

Number
Number: 0
Suspicious: True
Pointer
Pointer: 0
Suspicious: True
Directories
Number: 16
Suspicious: False

Checksum

Value: 0
Suspicous: True

Sections

Allowed: .text, .rsrc, .reloc
Suspicious
hasAllowed: True
hasSections: True
hasSuspicious: False

Versions

OS
Version: 4
Suspicious: False
Image
Version: True
Suspicious: 4
Linker
Version: 11.0
Suspicious: False
Subsystem
Version: 6.0
Suspicious: False
Suspicious: False

EntryPoint

Address: 10238
Suspicious: False

Anomalies

Anomalies: The header checksum and the calculated checksum do not ma
tch.
hasAnomalies: True

Libraries

Allowed: mscoree.dll
hasLibs: True
Suspicious
hasAllowed: True
hasSuspicious: False

Timestamp

Past: False
Valid: True
Value: 2021-08-20 12:36:51
Future: False

Compilation	**Packed**: False **Missing**: False **Packers** **Compiled**: True **Compilers**: Microsoft Visual C# / Basic .NET, Microsoft Visual Studio .NET, .NET executable, Microsoft Visual C# v7.0 / Basic .NET
Obfuscation	**XOR**: False **Fuzzing**: False

PEDetector

Matches	None
Suspicious	False

Disassembly

hasTricks	False
Tricks	

AVclass

File

Trace

11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\mscorrc.dll
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\mscorrc.dll.DLL
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\System32\mscorrc.dll
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\System32\mscorrc.dll.DLL
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\mscorrc.dll
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\mscorrc.dll

11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\system\mscorrc.dll	
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\mscorrc.dll	
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Monitor\mscorrc.dll	
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\mscorrc.dll	
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\mscorrc.dll	
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\wbem\mscorrc.dll	
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\mscorrc.dll	
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\malware.exe.config	
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\Microsoft.NET\Framework\v4.0.40305	
11/9/2021 - 20:45:43.418	Open	2476	C:\malware.exe	C:\Windows\Microsoft.NET\Framework\v4.0.40305	
11/9/2021 - 20:45:43.434	Open	2476	C:\malware.exe	C:\Windows\Fonts\StaticCache.dat	
11/9/2021 - 20:45:43.434	Read	2476	C:\malware.exe	C:\Windows\Fonts\StaticCache.dat	StaticCache.dat
11/9/2021 - 20:45:43.434	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\uxtheme.dll	
11/9/2021 - 20:45:43.434	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\uxtheme.dll	
11/9/2021 - 20:45:43.481	Open	2476	C:\malware.exe	C:\dwmapi.dll	
11/9/2021 - 20:45:43.481	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\dwmapi.dll	
11/9/2021 - 20:45:43.481	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\dwmapi.dll	
11/9/2021 - 20:45:43.481	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\ole32.dll	

11/9/2021 - 20:45:43.481	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\ole32.dll	
11/9/2021 - 20:45:43.481	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\rpcss.dll	
11/9/2021 - 20:45:43.481	Open	2476	C:\malware.exe	C:\Windows\SysWOW64\rpcss.dll	
11/9/2021 - 20:45:43.481	Open	2476	C:\malware.exe	C:\Windows\Globalization\Sorting\SortDefault.nls	
11/9/2021 - 20:45:43.481	Unknown	2476	C:\malware.exe	C:\Windows\Globalization\Sorting\SortDefault.nls	SortDefault.nls

Process

Trace

Analysis

Reason Timeout

Status Sucessfully Executed

Results 1

Registry

Trace

File Summary

Created **Identified**: False

Deleted **Identified**: False

Process Summary

Created **Identified**: False

Deleted **Identified**: False

Registry Summary

Proxy **Identified**: False

AutoRun **Identified**: False

Created **Identified**: False

Deleted **Identified**: False

Browsers **Identified**: False

Internet **Identified**: False

DNS

Query

Response

TCP

Info

UDP

Info

HTTP

Info

Summary

DNS	**False** ✗
TCP	**False** ✗
UDP	**False** ✗
HTTP	**False** ✗

Results

BINARY

NFS 2.0 (Threshold = 0.8)
confidence: 75.00%
suspicious: **False** ✗

NFS 3.0 (Threshold = 0.75)
confidence: 64.00%
suspicious: **False** ✗

Decision Tree (NFS-BRMalware)
confidence: 100.00%
suspicious: **True** ✓

MalConv (Ember: Raw Bytes, Threshold=0.5)
confidence: 98.02%
suspicious: **True** ✓

Random Forest (100 estimators, NFS-BRMalware)
confidence: 59.00%
suspicious: **True** ✓

Non-Negative MalConv (Ember: Raw Bytes, Threshold=0.35)
confidence: 89.15%
suspicious: **True** ✓

LightGDM (Ember: File Characteristics, Threshold=0.8336)

confidence: 99.99%
suspicious: **False**