xcitium

MALWARE
Xcitium Final Verdict

File Name: Servidor.exe
File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: 96ee36b80ad6918ccd1e5568ab9522c27cdeced7
MD5: 1ba88acd9206b22b8b55e903f86db7b6
First Seen Date: 2024-11-24 15:41:49 UTC
Number of Clients Seen: 2
Last Analysis Date: 2024-11-25 07:17:01 UTC
Human Expert Analysis Date: 2024-11-25 07:17:00 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2024-11-24 16:04:30 UTC	Malware
Static Analysis Overall Verdict	2024-11-25 07:17:01 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2024-11-25 07:17:01 UTC	Highly Suspicious
Precise Detectors Overall Verdict	2024-11-25 07:17:01 UTC	No Match
Human Expert Analysis Overall Verdict	2024-11-25 07:17:00 UTC	Malware
File Certificate Validation		Not Applicable

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Clean
Timestamp value suspicious	Clean
Header Checksum is zero!	Suspicious
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Anti-vm present	Clean
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean
TLS callback functions array detected	Clean

Packer detection on signature database

- Microsoft Visual C# / Basic .NET
- .NET executable

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

SUSPICIOUS BEHAVIORS	
Creates a child process	
Writes to address space of another process	
Uses a function clandestinely	
Reads memory of another process	
Opens a file in a system directory	
Has no visible windows	

Behavioral Information

LoadLibrary

ADVAPI32.dll
SHLWAPI.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
mscoree.dll
ntdll
advapi32.dll
shell32.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\38bf604432e1a30c954b2ee40d6a2d1c\mscorlib.ni.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
ole32.dll
kernel32.dll
AdvApi32.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\908ba9e296e92b4e14bdc2437edac603\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\12dc10e5c0e8d176cf21a16a6fc5fc3b\Microsoft.VisualBasic.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\5a401fd2a7689ff13fb54182953f9c40\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\6949c4470a81970ec3de0a575d93babc\System.Windows.Forms.ni.dll
shfolder.dll
kernel32
Secur32.dll
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
SHELL32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
OLEAUT32.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
CRYPTBASE.dll

LowerChar

file

CreateProcess

netsh firewall add allowedprogram "C:\Users\win7\Desktop\server.exe" "server.exe" ENABLE
"C:\Users\win7\Desktop\server.exe"

ReadFile

C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config

DeleteFile

C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.1660.1240093
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.1660.1240093
C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.1660.1240093

OpenMutex

Global\CLR_CASOFF_MUTEX

CreateMutex

<NULL>
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

QueryFilePath

C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Users\win7\Desktop\server.exe
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Servidor.exe

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\M
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Micro
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index1c2
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFra
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NE
\REGISTRY\USER\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

QueryProcessAddress

CreateProcess
CreateProcessW

CreateRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2024-11-24 15:41:45 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2024-11-24 15:41:45 UTC	No Match	NotDetected
Static Precise NI Detector 3	2024-11-24 15:41:46 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2024-11-24 15:41:46 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2024-11-24 15:41:46 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2024-11-24 15:41:46 UTC	No Match	NotDetected
Static Precise PUA Detector 6	2024-11-24 15:41:46 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2024-11-24 15:41:46 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2024-11-24 15:41:46 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2024-11-24 15:41:46 UTC	No Match	NotDetected
Static Precise Trojan Detector 13	2024-11-24 15:41:46 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2024-11-24 15:41:46 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2024-11-25 05:49:35 UTC
Analysis End Date: 2024-11-25 07:17:00 UTC
File Upload Date: 2024-11-24 15:41:38 UTC
Human Expert Analyst Feedback:
Verdict: Malware
Malware Family:
Malware Type: Worm

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5AC310B9 [Tue Apr 3 05:27:21 2018 UTC]
Debug Artifacts	
Entry Point	0x4101de (.text)
Exifinfo	[object Object]
File Size	73216
File Type Enum	6
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Translation	0x0000 0x04b0
Legal Copyright	
Assembly Version	1.0.0.0
Internal Name	Stub.exe
File Version	1.0.0.0
Product Version	1.0.0.0
File Description	
Original Filename	Stub.exe
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	fad707c342f6f41c9f76434d28df10df06a52c924fd915b09951bd2c62294f7a
Ssdeep	768:4pSOG3GqPvLzsrMHcskVqTz43fB4O3o81rS0cG/6MGDlrT2JaazYcHeUZ:Mo3f3qskVqTzIZLndnZ6tTUanU
Trid	56.7,Generic CIL Executable (.NET, Mono, etc.),21.3,Win64 Executable (generic),10.1,Windows screen saver,5,Win32 Dynamic Link Library (generic),3.4,Win32 Executable (generic)

File Paths

FILE PATH ON CLIENT	SEEN COUNT
Servidor.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0xe1e4	0xe200	5.5929722676	b0674191a97465b1ff73c929bb502c15
.rsrc	0x12000	0x3800	0x3800	3.98287079969	2989abfbf69fba60870a657d6e2e24a3
.reloc	0x16000	0xc	0x200	0.0815394123432	d0fff904de6b3ded996250744c03c5dc