xcitium

MALWARE
Xcitium Final Verdict

File Name: HEUR-Backdoor.Win32.Agent.gen-1867b4e2bff0da299be111bc931ce43ba5f3a1f65f399c71391b9326ab878ec2
File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: 08034ba0242dd08bedb4b51d035ad5719d13a287
MD5: 37f02ddf1ef0f4b25b24636bb7145391
First Seen Date: 2023-07-24 18:26:07 UTC
Number of Clients Seen: 5
Last Analysis Date: 2023-07-25 16:42:56 UTC
Human Expert Analysis Date: 2023-07-25 16:42:54 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-07-25 16:42:56 UTC	Malware
Static Analysis Overall Verdict	2023-07-25 16:42:56 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-07-25 16:42:56 UTC	No Match
Human Expert Analysis Overall Verdict	2023-07-25 16:42:54 UTC	Malware
File Certificate Validation		Not Applicable

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

SUSPICIOUS BEHAVIORS
Injects code to another process
Modifies context of another process
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
kernel32.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
ole32.dll
AdvApi32.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\culture.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\en-US\mscorrc.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\en\mscorrc.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorrc.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\908ba9e296e92b4e14bdc2437edac603\System.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
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\ntdll.dll
ntdll.dll

LowerChar

file

CreateProcess

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.2696.296203
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2696.296203
C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2696.296234

OpenMutex

Global\CLR_CASOFF_MUTEX

CreateMutex

<NULL>

QueryFilePath

C:\Windows\SYSTEM32\MSCOREE.DLL
C:\HEUR-Backdoor.Win32.Agent.gen-1867b4e2bff0da299be111bc931ce43ba5f3a1f65f399c71391b9326ab878ec2
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

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\M
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\61e7e666\c991064

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion
\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\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NE
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32

QueryProcessAddress

WriteProcessMemory
CreateProcess
CreateProcessA
GetThreadContext
SetThreadContext

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise NI Detector 3	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2023-07-24 18:26:02 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2023-07-24 18:26:02 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-07-25 05:39:48 UTC
Analysis End Date: 2023-07-25 16:42:54 UTC
File Upload Date: 2023-07-24 18:25:59 UTC
Human Expert Analyst Feedback: Kryptik
Verdict: Malware
Malware Family: Trojware
Malware Type: Trojan Generic

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5B22DD70 [Thu Jun 14 21:26:08 2018 UTC]
Debug Artifacts	[object Object]
Entry Point	0x44be5e (.text)
Exifinfo	[object Object]
File Size	445952
File Type Enum	6
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Translation	0x0000 0x04b0
Legal Copyright	@KTQYW
Assembly Version	0.0.2.3
Internal Name	QDEFLK.exe
File Version	0.0.2.3
Comments	KTQYW
Product Name	KTQYW
Product Version	0.0.2.3
File Description	KTQYW
Original Filename	QDEFLK.exe
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	1867b4e2bff0da299be111bc931ce43ba5f3a1f65f399c71391b9326ab878ec2
Ssdeep	6144:ErTLzV8Mb5ZVQhuaSZOPioKIWMgqPn2ijABoby:I53hrqidINF2
Trid	63.1,Generic CIL Executable (.NET, Mono, etc.),23.8,Win64 Executable (generic),5.6,Win32 Dynamic Link Library (generic),3.8,Win32 Executable (generic),1.7,Generic Win/DOS Executable

File Paths

FILE PATH ON CLIENT	SEEN COUNT
HEUR-Backdoor.Win32.Agent.gen-1867b4e2bff0da299be111bc931ce43ba5f3a1f65f399c71391b9326ab878ec2	2
C:\Users\nikol\Downloads\Virusshare.00324\HEUR-Backdoor.Win32.Agent.gen-1867b4e2bff0da299be111bc931ce43ba5f3a1f65f399c71391b9326ab878ec2	2

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0x49ed2	0x4a000	6.21490411221	3b44d27301ffa90ee3e42089fd605eac
.rsrc	0x4c000	0x22850	0x22a00	4.02927525127	97d4957530e762d7617e5f0a4625fe35
.reloc	0x70000	0xc	0x200	0.101910425663	fe1f2c1b4758325756b464a70310428b