xcitium

MALWARE
Xcitium Final Verdict

File Name: Trojan.MSIL.Crypt.dnbp-929b9dcfc8a43721ece5cb448cb486fbf5f5ded0f290eb1973a1ade67a1fab10
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: c85530bfd84b61f2aaad539a348d3032b934f8a2
MD5: 630582ca84cc7d3b995c79cf19f67397
First Seen Date: 2023-07-26 19:36:44 UTC
Number of Clients Seen: 4
Last Analysis Date: 2023-07-26 20:45:10 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-07-27 13:56:29 UTC	Malware
Static Analysis Overall Verdict	2023-07-26 20:45:10 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-07-26 20:45:10 UTC	No Match
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	Suspicious
Header Checksum is zero!	Clean
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	Suspicious
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

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	!

Behavioral Information

LoadLibrary

MSCOREE.DLL
Kernel32.dll
ADVAPI32.dll
kernel32.dll
SHLWAPI.dll
C:\Windows\system32\ole32.dll
C:\Windows\system32\uxtheme.dll
C:\Windows\system32\shell32.dll
ole32.dll
comctl32.dll
C:\Windows\system32\shfolder.dll
C:\Windows\system32\Rstrtmgr.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
C:\Users\win7\AppData\Local\Temp\is-ECSF5.tmp\isxdl.dll
wininet.dll
C:\Windows\system32\msi.dll
UxTheme.dll
IMM32.dll
C:\Windows\system32\imageres.dll
C:\Windows\system32\shlwapi.dll
C:\Windows\system32\RICHED20.DLL

CreateProcess

"C:\Users\win7\AppData\Local\Temp\is-ECSF5.tmp\dotnetchk.exe"

CreateMutex

<NULL>
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000

OpenMutex

Local\MSCTF.Asm.MutexDefault1
DefaultTabtip-MainUI

WriteFile

C:\Users\win7\AppData\Local\Temp\is-ECSF5.tmp\isxdl.dll
C:\Users\win7\AppData\Local\Temp\is-ECSF5.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-ECSF5.tmp\dotnetchk.exe
C:\[uTrojan.MSIL.Crypt.dnbp-929b9dcfc8a43721ece5cb448cb486fbf5f5ded0f290eb1973a1ade67a1fab10]

ReadFile

C:\[uTrojan.MSIL.Crypt.dnbp-929b9dcfc8a43721ece5cb448cb486fbf5f5ded0f290eb1973a1ade67a1fab10]

C:\Windows\Fonts\staticcache.dat

QueryFilePath

C:\Users\win7\AppData\Local\Temp\is-ECSF5.tmp\dotnetchk.exe
C:\Users\win7\AppData\Local\Temp\is-IFO05.tmp\[uTrojan.MSIL.Crypt.tmp
C:\Windows\system32\MSCOREE.DLL
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\system32\RICHED20.DLL

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\M
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Micro
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFra
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
\REGISTRY\MACHINE\SOFTWARE\Microsoft\.NETFramework
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NE

QueryProcessAddress

InternetReadFile

CreateRegistryKey

\REGISTRY\US

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-07-26 20:45:06 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2023-07-26 20:45:06 UTC	No Match		NotDetected
Static Precise NI Detector 3	2023-07-26 20:45:06 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2023-07-26 20:45:06 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2023-07-26 20:45:06 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2023-07-26 20:45:06 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2023-07-26 20:45:07 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2023-07-26 20:45:07 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2023-07-26 20:45:07 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2023-07-26 20:45:07 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2023-07-26 20:45:07 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2023-07-26 20:45:07 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Not Verified ✖

[+] null

Status	Not Valid ✖

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
Debug Artifacts	
Entry Point	0x40aa98 (CODE)
Exifinfo	[object Object]
File Size	4703240
File Type Enum	6
Imphash	2fb819a19fe4dee5c03e8c6a79342f79
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	2015
File Version	4.0
Company Name	Compusoft Hard- & Software GmbH
Comments	This installation was built with Inno Setup.
Product Name	ShopLuKaSOXID
Product Version	4.0
File Description	Artikel Abgleichsystem zu Oxid 4.x Shops
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	929b9dcfc8a43721ece5cb448cb486fbf5f5ded0f290eb1973a1ade67a1fab10
Ssdeep	98304:n5S5cx58o/LlOSfNugUO58ziZkgwtIEcXSHWkUfBpdASQSUV+YHtRJqq4O:E5c/8S5ugXEYkTL41fBXQzv714O
Trid	77.7,Inno Setup installer,10,Win32 Executable Delphi generic,4.6,Win32 Dynamic Link Library (generic),3.1,Win32 Executable (generic),1.4,Win16/32 Executable Delphi generic

File Paths

FILE PATH ON CLIENT	SEEN COUNT
Trojan.MSIL.Crypt.dnbp-929b9dcfc8a43721ece5cb448cb486fbf5f5ded0f290eb1973a1ade67a1fab10	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0xa1d0	0xa200	6.64374902859	b7ea439d9c6d5ec722056c9243fb3054
DATA	0xc000	0x250	0x400	2.74012451302	9b2268ed5360951559d8041925d025fb
BSS	0xd000	0xe94	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xe000	0x97c	0xa00	4.48607624623	df5f31e62e05c787fd29eed7071bf556
.tls	0xf000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x10000	0x18	0x200	0.190488766435	14dfa4128117e7f94fe2f8d7dea374a0
.reloc	0x11000	0x91c	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x12000	0x2374	0x2400	5.24117495604	7d190f730e071f82229f85f543e6873b