xcitium

CLEAN
Xcitium Final Verdict

File Name: 73cc3a2d9846e4a98158e080cf58190d249796de85f334859ad89fd9cec293f7.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 04da8b89c7390f01818a0a5cb9a7f4ef368607b7
MD5: 6953452ad7d9e8a32b59afc707b11147
First Seen Date: 2023-08-10 18:16:54 UTC
Number of Clients Seen: 2
Last Analysis Date: 2023-08-10 18:16:54 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Trusted Vendor

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-08-10 18:16:54 UTC	Clean
Static Analysis Overall Verdict	2023-08-10 18:16:54 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-08-10 18:16:54 UTC	No Match
File Certificate Validation		Certificate and Vendor name are Valid

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	Suspicious
Timestamp value suspicious	Clean
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	Clean
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	!
Uses a function clandestinely	!
Has no visible windows	!

Behavioral Information

QueryFilePath

C:\Windows\syswow64\CRYPT32.dll
C:\Windows\system32\cryptnet.dll
C:\Windows\System32\msxml3.dll
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll

LowerChar

http

OpenService

dbupdatem

CreateMutex

<NULL>

OpenMutex

Local\MSCTF.Asm.MutexDefault1

WriteFile

C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2023-08-10-18-16-58-824-556

ReadFile

C:\Windows\Fonts\staticcache.dat

LoadLibrary

SHLWAPI.dll
SHELL32.dll
USER32.dll
WINTRUST.dll
CRYPTSP.dll
ADVAPI32.dll
CRYPTBASE.dll
WINTRUST.DLL
C:\Windows\syswow64\CRYPT32.dll
imagehlp.dll
ncrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
bcrypt.dll
crypt32.dll

USERENV.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
cryptnet.dll
C:\Windows\system32\cryptnet.dll
profapi.dll
API-MS-WIN-Service-Management-L1-1-0.dll
API-MS-WIN-Service-winsvc-L1-1-0.dll
RPCRT4.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
CRYPT32.dll
VERSION.dll
ADVAPI32.DLL
cscapi.dll
dbghelp.dll
rpcrt4.dll
ntmarta.dll
kernel32.dll
comctl32.dll
UxTheme.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
C:\Windows\System32\msxml3r.dll
C:\Windows\system32\ole32.dll

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-08-10 18:16:51 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2023-08-10 18:16:51 UTC	No Match		NotDetected
Static Precise NI Detector 3	2023-08-10 18:16:51 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2023-08-10 18:16:51 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2023-08-10 18:16:51 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2023-08-10 18:16:51 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2023-08-10 18:16:51 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2023-08-10 18:16:51 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2023-08-10 18:16:52 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2023-08-10 18:16:52 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2023-08-10 18:16:52 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2023-08-10 18:16:52 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Verified ✔

[+] Dropbox, Inc

Status	Valid ✔

Certificate Validation - Success ✔

[+] Dropbox, Inc

Status	NoError ✔
Start Date	2020-11-16 02:00:00
End Date	2024-02-10 01:59:59
Sha256	f43608bcf51d74bdb9124f52bac0f87169817b07bb1a567bae099f18bc6699db
Serial	0F7A165550163D5ED7D1CAA3FC13DA06
Subject Name	Dropbox, Inc
Subject Key Identifier	14 1e 10 78 b6 75 d7 ca fb 3a 99 59 f2 6b c3 b6 ef 3b 5f 05
Subject Organization	Dropbox, Inc
Subject Locality	San Francisco
Subject State	California
Subject Country	US
Issuer Name	DigiCert SHA2 Assured ID Code Signing CA
Issuer Key Identifier	5a c4 b9 7b 2a 0a a3 a5 ea 71 03 c0 60 f9 2d f6 65 75 0e 58
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	http://crl3.digicert.com/sha2-assured-cs-g1.crl,http://crl4.digicert.com/sha2-assured-cs-g1.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] DigiCert SHA2 Assured ID Code Signing CA

Status	NoError ✔
Start Date	2013-10-22 03:00:00
End Date	2028-10-22 03:00:00
Sha256	febf4b512ecfb3aff46ebd345ddcb88497e1ce4e89245c2fd6e23a3146836e11
Serial	0409181B5FD5BB66755343B56F955008
Subject Name	DigiCert SHA2 Assured ID Code Signing CA
Subject Key Identifier	5a c4 b9 7b 2a 0a a3 a5 ea 71 03 c0 60 f9 2d f6 65 75 0e 58
Subject Organization	DigiCert Inc
Subject Country	US
Subject Organizational Unit	www.digicert.com
Issuer Name	DigiCert Assured ID Root CA
Issuer Key Identifier	45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl,http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] DigiCert Assured ID Root CA

Status	NoError ✔
Start Date	2006-11-10 02:00:00
End Date	2031-11-10 02:00:00
Sha256	69656a6548d46f112fad68a56675b12667e863fe923f84fb47014c2cc5352b40
Serial	0CE7E0E517D846FE8FE560FC1BF03039
Subject Name	DigiCert Assured ID Root CA
Subject Key Identifier	45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Subject Organization	DigiCert Inc
Subject Country	US
Subject Organizational Unit	www.digicert.com
Issuer Name	DigiCert Assured ID Root CA
Issuer Key Identifier	45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f
Issuer Organization	DigiCert Inc
Issuer Country	US
Issuer Organizational Unit	www.digicert.com
Crl link	undefined
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x642F63C0 [Fri Apr 7 00:28:48 2023 UTC]
Debug Artifacts	[object Object]
Entry Point	0x404c96 (.text)
Exifinfo	[object Object]
File Size	788872
File Type Enum	6
Imphash	958c2a9b1453bda1d16ee4d06228bab6
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Copyright: Dropbox, Inc. 2015 (Omaha Copyright Google Inc.)
Internal Name	Dropbox Update Setup
File Version	1.3.761.1
Company Name	Dropbox, Inc.
Language Id	en
Product Name	Dropbox Update
Product Version	1.3.761.1
File Description	Dropbox Update Setup
Original Filename	DropboxUpdateSetup.exe
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	73cc3a2d9846e4a98158e080cf58190d249796de85f334859ad89fd9cec293f7
Ssdeep	24576:O7eit0t9EsyC1XS64DbvYwdzv1n4WwwS6u3sK:O7eimfEsr1X/4wwbn4Wpi
Trid	42.2,Win32 Executable MS Visual C++ (generic),37.3,Win64 Executable (generic),8.8,Win32 Dynamic Link Library (generic),6,Win32 Executable (generic),2.7,Generic Win/DOS Executable

File Paths

FILE PATH ON CLIENT	SEEN COUNT
73cc3a2d9846e4a98158e080cf58190d249796de85f334859ad89fd9cec293f7.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xbcb2	0xbe00	6.6652747181	3860778f5779efc8591c093e44085a1f
.rdata	0xd000	0x2ae4	0x2c00	5.4368053299	95e296e5c8c6376cccbd9404ba2bcb2c
.data	0x10000	0x191c	0xe00	2.48258261615	b021e5ad7a13cc5ffe4115f9f8e19471
.rsrc	0x12000	0xaccd8	0xace00	7.95159280819	86030499f0e052bec9937f032ecaaf0a
.reloc	0xbf000	0x1530	0x1600	3.86610822062	a1cf57f9dbfb3eaf67c2f3aee2cd0bdc