xcitium

MALWARE
Xcitium Final Verdict

File Name: Virus.Hijack.ATA_virussign.com_3f9b65da3cbb6e85b37e3dd1bffd7c27.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: cc612626fc7d41cc411a3879f4f61904a7032b2d
MD5: 3f9b65da3cbb6e85b37e3dd1bffd7c27
First Seen Date: 2023-12-21 11:16:07 UTC
Number of Clients Seen: 2
Last Analysis Date: 2023-12-21 16:42:38 UTC
Human Expert Analysis Date: 2023-12-21 16:42:28 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-12-21 12:18:48 UTC	Malware
Static Analysis Overall Verdict	2023-12-21 16:42:38 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-12-21 16:42:38 UTC	No Match
Human Expert Analysis Overall Verdict	2023-12-21 16:42:28 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	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

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise NI Detector 3	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise PUA Detector 6	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise Trojan Detector 13	2023-12-21 11:17:17 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2023-12-21 11:17:17 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-12-21 12:57:22 UTC
Analysis End Date: 2023-12-21 16:42:28 UTC
File Upload Date: 2023-12-21 11:15:53 UTC
Human Expert Analyst Feedback:
Verdict: Malware
Malware Family:
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	0x3B6DF214 [Mon Aug 6 01:25:40 2001 UTC]
Debug Artifacts	
Entry Point	0x401002 (.text)
Exifinfo	[object Object]
File Size	210944
File Type Enum	6
Imphash	4de9a64c7b78c158a506f9a22164c6d2
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Slodge
File Version	2.3.6.0
Company Name	Symantec Corporation
Product Name	Eudaemonism
Product Version	5.5.1.3
File Description	preagriculture
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	11
Sha256	15088529f28727662902dde6f51468fa368dbc463ea0dbe7a803728a2aa929d4
Ssdeep	6144:ru6ABIdHMnMMYGlPtFYmeiGLaMt8ApYUBvNdP4y2:ruLIHMhPtFvei8aM2Aa8N+y2
Trid	67.4,Win32 Executable MS Visual C++ (generic),14.2,Win32 Dynamic Link Library (generic),9.7,Win32 Executable (generic),4.3,Generic Win/DOS Executable,4.3,DOS Executable Generic

File Paths

FILE PATH ON CLIENT	SEEN COUNT
Virus.Hijack.ATA_virussign.com_3f9b65da3cbb6e85b37e3dd1bffd7c27.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x30cd	0x3200	6.27552805821	45f953b4fc1712afcc19a0d4cd2e2e5b
.NkRgVz	0x5000	0x5326	0x400	4.11404297885	3713e2c1cd85545ab87c34355df4b918
.iggwRn	0xb000	0x632f	0x800	2.66080873609	44482ad21916bf1f811ea61d34b0c338
.VcFX	0x12000	0x8c30	0x1000	5.10882677077	907a07be9fc671f17f6e6efb91a693fb
.fEO	0x1b000	0xab7f	0x200	0.678487628487	ae4c46b09e665b288b08879631dccfb5
.vLt	0x26000	0x2166	0x200	5.73441849966	b91e4f2644ad88413c02e71710b8f928
.data	0x29000	0x2788	0x2800	6.91759646568	cccc31b69afc68fa5f429b0efe69b153
.cJGHT	0x2c000	0x4edd	0x800	6.51399236334	616094adae796b16859d62f612de4472
.XUTdU	0x31000	0x346e3	0x200	1.00934536028	5afc59354a50ffe7aff6c73c6193f6e7
.rsrc	0x66000	0x2a8bc	0x2aa00	7.97331447483	24737936d890e3eda87e6840b65018bd
.reloc	0x91000	0x4b2	0x600	6.20248544531	c18905d312147e3f3ac36951e6f091d6