xcitium

MALWARE
Xcitium Final Verdict

File Name: virussign.com_754ab92ada89fdd88a100e5dd854dcb0.exe
File Type: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
SHA1: f2c7dbed7119e7c49e43bbc00bcfa56ddd091a2b
MD5: 754ab92ada89fdd88a100e5dd854dcb0
First Seen Date: 2024-12-02 09:26:55 UTC
Number of Clients Seen: 2
Last Analysis Date: 2024-12-02 14:39:43 UTC
Human Expert Analysis Date: 2024-12-02 14:38:34 UTC
Human Expert Analysis Result: Malware
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2024-12-02 09:48:24 UTC	Malware	!
Static Analysis Overall Verdict	2024-12-02 14:39:43 UTC	Highly Suspicious	!
Precise Detectors Overall Verdict	2024-12-02 14:39:43 UTC	No Match	?
Human Expert Analysis Overall Verdict	2024-12-02 14:38:34 UTC	Malware	!
File Certificate Validation		Not Applicable	?

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	!

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!	Suspicious	!
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Suspicious	!
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	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise PUA Detector 4	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise NI Detector 3	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise PUA Detector 5	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 1	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 3	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise PUA Detector 6	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 12	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise Virus Detector 1	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise Virus Detector 2	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 13	2024-12-02 09:26:51 UTC	No Match	?	NotDetected
Static Precise PUA Detector 2	2024-12-02 09:26:51 UTC	No Match	?	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2024-12-02 10:40:05 UTC

Analysis End Date: 2024-12-02 14:38:34 UTC

File Upload Date: 2024-12-02 09:26:44 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	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
Debug Artifacts	
Entry Point	0x456464 (UPX1)
Exifinfo	[object Object]
File Size	626454
File Type Enum	6
Imphash	bcf75e287e43fcf41bb59e2f7e37a071
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Sunward Information Technology Co.Ltd
Internal Name	BarClientView.exe
File Version	2010, 8, 6, 1
Company Name	Sunward Information Technology Co.Ltd
Product Name	BarClientView.exe
Product Version	7, 1, 3, 0
File Description	BarClientView.exe
Original Filename	BarClientView.exe
Translation	0x0804 0x03a8
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	ee459eb850f0c934651a4b7b85827cd033834e1f3efec3d0f1c6ac8f772f293c
Ssdeep	12288:TGzQYR4IeaAVB6ETW82Ku8UKfdndrQwoS:T8lgaAVB6evW8UKlndr
Trid	31.8,UPX compressed Win32 Executable,31.2,Win32 EXE Yoda's Crypter,16.6,Win32 Executable Delphi generic,7.7,Win32 Dynamic Link Library (generic),5.3,Win32 Executable (generic)

File Paths

FILE PATH ON CLIENT	SEEN COUNT
virussign.com_754ab92ada89fdd88a100e5dd854dcb0.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x46000	0x46000	6.55769308275	383abeef443b2fc8705703d906449477
UPX1	0x47000	0x25000	0x24400	4.59093188705	50a563cd7035d408d6c11ae2cbbe0c4b
.rsrc	0x6c000	0x1000	0xe00	4.62426498288	0430fbc0a5270693a437c9a5fb069fd7
.imports	0x6d000	0x2000	0x1800	4.49361700883	b0bb39e16175f74c1a74a094dfc5e365