xcitium

MALWARE
Xcitium Final Verdict

File Name: virussign.com_0c9f08df1bf2a0666465ecbaf5aa2429.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 45dfed147a1f20b0de6a4d505c7b5cbca9af9215
MD5: 0c9f08df1bf2a0666465ecbaf5aa2429
First Seen Date: 2025-08-20 13:56:12 UTC
Number of Clients Seen: 3
Last Analysis Date: 2025-08-22 10:34:50 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	2025-08-22 10:32:20 UTC	Malware
Static Analysis Overall Verdict	2025-08-22 10:34:50 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2025-08-22 10:34:50 UTC	No Threat Found
Precise Detectors Overall Verdict	2025-08-22 10:34:50 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!	Suspicious
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

Packer detection on signature database

BobSoft Mini Delphi -> BoB / BobSoft

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	
Uses a function clandestinely	

Behavioral Information

CreateMutex

<NULL>

LoadLibrary

C:\[uvirussign.com_0c9f08df1bf2a0666465ecbaf5aa2429.ENU
C:\[uvirussign.com_0c9f08df1bf2a0666465ecbaf5aa2429.EN
comctl32.dll
SXS.DLL
API-MS-Win-Security-LSALookup-L1-1-0.dll
ADVAPI32.dll
CRYPTBASE.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
C:\Windows\system32\advapi32.dll
OLEAUT32
ole32.dll
OLEAUT32.dll
uxtheme.dll
UxTheme.dll
IMM32.dll

QueryFilePath

C:\[uvirussign.com_0c9f08df1bf2a0666465ecbaf5aa2429.exe]

ReadFile

C:\Windows\system32\wbem\wbemdisp.TLB
C:\Windows\SysWOW64\stdole2.tlb
C:\Windows\Fonts\staticcache.dat

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\WBEM\Sc

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2025-08-22 10:34:46 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2025-08-22 10:34:46 UTC	No Match	NotDetected
Static Precise NI Detector 3	2025-08-22 10:34:46 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2025-08-22 10:34:46 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2025-08-22 10:34:46 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2025-08-22 10:34:46 UTC	No Match	NotDetected
Static Precise PUA Detector 6	2025-08-22 10:34:47 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2025-08-22 10:34:47 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2025-08-22 10:34:47 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2025-08-22 10:34:47 UTC	No Match	NotDetected
Static Precise Trojan Detector 13	2025-08-22 10:34:47 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2025-08-22 10:34:47 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

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	0x49f310 (CODE)
Exifinfo	[object Object]
File Size	766976
File Type Enum	6
Imphash	1e1b13fd9d6cf9b82e5bb930338cf535
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	\xa9 2010 A&C
Internal Name	SpamAgree
File Version	1.0.0.0
Company Name	A&C
Legal Trademarks	No trademarks available
Comments	\u0415\u0441\u043b\u0438 \u0412\u044b \u0437\u0430\u043f\u0443\u0441\u043a\u0430\u0435\u0442\u0435 \u043f\u0440\u043e\u0433\u0440\u0430\u043c\u043c\u0443 \u0432\u043f\u0435\u0440\u0432\u044b\u0435, \u043f\u043e\u0436\u0430\u043b\u0443\u0439\u0441\u0442\u0430, \u043f\u043e\u0437\u0430\u0431\u043e\u0442\u044c\u0442\u0435\u0441\u044c \u043e \u0442\u043e\u043c, \u0447\u0442\u043e\u0431\u044b \u043f\u043e\u043b\u0443\u0447\u0438\u0442\u044c \u043a\u043e\u043c\u0444\u043e\u0440\u0442\u043d\u0443\u044e \u0440\u0430\u0431\u043e\u0442\u0443 \u0441\u043e \u0441\u043b\u0443\u0436\u0435\u0431\u043d\u044b\u043c \u0441\u0442\u0438\u043a\u0435\u0440\u043e\u043c.
Product Name	VK LoveMachine
Product Version	1.0.0.0
File Description	VK Love Machine
Original Filename	vk-love.exe
Translation	0x0419 0x04e3
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	73e6a344c741d910edcb5063defae65b869dbe6cdbc46e46d93711ca98d58d7e
Ssdeep	12288:zpiPwxtupQm/OLsGbQyBk6FZE/JwW7jamnfoNhCXJr:zpo2tzm/O98h6FZqORy06r
Trid	65.5,Win32 Executable Borland Delphi 7,25.9,Win32 Executable Borland Delphi 6,4.1,Win32 EXE PECompact compressed (generic),1.3,Win32 Executable Delphi generic,1.2,Windows screen saver

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x9e3a8	0x9e400	6.53999656747	dd86969847a3c1ce282cbfbade841996
DATA	0xa0000	0x29b0	0x2a00	4.94939034513	65f4d4cc5a4da7e11995e7705f8f051f
BSS	0xa3000	0xffd	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xa4000	0x250c	0x2600	4.88203058627	f064811bd4a4e8eb383dce479b2d0d62
.tls	0xa7000	0x10	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xa8000	0x18	0x200	0.180244406087	e28d5301ee1bf2f9dfa5ba959382df06
.reloc	0xa9000	0xb704	0xb800	6.64577000908	6e66fb2b8e6a2e459933f3e99956fb80
.rsrc	0xb5000	0xc200	0xc200	5.06423016841	6741c6c1a4e4d93fa5e553f22fc2ccaa