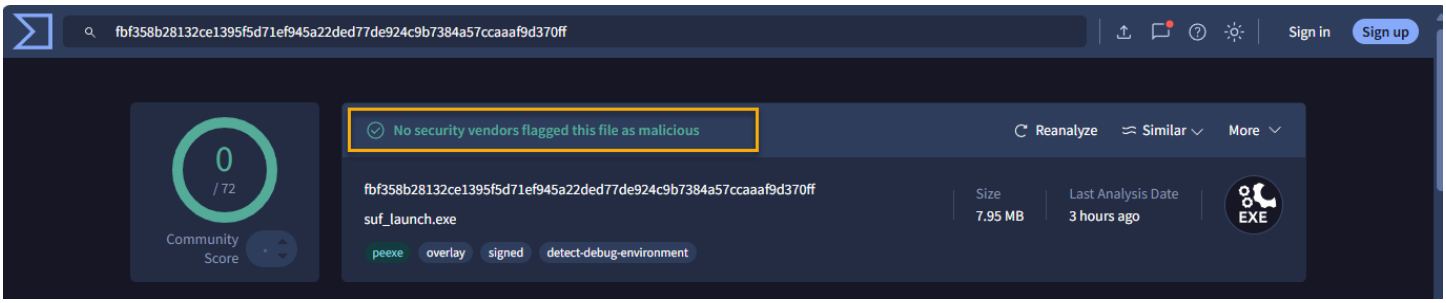
fbf358b28132ce1395f5d71ef945a22ded77de924c9b7384a57ccaaaf9d370ff
Sign in
Sign up
0
/ 72
Community Score
No security vendors flagged this file as malicious
Reanalyze
Similar
More
fbf358b28132ce1395f5d71ef945a22ded77de924c9b7384a57ccaaaf9d370ff
suf_launch.exe
peexe
overlay
signed
detect-debug-environment
Size
7.95 MB
Last Analysis Date
3 hours ago
EXE

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | RELATIONS | BEHAVIOR

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Basic properties

MD5	6a41a345400c1c14e2ef70d4c63cc145
SHA-1	f03ac8b68ddd06eeb9a2441512c69d4f906f2be9
SHA-256	fbf358b28132ce1395f5d71ef945a22ded77de924c9b7384a57ccaa…
Vhash	086056655d555550a01010061z996z130a5zb0500da3z19z
Authentihash…	973473aecaa8d61fe161166caf69eec2ca6ea969ebf448a9e157a5f…
Imphash	42f8ab45a28dc8866c775fcbab7b12b0
Rich PE heade…	d633ecfd47f96fef15f96bd66da89941
SSDEEP	196608:MHfQbVTS8R4hsGduATf9wESYMlCXsu6KKOyf9KCvjSNOI…
TLSH	T11E86123A7A72C072D6323230969DA379E6BDB8305B3546931A…
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	InstallShield setup (42%) Win32 Executable MS Visual C++ (ge…
DetectItEasy	PE32 Installer: Setup Factory (9.0) Compiler: EP:Microsoft …
Magika	PEBIN
File size	7.95 MB (8334768 bytes)

History

Creation Time…	2025-03-25 15:19:56 UTC
Signature Dat…	2025-04-17 17:07:00 UTC
First Submissi…	2025-04-17 17:46:50 UTC
Last Submissi…	2025-04-17 17:46:50 UTC
Last Analysis	2025-04-17 17:46:50 UTC

Names

basicAppraisals Setup.exe

suf_launch

suf_launch.exe

Signature info

Signature Verification

Signed file, valid signature

File Version Information

Copyright	Setup Engine Copyright © 2004-2025 Indigo Rose Corporation
Product	Setup Factory Runtime
Description	Setup Application
Original Name…	suf_launch.exe
Internal Name…	suf_launch
File Version	10.0.0.0
Comments	Created with Setup Factory
Date signed	2025-04-17 17:07:00 UTC

Signers

Phase25, LLC

Sectigo Public Code Signing CA R36

Sectigo Public Code Signing Root R46

Sectigo (AAA)

Counter Signers

Sectigo Public Time Stamping Signer R36

Sectigo Public Time Stamping CA R36

Sectigo Public Time Stamping Root R46

X509 Certificates

Sectigo Public Code Signing Root R46

Sectigo Public Code Signing CA R36

Phase25, LLC

Sectigo Public Time Stamping Signer R36

Sectigo Public Time Stamping CA R36

Sectigo Public Time Stamping Root R46

Indigo Rose Software Design Corporation

USERTrust RSA Certification Authority

Certera Code Signing CA

Sectigo Public Time Stamping Signer R35

Portable Executable Info

Compiler Products

[C++] VS2008 SP1 build 30729 count=1

[ASM] VS2010 SP1 build 40219 count=43

[C] VS2010 SP1 build 40219 count=180

[C] VS2008 SP1 build 30729 count=12

[IMP] VS2008 SP1 build 30729 count=35

[---] Unmarked objects count=763

[C++] VS2010 SP1 build 40219 count=373

[RES] VS2010 SP1 build 40219 count=1

[LNK] VS2010 SP1 build 40219 count=1

Header

Target Machin…	Intel 386 or later processors and compatible processors
Compilation T…	2025-03-25 15:19:56 UTC
Entry Point	988763
Contained Se…	5

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	1125362	112537 6	6.52	9910e488 25765e90 bb2756e7 356fa653	7222 902
.rdata	1130496	264908	265216	5	8dd1dea8 94c16507 9fad50e4 b77c1ec4	1322 6036
.data	1396736	52608	22528	4.7	5864de61 278e56d6 81c6acad 4c7aa0d9	9129 93.88
.rsrc	1449984	28564	28672	5.87	0a426ad8 bd05278a 5ba973bc 4eca93c1	7235 05.75

.reloc	1478656	165164	165376	4.91	5e0dc7fbc004ebc65c58b623fdd7f31a	6652644.5

Imports

- KERNEL32.dll
- USER32.dll
- ADVAPI32.dll
- SHELL32.dll
- MSIMG32.dll
- COMCTL32.dll
- SHLWAPI.dll
- OLEACC.dll
- gdiplus.dll
- IMM32.dll

Contained Resources By Type

RT_ICON	9
RT_GROUP_IC…	1
RT_VERSION	1
RT_MANIFEST…	1

Contained Resources By Language

ENGLISH US	12

Contained Resources

SHA-256	File Type	Type	Language	Entropy	Chi2
bb69db8fabd21337e457a739d0c541c759678d349e900d52f5dfa22828f326e5	unkn own	RT_ICON	ENGLISH US	3.37	1559 3.3
1f8d3da0dd89dca26c6bb14ac7be9ed5a0	unkn own	RT_ICON	ENGLISH US	4.31	1085 14.33

1bc929574ad46b875					
24f251e80e2be					
06fb164c24b5774aa	unkn	RT_I	ENGLISH	5.95	2049
1cc61dee3855f98998	own	CON	US		4.46
e7d8b80e7370403da					
6c202f054da8					
a8af8d3e6282e1efdd	unkn	RT_I	ENGLISH	3.78	2769
38fb2787c9ec42cfbb	own	CON	US		1.95
f9cd1d473f6845590c					
3e31ea3c11					
31e4e1eea0a0e2e64	unkn	RT_I	ENGLISH	6.15	4630
43773d356ddca1fe2	own	CON	US		0.79
8d32e74727a13638c					
85bdbd78281a6					

Overlay

chi2	166071.48
filetype	unknown
entropy	7.987391471862793
offset	1608192
md5	b0597c75a39da0e886eb98f534687b84
size	6726576