2 / 72

Community Score 1

2/72 security vendors flagged this file as malicious

Reanalyze Similar More

91e405e8a527023fb8696624e70498ae83660fe6757cef4871…

boinc.exe

Size 5.63 MB

Last Analysis Date 7 days ago

EXE

peexe overlay checks-network-adapters checks-cpu-name detect-debug-environment signed long-sleeps 64bits

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

Basic properties

MD5	760f00e30887017cdea9809fd1c38e52
SHA-1	b09271e96ff73b86bd54489fbae1c224369a8bc8
SHA-256	91e405e8a527023fb8696624e70498ae83660fe6757cef4871ce9bcc659264d3
Vhash	056076655d1565551552d2z132zc2fz1013zf5z77z
Authentihash	4d3f7e268c1fe8833f5526b853ef7f8fbe93699ca8df36de3ddc2c79531df9cb
Imphash	d5e3ebbf14ec4a1d261dc82f389028f3
Rich PE header hash	ad5d9ae329862bf4aa0071976171077f
SSDEEP	98304:6+2pAHOueLXU0GbPaJXlr99CvGisAbPwCWTxvXXE+NKTyqp+:6JAHOueLXfCPaJXlr99Cvt3b4CYxvXXV
TLSH	T12C56AEA9A6BD00DAD8FA81B9C3865233D772781517B067CF56A09AF50F27AD01F7B700
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32+ executable (console) x86-64, for MS Windows
TrID	Windows Control Panel Item (generic) (72.7%) | Win64 Executable (generic) (13.2%) | Win16 NE executable (generic) (6…
DetectItEasy	PE64 | Compiler: Microsoft Visual C/C++ (19.36.33523) [C++] | Linker: Microsoft Linker (14.36.33523) | Tool: Visual Stud…
Magika	PEBIN
File size	5.63 MB (5900128 bytes)

History

Creation Time	2024-05-24 12:27:56 UTC
Signature Date	2024-05-26 00:05:00 UTC
First Seen In The Wild	2024-07-09 16:59:05 UTC
First Submission	2024-05-27 21:40:29 UTC
Last Submission	2024-10-22 18:34:32 UTC
Last Analysis	2024-10-26 07:23:18 UTC

Names

boinc.exe
SecurityHealthService.exe
boinc_cli
SecurityHealthService.exe (copy)
trustedinstaller.exe
gupdate.exe
.exe
xxx_trustedinstaller_exe.xxx
.exe (copy)
EULA_Updater_trustedinstaller.exe

Signature info

Product	BOINC client
Description	BOINC client
Original Name	boinc.exe
Internal Name	boinc_cli
File Version	8.0.2
Date signed	2024-05-26 00:05:00 UTC

Signers

+ University of California, Berkeley
+ Sectigo Public Code Signing CA R36
+ Sectigo Public Code Signing Root R46
+ Sectigo (AAA)

Counter Signers

+ Sectigo RSA Time Stamping Signer #4
+ Sectigo RSA Time Stamping CA
+ Sectigo

X509 Certificates

+ Sectigo Public Code Signing Root R46
+ Sectigo Public Code Signing CA R36
+ University of California, Berkeley
+ Sectigo RSA Time Stamping CA
+ Sectigo RSA Time Stamping Signer #4

SpcSpOpusInfo

+ BOINC Client Software

Portable Executable Info

Compiler Products

[C] VS2022 v17.9.0 pre 1.0 build 33218 count=19
[ASM] VS2022 v17.9.0 pre 1.0 build 33218 count=23
[C++] VS2022 v17.9.0 pre 1.0 build 33218 count=85
[---] Unmarked objects count=351
[C] VS2008 SP1 build 30729 count=1
[C++] VS2008 SP1 build 30729 count=1
[---] Unmarked objects (old) count=36
[---] Resource count=1
id: 0x103, version: 30795 count=20
id: 0x105, version: 30795 count=211

Header

Target Machine	x64
Compilation Timestamp	2024-05-24 12:27:56 UTC
Entry Point	2318520
Contained Sections	7

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	4237692	4237824	6.82	eff2d8fa0b367f8e50d2ab0426feffc1	19276056
.rdata	4243456	1135080	1135104	5.43	fb45abf9fb9c06e49a9cfa3290b8d074	38479636
.data	5382144	538584	44544	2.74	04ccd21fd4d842cfcaec9e4adbf33183	3940653.5
.pdata	5943296	160068	160256	6.32	9077e3c5aa5002a2fd0ee8fa1f994ab8	2828232.25
_RDATA	6107136	69892	70144	5.37	4ab051b5326cfd256e7ccaf706cd2a82	3392525.25

Imports

- WSOCK32.dll
- WINHTTP.dll
- SensApi.dll
- USERENV.dll
- IPHLPAPI.DLL
- KERNEL32.dll
- USER32.dll
- ADVAPI32.dll
- Secur32.dll
- WTSAPI32.dll

Contained Resources By Type

RT_ICON	11
RT_GROUP_ICON	1
RT_VERSION	1
RT_MANIFEST	1

Contained Resources By Language

NEUTRAL	12
ENGLISH US	2

Contained Resources

SHA-256	File Type	Type	Language	Entropy	Chi2
fa69adfb35340e780a63fee37a09767c7c489552a600f380f4bc25ce75d64033	unknown	RT_ICON	NEUTRAL	5.43	34365.23
a4910ba0b77b5fab2fae22fd1f09b94f27020fb301930822318abadf01a5d510	unknown	RT_ICON	NEUTRAL	5.31	60047.18
9366d51c6e4091a03b947330fe8975c8b0e9e1a75b028e9d92d9a0b82177b7fa	unknown	RT_ICON	NEUTRAL	5.11	101172.01
021cab81717656eff2638c2576275933b3d6293b0737294d500c6d4847562856	unknown	RT_ICON	NEUTRAL	4.65	210061.36
738bc7feaa68b76be9261460b6d718c44a51479268f33317cb258d9bf0094ace	unknown	RT_ICON	NEUTRAL	4.24	407718.31

Overlay

chi2	8484.73
filetype	unknown
entropy	7.626925468444824
offset	5890048
md5	6eb8d0d8925dc13274e2449d9ca1c972
size	10080