

364275326bbfc4a3b89233dabdaf3230a3d149ab774678342a40644ad9f8d614

Sign in

Sign up

42

/ 71

Community Score

⚠️ 42/71 security vendors flagged this file as malicious

↻ Reanalyze

⌵ Similar

⌵ More

364275326bbfc4a3b89233dabdaf3230a3d149ab774678...

Size

Last Analysis Date

⚙️🌙

EXE

Maxar.dll

182.46 MB

26 days ago

peexe

overlay

64bits

- DETECTION
- DETAILS
- RELATIONS
- BEHAVIOR
- COMMUNITY1

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic properties ⓘ	
MD5	6fd5d31d607a212c6f7651c79e7655a3
SHA-1	ddd18e208aff7b00a46e06f8d9485f81ff4221ea
SHA-256	364275326bbfc4a3b89233dabdaf3230a3d149ab774678342a40644ad9f8d614
Vhash	0180a666155d156d1d055148zc76z141c5z13z2ez5
Authentihash	b1a875c95e50fc472b16ef6f2448fdb08deb2a9334b2cc6ada71d4209e704fed
Imphash	68031a2b11c02bee00a0a687110994be
Rich PE header hash	4cf709c26001c9fad8711318c8c4abd7
SSDEEP	786432:fcfVFSPtqkFfux1Kq0DsqEnz1XSY3v9XSIsmhidXposvHH7QdPA0mgErPrzlEsp:EfzSPTqkGM16zsY3hSCKWsf7Qggmz...
TLSH	T10A988C14A7E81B15D27BC27896778552E6B1BC47A320C2CF0085FA493F73BC27A3576A
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32+ executable (GUI) x86-64, for MS Windows
TrID	Windows Control Panel Item (generic) (63.7%) Win64 Executable (generic) (11.6%) Win32 Dynamic Link Library (gen...
DetectItEasy	PE64 Compiler: Microsoft Visual C/C++ (19.36.32534) [LTCG/C++] Linker: Microsoft Linker (14.36.32534) Tool: Visua...
Magika	PEBIN
File size	182.46 MB (191326614 bytes)

History ⓘ	
Creation Time	2023-07-13 21:34:00 UTC
First Seen In The Wild	2023-11-13 13:52:43 UTC
First Submission	2024-01-05 06:57:35 UTC
Last Submission	2024-06-26 12:59:15 UTC
Last Analysis	2024-10-07 06:27:34 UTC

Names ⓘ	
Maxar.dll	
malwaresample.exe.vir	
364275326bbfc4a3b89233dabdaf3230a3d149ab774678342a40644ad9f8d614	

Signature info ⓘ											
<div>Signature Verification</div> <div>⚠️ File is not signed</div>											
<div>File Version Information</div> <table><tr><td>Product</td><td>Maxar</td></tr><tr><td>Description</td><td>Maxar</td></tr><tr><td>Original Name</td><td>Maxar.dll</td></tr><tr><td>Internal Name</td><td>Maxar.dll</td></tr><tr><td>File Version</td><td>1.0.0.0</td></tr></table>		Product	Maxar	Description	Maxar	Original Name	Maxar.dll	Internal Name	Maxar.dll	File Version	1.0.0.0
Product	Maxar										
Description	Maxar										
Original Name	Maxar.dll										
Internal Name	Maxar.dll										
File Version	1.0.0.0										

X509 Certificates

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Notice](#).

Microsoft Code Signing PCA 2010

Ok

↑

💬

?

⚙

Sign in

Sign up

DotNetRuntimeInfo

MetaDataGetDispenser

g_CLREngineMetrics

g_dacTable

Contained Resources By Type

RT_RCDATA2

RT_GROUP_ICON1

RT_VERSION1

RT_MANIFEST1

RT_ICON1

Contained Resources By Language

NEUTRAL6

Contained Resources

SHA-256	File Type	Type	Language	Entropy	Chi2
f25f7a77e972ecf9bb41ef7b8f9cb1874faffad919a1a04283fd98329bb978d0	PNG	RT_ICON	NEUTRAL	7.97	972.61
53b86f9ea370f113ab680bcc19c5193f342bbb4607552d7acf4d366d58efa185	unknown	RT_RCDATA	NEUTRAL	4.34	660.89
e80b5b0a8fd69dc538bcaf660d27a54d7a919a87e3fb149fadead76ccfa7df01	DOS EXE	RT_RCDATA	NEUTRAL	6.36	11958989
c754dda45cd91b4ad5171aabf8fd5e3ec32322e5d5c6ad3ab2f125fd30f1a0a1	ICO	RT_GROUP_ICON	NEUTRAL	1.52	2386.4
9aaeecb9678baca413ad7484341e67ff73b138534e555e3fd0e9fdfb64d931a4	unknown	RT_VERSION	NEUTRAL	3.23	56130.23

▼

Overlay

chi2	1880147584
filetype	unknown
entropy	6.67561149597168
offset	9496576
md5	f382589df8fcc0c3479c5a92fa71d9f4
size	181830038

Our product	Community	Tools	Premium Services	Documentation
Contact Us	Join Community	API Scripts	Get a demo	Searching
Get Support	Vote and Comment	YARA	Intelligence	Reports
How It Works	Contributors	Desktop Apps	Hunting	API v3 v2
ToS Privacy Notice	Top Users	Browser Extensions	Graph	Use Cases
Blog Releases	Community Buzz	Mobile App	API v3 v2	