

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

https://github.com/ch2sh/Jlaive

Go

APR

MAY

SEP

14

2022

2023

About this capture

4 captures

14 May 2022 - 9 Ju

ch2sh / Jlaive

Public

Notifications

Fork 4

Star 16

<> Code

Issues 1

Pull requests

Actions

Projects

Wiki

Security

Insights







main

2 branches

15 tags

Go to file

Code

	ch2sh Use AES encryption	c1c717a 6 minutes ago	🕒 31 commits
	Jlaive-CLI	Use AES encryption	6 minutes ago
	Jlaive	Enable "Bypass AMSI" by default	6 hours ago
	Jlaive.sln	Add CLI version	yesterday
	LICENSE	Initial commit	3 days ago
	README.md	Update README.md	yesterday

☰ README.md

# Jlaive

Jlaive is an antivirus evasion tool that can convert .NET assemblies into undetectable batch files.

Support for native applications will come soon.

Join the Discord server for discussion and enquiries: <https://discord.gg/RU5RjSe8WN>.

## Screenshots

Jlaive

File path:

...

☐ Bypass AMSI

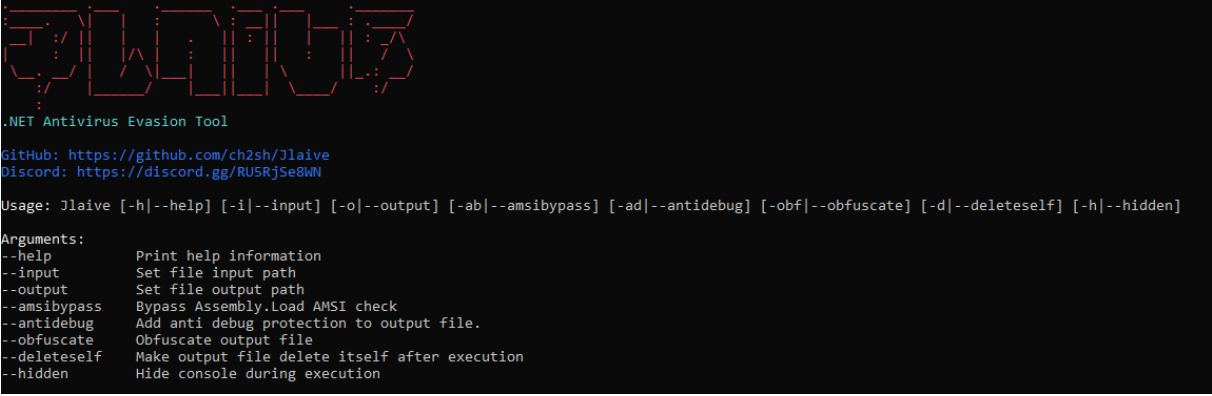
☐ Self delete

☐ Anti Debug

☐ Hidden

☐ Obfuscate

Build



### About

.NET Antivirus Evasion Tool (Exe2Bat)

[ch2sh.github.io/jlaive/](https://ch2sh.github.io/jlaive/)

- windows
- batch-file
- batch-script
- crypter
- av-evasion
- fileless

-  Readme
-  MIT license
-  16 stars
-  2 watching
-  4 forks

### Releases

🏷 15 tags

### Languages



4 captures

14 May 2022 - 9 Ju

APR

MAY

SEP

14

2022

2023

About this capture

83332a95f5031f139c5e821311df0cd940d0defacb132ff68adae43da3256dd

26

28 security vendors and no sandboxes flagged this file as malicious

83332a95f5031f139c5e821311df0cd940d0defacb132ff68adae43da3256dc

5.50 KB

2022-05-10 12:16:44 UTC

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	IL.Trojan.MSIL.Zilla.8893
AhnLab-V3	Trojan/Win32.RL_AgentTesla.C4181110	ALYac	IL.Trojan.MSIL.Zilla.8893
Arcabit	IL.Trojan.MSIL.Zilla.D22BD	Avira (no cloud)	HEUR/AGEN.1240951
BitDefender	IL.Trojan.MSIL.Zilla.8893	BitDefenderTheta	Gen.NN.ZemslCO.34638.am0@a5@q...
Bkav Pro	W32.AiDetectNet.01	Cybereason	Malicious.46421
Cynet	Malicious (score: 100)	Elastic	Malicious (high Confidence)
Emsisoft	IL.Trojan.MSIL.Zilla.8893 (B)	eScan	IL.Trojan.MSIL.Zilla.8893
Fortinet	MSIL/Kryptik.YPHtr	GData	IL.Trojan.MSIL.Zilla.8893

cf954e4b89a3b3dfe3eeefcdc02101728226ee09ad9a67cd6613035e7566dd0d

0

No security vendors and no sandboxes flagged this file as malicious

cf954e4b89a3b3dfe3eeefcdc02101728226ee09ad9a67cd6613035e7566dd0c

14.74 KB

2022-05-10 12:20:59 UTC

test\_hcrypt.bat

direct-cpu-clock-access

Community Score

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	Cynet	Undetected

## Known issues

- `Assembly.GetEntryAssembly()` returns null. Use `Assembly.GetExecutingAssembly()` instead.
- `Hidden` option does not work on Windows Terminal.

## Disclaimer

This project was made for educational purposes only. I am not responsible if you choose to use this illegally/maliciously.