a0rtega / **pafish**

Pafish is a demonstration tool that employs several techniques to detect sandboxes and analysis environments in the same way as malware families do.

malware reverse-engineering virtual-machine malware-families analysis-environments sandbox

163 commits **2** branches **16** releases **8** contributors GPL-3.0

Branch: **master** New pull request Find file Clone or download

a0rtega Bump v058 Latest commit `184b3fc` on Aug 27, 2016

pafish	Bump v058	2 years ago
screenshots	Add v057 screenshot	3 years ago
.gitignore	house-keeping	4 years ago
CHANGELOG	Bump v058	2 years ago
LICENSE.txt	Added LICENSE.txt	6 years ago
README.md	Update README with screenshot	3 years ago
pafish.exe	Bump v058	2 years ago

README.md

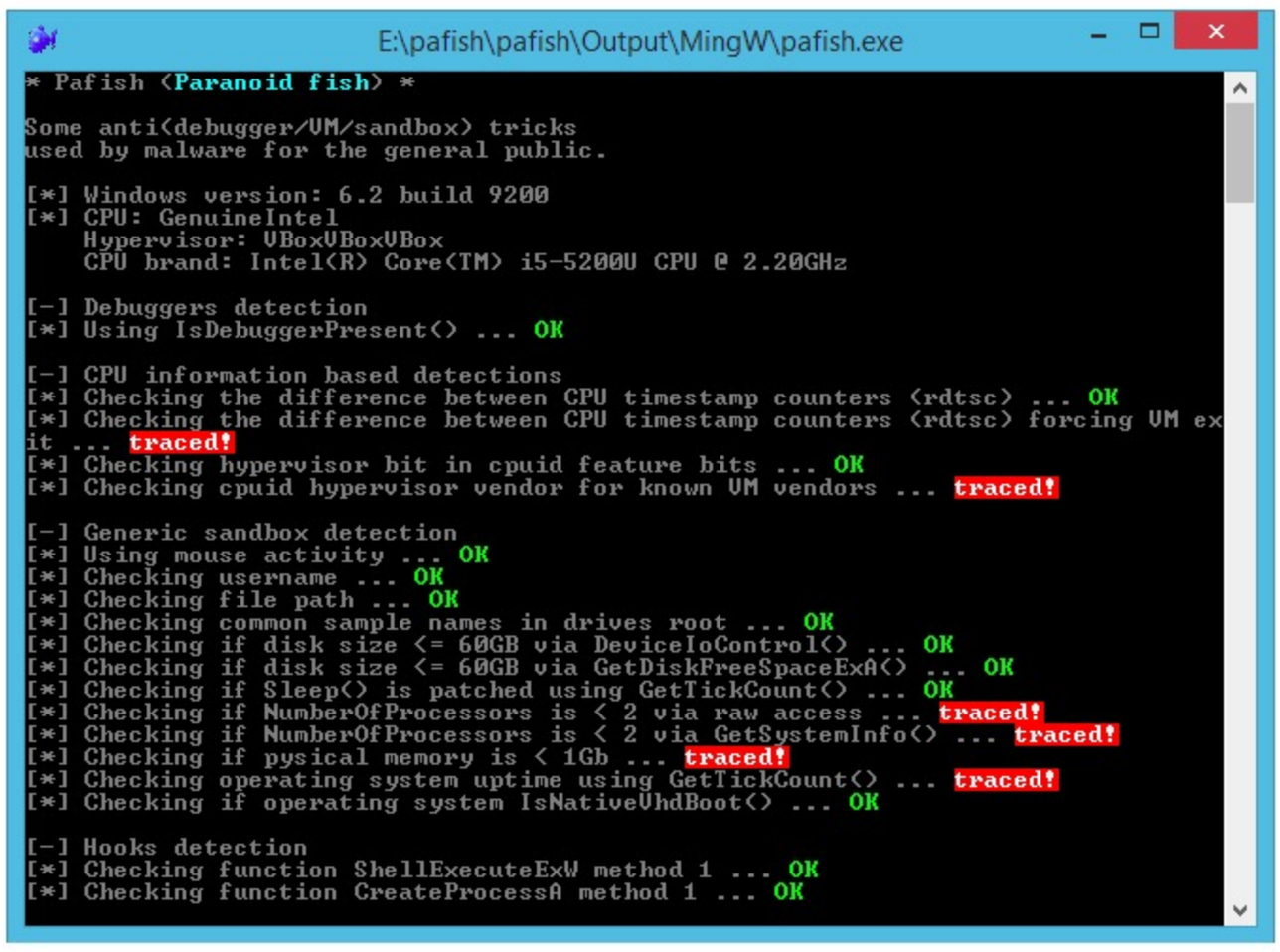
Pafish

(Paranoid Fish)

Pafish is a demonstration tool that employs several techniques to detect sandboxes and analysis environments in the same way as malware families do.

The project is open source, you can read the code of all anti-analysis checks. You can also **download** the executable of the latest stable version.

It is licensed under GNU/GPL version 3.



Scope

The objective of this project is to collect usual tricks seen in malware samples. This allows us to study them, and test if our analysis environments are properly implemented.

Build

Pafish is written in C and can be built with MinGW (gcc + make).

Check out "How to build" for detailed instructions.

Author

Alberto Ortega (@a0rtega - profile)