Pafish란?

Pafish(Paranoid Fish)는 멀웨어 패밀리와 동일한 방식으로 가상 머신 및 멀웨어 분석 환경을 탐지하기 위해 다양한 기술을 사용하는 테스트 도구이다. 해당 도구는 자유 오픈 소스이며 모든 anti-analysis 기술의 코드는 공개적으로 사용 가능하다.

Pafish에서 탐지하는 항목은 크게 아래와 같이 나눌 수 있다.

* 디버거 탐지
* CPU 정보 기반 탐지
* 리버스 튜링 테스트를 통한 가상화 탐지
* 샌드박스 탐지
* 후킹 탐지
* Sandboxie 탐지
* Wine 탐지
* VirtualBox 탐지
* VMware 탐지
* Qemu 탐지
* Bochs 탐지
* Cuckoo Sandbox 탐지

Paranoid Fish 전체 진단 결과

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

Pafish.exe를 통해 가상 환경 탐지 목록은 위와 같다. 위 이미지 중 traced! 문자열이 나온 항목이 실제 탐지된 항목이다.

Anti-Debugging Project

1) <https://www.github.com/hfiref0x/VBoxHardenedLoader>

- 2020년 중반 이후 더 이상 유지 관리되지 않음.

2) https://www.github.com/JayMontana36/vBoxSysInfoMod (6년전)

3) https://github.com/xyafes/VBoxAntiDetection(3년전)

4) https://www.github.com/d4rksystem/VBoxCloak (10개월전)

텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

VBoxCloak.ps1 -all