Выгодные покупки ТОП-10 для геймера, программиста!

ВЗЛОМ ОБЗОР

Разбираем REvil. Как известный шифровальщик прячет вызовы WinAPI

Sk.Devif 1 ноября 2021 WinAPI Дешифрование

Не так давно атаке подверглась международная система денежных переводов Travelex, а внимание этого оказался шифровальщик REvil, чьи жертвы были не знакомы. Забегая вперёд, скажу, что в этом тексте использованы простые, но интересные методы обфускации, которые не позволяют полностью скрыть от глаз используемые не вызовы WinAPI. Давай посмотрим, как устроен этот эмиссар изнутри.

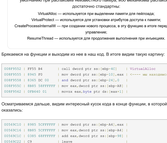
По дробной трудным запуску сенсиз в DIE и потоящих, что он нам покажет:

PE64 в программе DIE

DIE сочтет, что файл ничем не упакован. Хотя постой-ка, давай переспросимся на показания энтропии снова:

Энтропия чем больше, тем хуже

Суда по названию секций, файл упакован UPX, но он энтропии выглядит очень странно. Почему тогда DIE не распознал упаковщик? Ну, например, сигнатуры UPX может быть, намеренно искажены, чтобы запутать дизассемблеры. Так или иначе, перед нами упакованный файл, поэтому загружаем в отладчик x64dbg. Давай поставим точку остановки на функции `VirtualAlloc`, которая вмешается у нас в окрестностях точки входа, и запустим прог.


Run
Pause
Restart
Close
Settings
Trace into
Trace over
Execute till return
Execute till user code
Animate into
Animate over
Time
Trace
Trace: 0.00%
Log
Notes
Breakpoints
Memory map
Call stack
SEH
Script
Symbols
Source
00007FFD7A1A0000 00007FFD7A1A0000 00007FFD7A1A0000