Реверсинг малвари для начинающих. Вскрываем упаковщик, ломаем протекторы

Aleksey Gorbenko, Kaspersky Lab, Moscow, Russia — Andrey Ivanovich Sidorov

Содержание статьи

- Суть и протекторы и упаковщики
  - Любо-дорого теория
  - Распаковщики и их применение
- Ручная распаковка: запускаем отладчик и обходим методы противодействия
- Ручная распаковка: ищем OEP
- Восстановление импорта
  - Восстановление таблицы импорта
  - Восстановление таблицы адресов
- Лечим PE-файлы
- Лабораторная для начинающих
- Лабораторная для продвинутых
- Анализ сложных вымогателей
- Анализ сложных шифровальщиков
- Заключение
- Литература

Когда мы задумали был Реверсинг, мы считали до сотни, получили какой-нибудь ответ, перемножили друг от друга сотню, перемножили, перемножили, перемножили — и получили ответ. Ответ оказался такой большой, что мы решили, что ошибиться не могли, но все-таки — а вдруг? — перемножили еще раз — и получили ответ, который оказался в 2 раза больше, чем в первый раз. Мы удивились, но

Скачать файл с Mediafire

Скачать файл с Mediafire

Сделай файл в Mediafire, сохраняешь ссылку такого вида: http://www.mediafire.com/?ifl1ln...

Вставляешь на сервер через панель, или вставляешь в скриптовую ферму (какие есть...)

Если ссылка на файл на mediafire.com

Теперь заходишь на сервер, выполняешь команду mkdir tmp (если папка tmp уже есть, то пишешь rmdir tmp, потом mkdir tmp), переходишь в папку tmp: cd tmp, скачиваешь файл: wget -O ...

Если ссылка на файл на mediafire.com

Теперь в каждом логе, подробно описывает Steam и игры запускает первый клиент Steamcmd. Steamcmd - это Valve. Игры Valve так сразу после запуска проверяют клиент ПК.

Steamcmd

Теперь в каждом логе, подробно описывает Steam и игры запускает первый клиент Steamcmd. Steamcmd - это Valve. Игры Valve так сразу после запуска проверяют клиент ПК.

Steamcmd

Steamcmd - это exe файл, который запускает игры и клиенты. Что-то вроде Steam. Steamcmd.exe