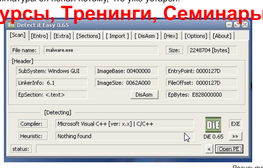
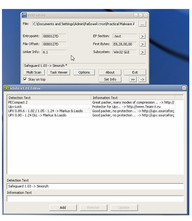
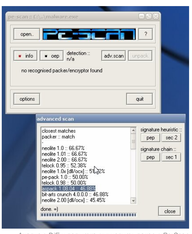
упаковщик, а в сигнатуры он попал потому, что уже устарел.



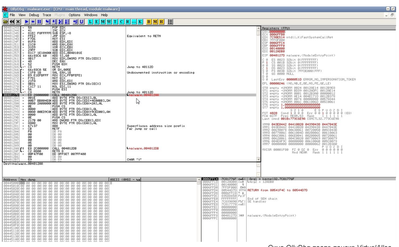
Результаты анализа PEiD





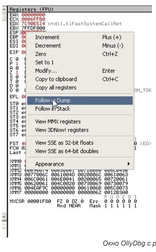
Анализ в DiE и попытка вычислить пакер в Pe-Scan

Грузим файл в OllyDbg, открываем диалог поиска по Ctrl-G, пишем VirtualAlloc, жмем OK и попадаем на нужную нам строку кода, на которой устанавливаем брейк-пойнт по F2.



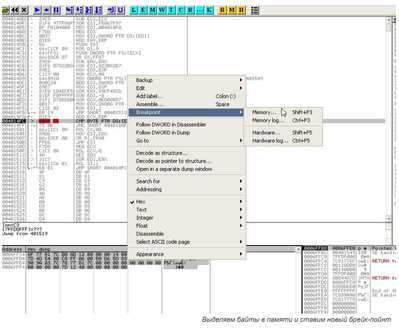
Окно OllyDbg после поиска VirtualAlloc

Теперь смело по F9 запускаем программу, пока она не остановится на брейк-пойнте. В правом окне со значением регистров на значении EAX правый щелчок мышью и выбираем Follow in Dump.



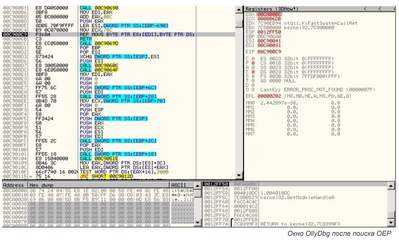
Окно OllyDbg с регистрами при выполнении дампа

Теперь в нижнее окно, выделяем несколько байтов и снова щелкаем правой кнопкой Breakpoint → Hardware, write → Byte, после чего снова запускаем программу клавишей F9.



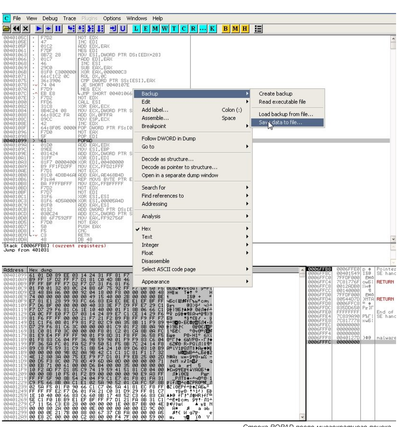
Выделяем байты в памяти и ставим новый брейк-поинт

Повторяем это до тех пор, пока снова не упремся в точку останова. Что мы видим? Неужели это нужная нам PE-секция?



Окно OllyDbg после поиска OEP

Все же нет, потому что семпл многократно запакован, соответственно, у него несколько точек загрузки пакера. Повторяем запуск по F9 еще несколько раз. Для того чтобы добраться до оригинальной OEP, нужно каждый раз ставить новые брейк-пойнты, выбирать в секции регистров Follow in Dump. Наконец мы попадем на строчку POPAD и увидим оригинальный код.



Строка POPAD после многократного поиска

Теперь все, что нам осталось, — это сдампить образ из памяти в файл на жесткий диск, выбрав в нижнем окне несколько байтов и щелкнув правой кнопкой BackUp → Save data to file.

Заключение

Сегодня мы проделали хорошую работу, вспомнили матчасть по PE-архитектуре файлов и на практике познакомились с методикой анализа и распаковки различных пакеров. Не забывай тренироваться, читать дополнительную информацию по предложенным ссылкам, самостоятельно анализируй семплы, и, безусловно, тебя будет ждать успех!

Буду рад ответить на все вопросы, связывайтесь со мной по почте или пишите в комментарии. Всем удачи в исследованиях и до новых встреч!

Благодарности

Автор и редакция благодарят Сергея Харламова, антивирусного эксперта «Лаборатории Касперского», за ценные коррективы и комментарии к готовому тексту.

WWW

— Исходные семплы малвари (пароль — malware)