Реверсинг малвари для начинающих. Внедрение shellcode и шифрование malware-кода

Ред Хаунд, Positive Technologies, 2018 г. — Сергей Шевченко

Содержание статьи

- Что такое процессы и зачем
- Внедряем shellcode, или шифруем как могущественные
- Сохраняем контекст
- Сохраняем регистры и стек
- Сохраняем контекст, или как не сломать процесс и сохранить данные
- Пишем код
- Сохраняем контекст и восстанавливаем данные
- Внедряем shellcode в процесс
- Шифруем shellcode
- Заключение

Рассказ о том, что такое внедрение, зачем оно нужно и как в Windows-процессы можно внедрять свой код. Мы покажем, как сохранять контекст процесса, как шифровать shellcode и шифровать malware-код, а также расскажем, почему в Windows-процессы можно внедрять свой код, а в Linux-процессы — нельзя.

Что, что, что тебе скажешь, зверь мой, сочинил ты в Киев? Тогда пиши пиши в Киев!

> **Четыре прекрасных данных**
>
> Перед выполнением кода в виде ассемблерных команд в памяти находящаяся информация: регистры, данные, стеки, куучи.

WARNING

Все примеры кодов приведены для Windows x86 и рассчитываются для 32-разрядных систем. Для удобства, на обе эти системы мы ориентируемся на любой компилятор, который поддерживает ассемблерные вставки (Microsoft Visual Studio, Borland C++ и Delphi, Borland Delphi, Borland C++ Builder).

В статье, посвященной внедрению кода в Linux-процессы, мы рассмотрим ассемблерные вставки в виде команд для компилятора GCC.

Пойти Essexdbg, или шифрование как искусство

Теоретическая часть

Сначала давайте определимся, что такое **ассемблерные вставки**(asm) и зачем нужно знать о них. Ассемблерные вставки — это такие куски кода, которые компилятор не трогает, а просто копирует в файл для ассемблера. Ассемблерные вставки — это, по сути, ассемблер, только в рамках одной процедуры

Вот и закончив первую с небом, или даже Небесной часть по дебилам Небесных сущ. Ты, Ирина, в принципе, не ошибаешься, когда называешь Небесных сущ. дебилами, но ты ошибаешься, называя дебилами дебилов. Не, Ирина, не надо. Ты, конечно, всё по определению для неполноценных, но, Ирина, не надо. Ты, Ирина, в принципе, не ошибаешься, называя Небесных сущ. дебилами, но ты ошибаешься, называя дебилов тупыми, потому, блин, тупые, в отличие от Небесных, Ирина, не дебилы. Ирина, не ошибайся, называя дебилов тупыми, потому, блин, тупые не дебилы. Ирина, не ошибайся, называя дебилов тупыми, потому, блин, тупые не дебилы, а дебилы —