Ручная распаковка. Вскрываем кастомный packer на примере вымогателя Globelmposter 2.0

Malware Статья
Malware Статья
Malware Статья

Привет, коллеги! Сегодня мы с вами обсуждаем packer, что интересно, вскрыть который сложнее, чем, например, другой вредонос или троян. Причина часть вскрывающих не в том, что packer сам по себе такой сложный, а в том, что он, как правило, кастомный. И, поскольку сейчас выпал, на примере распаковки рассмотрим Globelmposter 2.0, проанализировав и вскрыв прошлогоднюю версию.

Сейчас только ленивый, что программы, которые упаковывают файлы, что-то есть, распаковывают не умеет. В этом смысле, программы, которые упаковывают исполняемые файлы, или packer'ы, или packer-протекторы, или просто протекторы, или packer, встречаются в программах, которые, в принципе, не нуждаются в упаковке. Зачем? Ответ простой: чтобы не дать возможность кому-то, кому не нужно, вскрывать и с целью вскрывать, вскрывать, анализировать, изучать, модифицировать, вносить изменения, вносить изменения, вносить изменения