Статья Немного о рынке малвари

Этот текст написан с определенной целью: дать участникам форума, в первую очередь, новичкам, базовое понятие о рынке малвари.
Все нижеизложенное касается малвари под Windows. Ситуацию в андроиде я не знаю, но подозреваю, что она похожа.

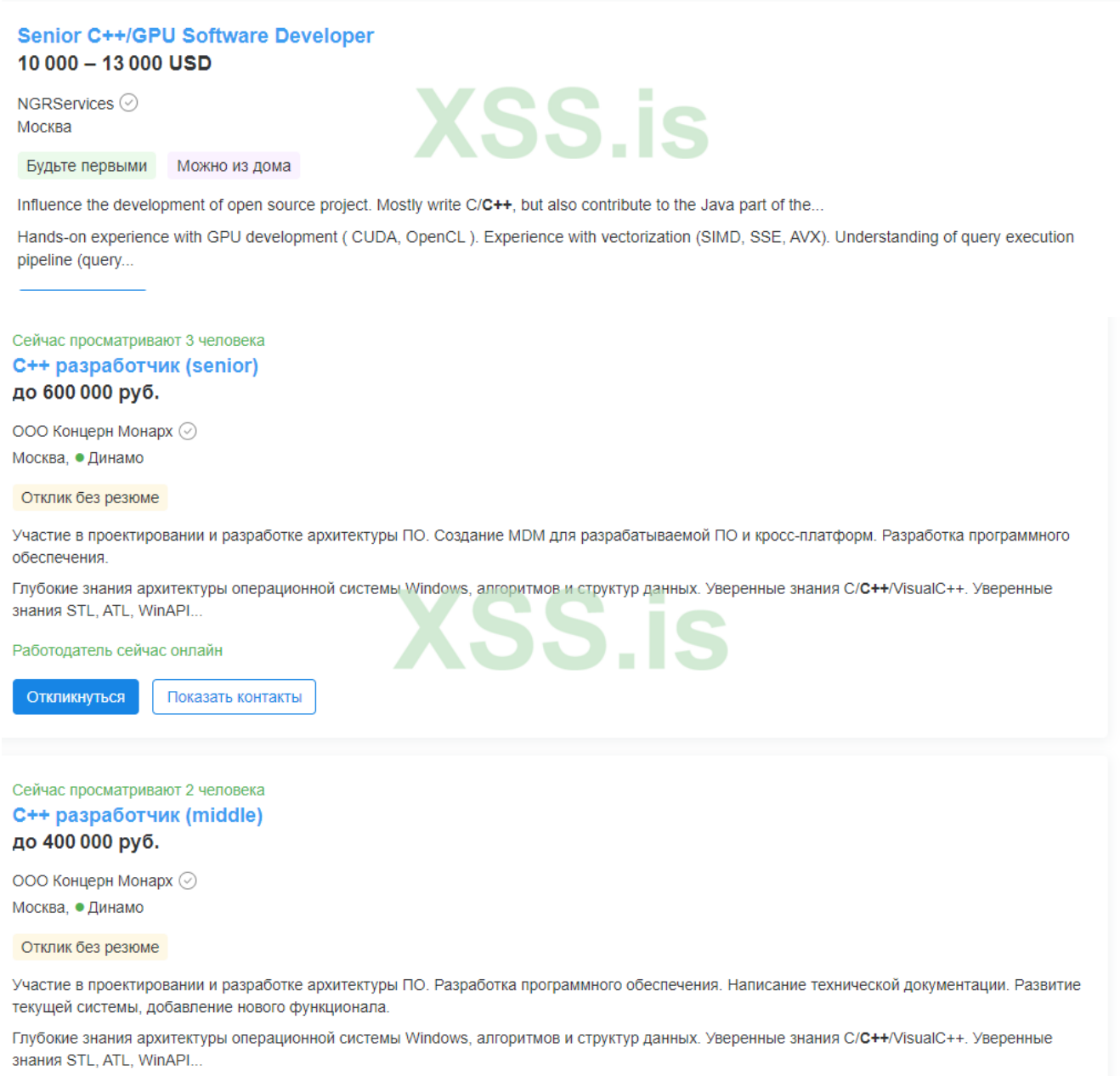
Итак, начнем. Малварь представляет собой обычную программу, выполняющую некоторые, заложенные программистом действия на компьютере. Например, скачать и запустить что-то, или найти все файлы по маске, открыть и пошифровать и так далее. Для простоты возьмём такой софт, как лоадер - он скачивает и запускает другие программы. На первый взгляд, написать такой софт (скачать и запустить) может абсолютно любой программист уже после 2-3х месяцев изучения матчасти, а уж на гитхабе такого кода полным-полно. Однако, цены на приватный лоадер стартуют от 10-15к и далее. Разумеется, речь идет о действительно качественном продукте для нормального, понимающего заказчика.

Откуда берётся эта цена, если основной функционал (скачать и запустить), как выяснилось выше, не может стоить таких денег? Цена эта берётся из двух факторов:
1. уникальные алгоритмы.
2. поддержка.

1. К сожалению для одних, и к счастью для других, в мире существует антивирусное ПО. Малварь, чтобы ее купил кто-то кроме далекого от темы новичка, должна минимально детектиться аверами. Понятно, что полного FUD не может быть, сейчас не 98 год и даже не 2008, но все же, к этому нужно стремится. Чем меньше аверов ловят малварь, тем выше ее цена. Однако, в антивирусных конторах тоже работают не дураки, там полно хороших спецов, знающих winapi , умеющих реверсить. Чтобы обойти все это дело нужна хорошая квалификация, такому за один месяц не научиться и в книжках этого не пишут.

Более того, обходы аверов это в некотором вроде извращат, ненормальное программирование. Такие методики обычно не нужны в "нормальном" программировании, поскольку их суть их в чем - запутать эмулятор, придумать что-то такое интересное, новое, необычное, то, что собьёт привычные средства обнаружения. Навскидку, вот пример http://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/threads/34637/ концепта. Понятно, что нельзя один раз сесть и изобрести метод, а потом годами его продавать - семплы попадают в аверлабы, где на все эти ухищрения пишутся новые правила детекта и так по кругу, пока наконец винда не загнётся.

Теперь возвращаемся к цене. Чтобы придумать такие моменты и закодить стабильный софт, нужна неплохая квалификация. Открываем hh.ru, первые попавшиеся объявления по языку C++:



Т.е. имея такие знания, человек может претендовать на белую работу. На которой ему не надо выдумывать все то, что описано выше. Он может делать все документировано, не беспокоиться об "обходах" и "детектах" (не просыпаться в 6 утра от смс "вставай_нас_палит_нод!"). Решать задачи без противодействия антивирусов , без извращений с поиском апи через одно место, шифрованием строк и прочими прелестями. Есть отпуск, больничные, нет постоянного стресса что найдут, поймают, и так далее. И при этом достойная зарплата - даже в Москве 2-3 штуки баксов вполне хватает для комфортной жизни с такси и ресторанами. Поэтому мне всегда смешно,

когда создают объявления с целью найти кодера под малварь за штуку-две да еще и с поддержкой. Адекватный специалист не напишет по такому объявлению! Потому что профессионал может и в белую заработать гораздо больше и без нервов, а блекушнику ваши копейки тем более не нужны. В лучшем случае пишут новички - людям надо где-то учиться, или же разные наркоманы и кидалы.

2. Даже супер-крутой софт мало чего стоит без постоянной поддержки и сопровождения его автором. Выходят новые версии софта, аверы анализируют малварь, так или иначе, надо постоянно что-то менять, обновлять, доделывать. Естественно, поддержка должна стоит денег, такая себе ежемесячная зарплата - никто не будет пожизненно поддерживать что-то там. Покупать софт без сопровождения кодером можно только в одном случае - если покупать с исходным кодом (и, естественно, если у вас есть свой программист). Иначе это пустая трата денег. Завтра кодер пропал, послезавтра обновился софт, и малварку можно хранить разве что для истории.

Депозит. Мы принудительно ставим все темы по продаже на депозит. Некоторые продавцы не соглашаются, мотивируя тем что "работают через гарант". Казалось бы да, оформил сделку через гаранта и норм. Но, как уже обсуждалось выше, для малвари крайне важна поддержка. Обновляются программы, обновляются базы аверов, и софт без поддержки за месяц-два-три (зависит от многих факторов) становится ничем не лучше паблика. Для примера, возьмём Azor , который был самым популярным стиллером в свое время, но очень быстро загнулся после пропажи автора. Сначала из-за большого количества детектов, но окончательно его добил апдейт хрома (80 версия), в котором поменяли алгоритмы шифрования. Поэтому, депозит - это какая-то гарантия, что продавец не забьет болт на поддержку сразу же после продажи софта.

Крипт. Кто-то считает, что крипт это панацея, неважно что софт палит даже виндеф, можно закриптовать да пойти работать дальше. Это не так. Запомните раз и навсегда - крипт спасает только от детектов в статике. Т.е. когда файл лежит на диске, или пересылается по почте, скачивается откуда-то.. Если же он запущен - все, в динамике убирать детекты должен создатель софта и никак иначе. По форумах ходят легенды о чудо-криптовальщиках, якобы убирающих детекты рантайма, но это очередная городская легенда. Не хочу сейчас погружаться в технические дебри, просто примите как факт - это сделать нельзя.

p.s. специально не хочу касаться холиварных тем про язык программирования, итак уже написали 50 страниц бреда.