Краткая теория защиты специфического программного обеспечения от детектирования антивирусами в вопросах и ответах «на пальцах»

1. ***>Сколько продержится FUD?***

   Один из самых тупых и надоедливых вопросов клиентов. Клиент даёт нам файл, мы его криптуем, убеждаемся на чекерах, что он ФУД; проверяем на Virtual Box, как правило на x64 Windows 7 и x86 Windows XP, что он работает (если встроена защита от VM – смотрим что крипт отрабатывает без проблем) и передаем закриптованный файл. Дальнейшие очевидные действия клиента – постановка на траф или обновление существующего ботнета. Причем на всем вашем трафе или ботнете будет находиться один и тот же файл – с одинаковой сигнатурой. Сигнатура, как правило, может быть выделена антивирусным программным обеспечением на многих этапах.
   Этапы возможного выделения сигнатур файла антивирусным ПО, по порядку использования:

   - Выделение сигнатуры на этапе использования не надёжной связки или при обновлении ботнета;
   - Непосредственно на целевой машине, при подозрениях с точки зрения эвристики и поведенческих аналализаторов, защищаемого софта;

   [Здесь не рассмотрена возможность анализа файлов загружаемых извне в чистом не зашифрованном виде на Облачном уровне корпоративными системами раннего обнаружения вирусной угрозы и подобными системами провайдеров]

   После обнаружения подозрений, файл, как правило передается в АВ – контору для исследований и его сигнатура добавляется в базу, после чего АВ – конторы иногда обмениваются между собой информацией или просто воруют друг у друга. Все файлы вашего ботнета с момента обновления базы становятся частично детектируемыми (PD), а со временем практически полностью детектируемыми (FD). Тем не менее, если использовался полиморфный криптор, данная проблема может быть решена как правило вовремя элементарным рекриптом без чистки.

   Рекомендации:

   - На этапе разработки применение модульности, обеспечивать максимальную скрытность основного модуля софта. Или при покупке софта – смотреть не только на его функционал но и на количество детектов и чем детектится новый билд, а так же на отсутствие специфики файла, например таких как оверлей; обращать особое внимание на «криптуемость» файла;
   - Передавать не закриптованные и закриптованные файлы только в архивах с не тривиальным паролем;
   - Использование обязательного динамического шифрования данных при обновлении ботнета;
   - Использование только «надёжных» связок при прогрузах, т.к. она сама по себе может «спалить» файлы;
   - Самое оптимальное, что может быть – использование встроенного в Админ – автоматического криптора, с возможностью криптования на лету, так что бы на каждой машине ботнета файл был с уникальной сигнатурой.

Криптование на высоком уровне:

JID: sysenter@jabber.com.ua

Продолжение следует….