АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Stantinko: масштабная adware-кампания, действующая с 2012 года

20 июля 2017 года

Рекламное ПО – не самый простой для анализа тип вредоносных программ. Обнаружив комплексную угрозу Stantinko, мы не сразу поняли, что это: рекламное ПО, вредоносная или шпионская программа. Потребовалось время, чтобы выявить ее цели и схемы, поскольку угроза оставляет не так много следов на зараженной машине. Разбираться в экосистеме Stantinko – примерно как собирать пазл.

Stantinko специализируется на рекламном мошенничестве, но выделяется на общем фоне технической сложностью. Шифрование кода и оперативная адаптация для защиты от обнаружения антивирусами позволили операторам Stantinko оставаться вне зоны видимости как минимум на протяжении пяти лет. Кроме того, внимание привлекает масштаб Stantinko – это одна из наиболее распространенных в России киберугроз, в составе ботнета около 500 000 устройств.

Обзор

Для заражения системы операторы Stantinko вводят в заблуждение пользователей, которые ищут пиратское ПО и загружают исполняемые файлы, иногда замаскированные под торренты. Далее FileTour, начальный вектор заражения, демонстративно устанавливает множество программ, чтобы отвлечь внимание пользователя от скрытой установки первой службы Stantinko в фоновом режиме. В видео 1 показано, как пользователь запускает вредоносный файл.exe.

ВИДЕО: https://youtu.be/OYncoW7X5wA
Видео 1. Пользователь загружает и запускает вредоносный файл

Операторы Stantinko управляют ботнетом и монетизируют его, в основном, путем установки вредоносных расширений браузера для несанкционированного внедрения рекламы и кликфрода. Проблема в том, что на этом они не останавливаются. Вредоносные службы позволяют исполнить на зараженной системе все, что угодно. Мы наблюдали отправку полнофункционального бэкдора, бота для массового поиска в Google, а также утилиты для брутфорс-атак на панели управления Joomla и WordPress (предназначена для взлома и возможной перепродажи).

На рисунке ниже представлена полная схема киберкампании Stantinko – от вектора заражения до постоянных сервисов и соответствующих плагинов.

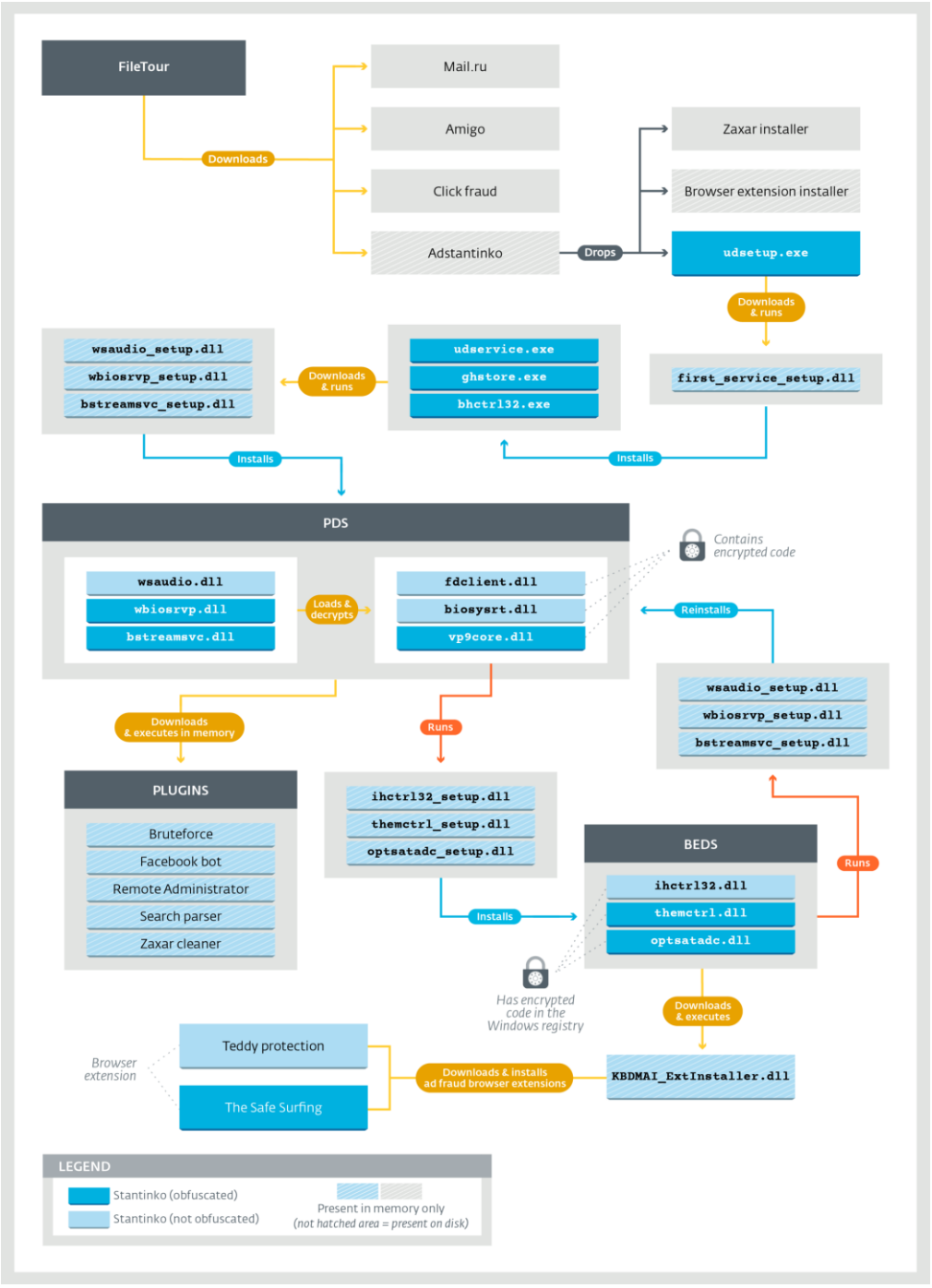

Рисунок 1. Полная схема угрозы Stantinko

Ключевые параметры

Характерная особенность Stantinko – обход обнаружения антивирусом и противодействие реверс-инжинирингу, определяющему вредоносное поведение. Для проведения всестороннего анализа угрозы необходимо несколько компонентов – загрузчик и зашифрованный компонент. Вредоносный код скрыт в зашифрованном компоненте, который находится либо на диске, либо в реестре Windows. Код загружается и расшифровывается безвредным на первый взгляд исполняемым файлом. Ключ генерируется для каждого из заражений. Некоторые компоненты используют идентификатор бота, другие – серийный номер тома жесткого диска ПК жертвы. Детектирование по незашифрованным компонентам – крайне сложная задача, поскольку артефакты, хранящиеся на диске, не показывают вредоносного поведения до выполнения.

Кроме того, в Stantinko предусмотрен механизм восстановления. После успешного заражения на машину жертвы с операционной системой Widnows устанавливаются две вредоносные службы, которые запускаются вместе с системой. Службы могут переустанавливать друг друга в случае удаления одной из них. Таким образом, чтобы успешно устранить угрозу, необходимо одновременно удалить две службы. Иначе C&C-сервер направит новую версию удаленной службы, которая еще не была обнаружена, либо содержит новую конфигурацию.

Основные функциональные возможности Stantinko – установка в зараженной системе вредоносных расширений браузера *The Safe Surfing* и *Teddy Protection*. На момент анализа оба расширения были доступны в Chrome Web Store. На первый взгляд, это легитимные браузерные расширения, блокирующие нежелательные URL-адреса. Но при установке в рамках схемы Stantinko расширения получают иную конфигурацию, содержащую правила кликфрода и несанкционированного показа рекламы. В видео 2 показан процесс установки расширения *The Safe Surfing*. Кликнув по ссылке, пользователь перенаправляется в поисковик Rambler.

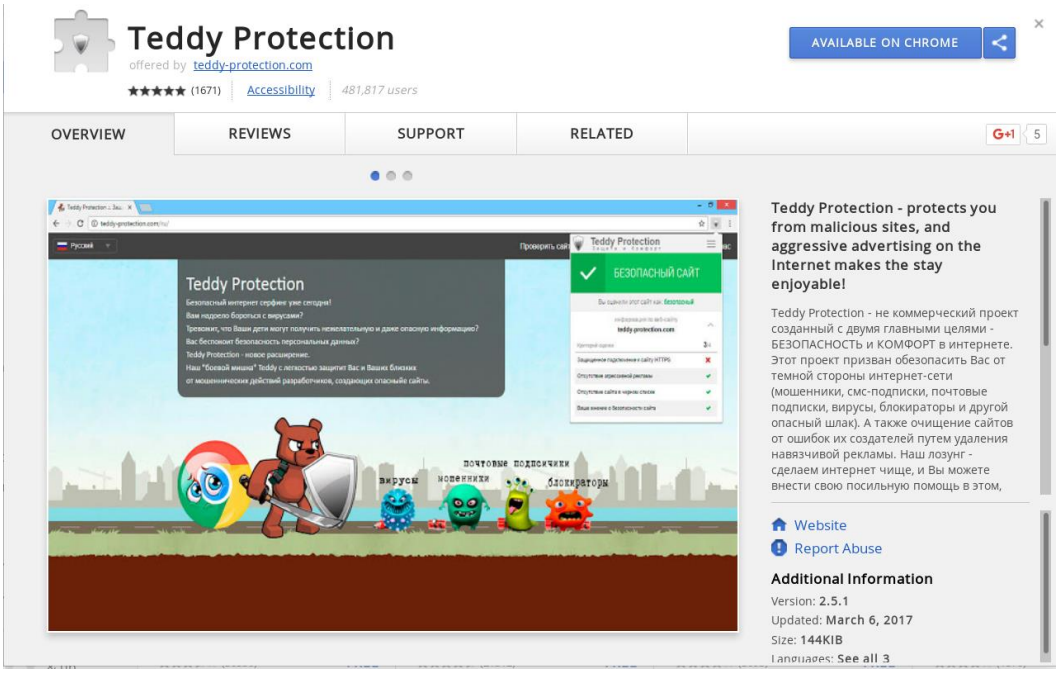

Рисунок 2. Teddy Protection в Chrome Web Store

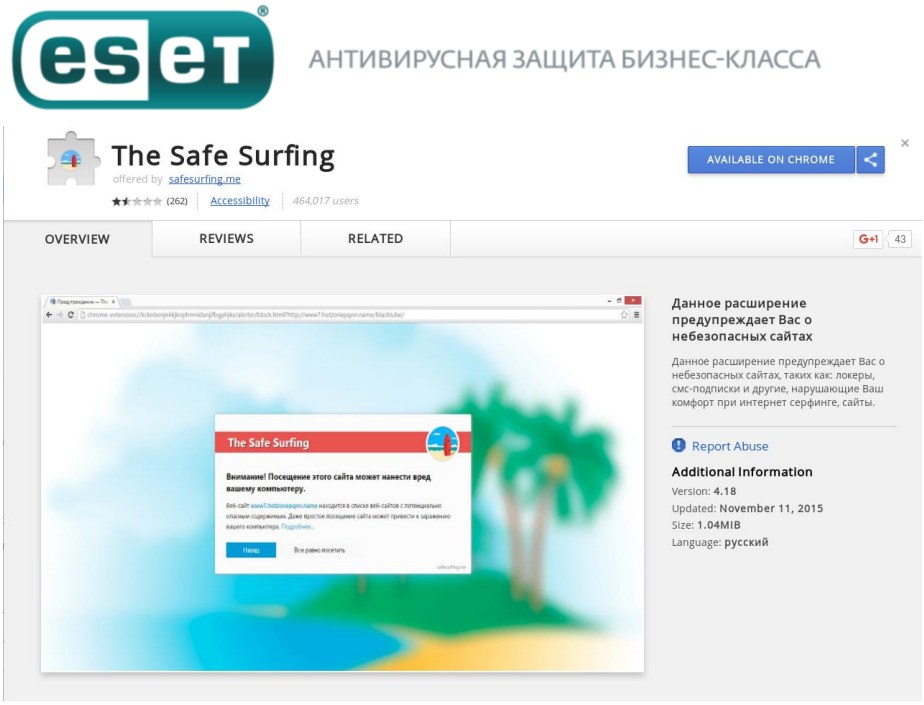

Рисунок 3. The Safe Surfing в Chrome Web Store

ВИДЕО: https://youtu.be/FirDn0O-PTY
Видео 2. Переадресация трафика на сайт Rambler

Stantinko – модульный бэкдор. Его компоненты включают загрузчик, позволяющий выполнять любой исполняемый Windows-файл, передаваемый C&C-сервером напрямую в память. Эта функция реализована в виде гибкой системы плагинов, которая позволяет операторам выполнить в зараженной системе все, что угодно. В таблице ниже приведено описание известных нам плагинов Stantinko.

Имя модуля	Анализ
Brute-force	Распределенная атака на панели управления Joomla и WordPress, используется метод перебора по словарю.
Search Parser	Выполняет массированный распределенный и анонимный поиск в Google с целью найти сайты на Joomla и WordPress. Использует взломанные сайты на Joomla в качестве серверов C&C.
Remote Administrator	Бэкдор, выполняющий полный спектр действий – от разведки до эксфильтрации данных.
Facebook Bot	Бот, выполняющий мошеннические действия на Facebook. В числе возможностей – создание аккаунтов, лайки под фото и страницами, добавление в друзья.

Монетизация

Разработчики Stantinko используют методы, которые чаще встречаются в APT-кампаниях. Тем не менее, их главная цель – деньги. Операторы предлагают свои услуги на самых доходных рынках компьютерных преступлений.

Во-первых, кликфрод сегодня является крупным источником доходов в экосистеме киберпреступников. Исследование, проведенное компанией White Ops и Национальной ассоциацией рекламодателей (США), оценило мировые издержки от кликфрода в 2017 году в 6,5 млрд долларов США.

Как уже описывалось выше, Stantinko устанавливает два расширения браузера – *The Safe Surfing* и *Teddy Protection*, которые показывают рекламу или осуществляют редирект. Это позволяет операторам Stantinko получать деньги за трафик, который они обеспечивают рекламодателям. На рисунке ниже показана схема переадресации.

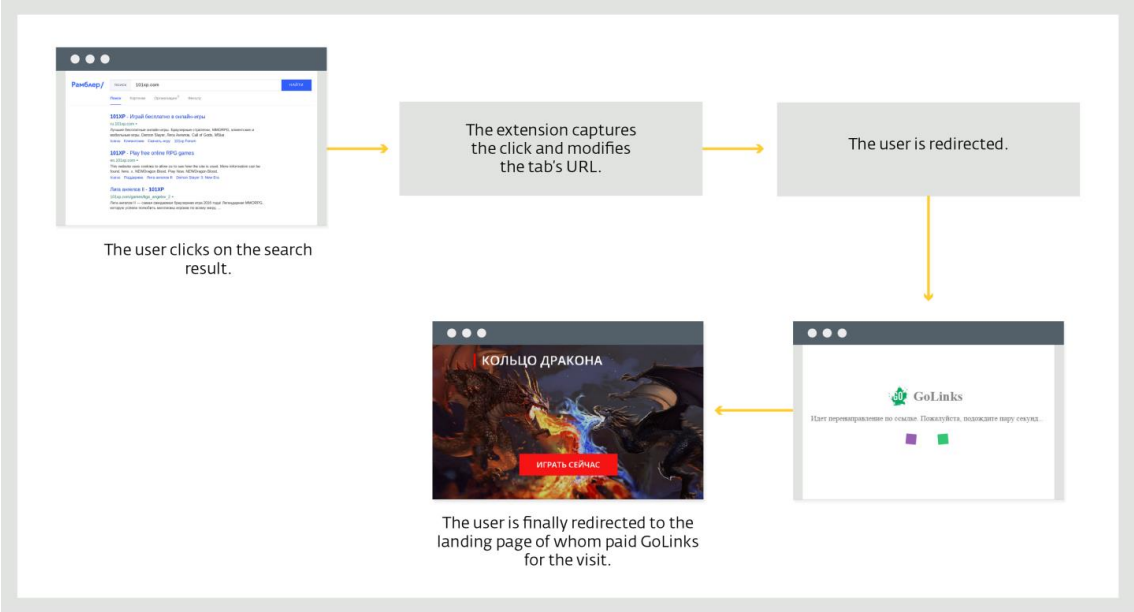

Рисунок 4. Кликфрод, процесс переадресации

Традиционные схемы кликфрода строятся на серии переадресаций между несколькими рекламными сетями, чтобы «отмыть» трафик. Но в случае со Stantinko операторы ближе к рекламодателям – в некоторых случаях (см. рисунок 4) пользователь попадает на сайт рекламодателя сразу из сети Stantinko. Это означает, что злоумышленники, стоящие за кампанией Stantinko, могут не только эффективно скрывать вредоносное ПО, но и нарушать традиционную рекламную экономику, и это сходит им с рук.

Во-вторых, операторы Stantinko пытаются получить доступ к панелям управления сайтов на Joomla и WordPress. Атака построена на брутфорсе с перебором логинов и паролей по списку. Цель – угадать пароль, испробовав десятки тысяч комбинаций. Взломанные аккаунты могут быть перепроданы и далее использоваться для переадресации посетителей сайтов на набор эксплойтов или для размещения вредоносного контента.

В-третьих, наше исследование раскрыло, как Stantinko работает в соцсетях. Мы уже описывали этот тип мошенничества в отчете по Linux/Moose. Схема действительно приносит прибыль – 1000 лайков на Facebook стоят около 15 долларов (даже если их генерируют фейковые аккаунты в составе ботнета).

Операторы Stantinko разработали плагин, взаимодействующий с Facebook. Помимо всего прочего, он может создавать аккаунты, ставить лайк на странице и добавлять друзей. Для обхода капчи в Facebook он использует специальный сервис (на рисунке 5). Масштаб сети Stantinko является преимуществом операторов, поскольку позволяет им распределять запросы между всеми ботами – это усложняет задачу Facebook по распознаванию мошенничества.

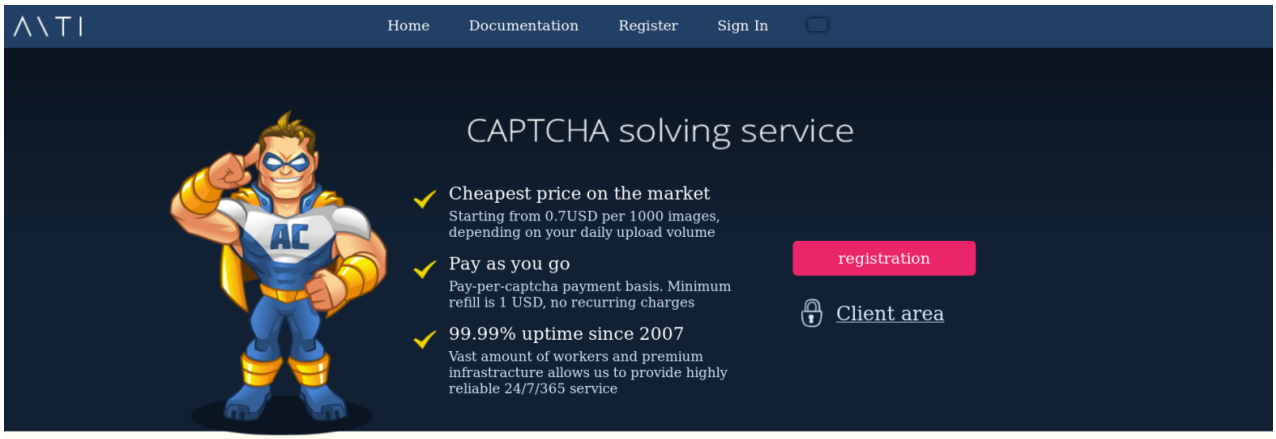

Рисунок 5. Сервис по обходу капчи, используемый Stantinko

Заключение

Stantinko – это ботнет, который специализируется на рекламном мошенничестве. Продвинутые технологии, включая шифрование кода и хранение кода в реестре Windows, позволяли операторам оставаться незамеченными на протяжении пяти лет.

Кроме того, операторам Stantinko удалось выложить в Chrome Web Store два расширения для браузера, которые выполняли несанкционированное размещение рекламы. Одно из них впервые появилось в Chrome Web Store в ноябре 2015 года.

Пользователь вряд ли заметит присутствие Stantinko в системе, поскольку угроза не перегружает ЦП. С другой стороны, Stantinko приносит убытки рекламодателям и значительный доход – операторам. Кроме того, присутствие полнофункционального бэкдора позволяет злоумышленникам следить за всеми зараженными машинами.

Основные выводы:

- Около 500 000 компьютеров скомпрометировано Stantinko
- Основные цели – Россия (46%) и Украина (33%)
- Операторы Stantinko монетизируют ботнет, устанавливая расширения браузера для несанкционированного показа рекламы
- Компоненты, остающиеся на диске, используют кастомный обфускатор кода, который усложняет процесс анализа угрозы
- В большинстве компонентов Stantinko вредоносный код скрыт внутри легитимного бесплатного ПО с открытым исходным кодом, которое было модифицировано и перекомпилировано
- Stantinko устанавливает несколько перманентных служб, которые могут восстанавливать друг друга, предотвращая удаление из системы
- Наиболее распространенное использование Stantinko – рекламное мошенничество. Тем не менее, его возможности значительно шире. Мы наблюдали отправку полнофункционального бэкдора для удаленного администрирования, бота для массового поиска в Google и утилиты для брутфорс-атак на панели управления Joomla и WordPress

Индикаторы заражения доступны в нашем аккаунте на GitHub. По любым вопросам, связанным с Stantinko, включая передачу образцов, пишите на threatintel@eset.com.