Асеев Евгений Алексеевич
Старший вирусный аналитик,
ЗАО «Лаборатория Касперского».

Небезопасный Интернет

Как происходит заражение компьютера при веб-серфинге? Каким образом злоумышленники наживаются на пользователях? На эти вопросы специалист «Лаборатории Касперского» попытается ответить в предлагаемой статье-предостережении.

Цель

В последние годы угроза веб-заражений стремительно растёт. Это обусловлено, с одной стороны, увеличением числа активных пользователей веб-ресурсов, а с другой – жаждой наживы у злоумышленников. На сегодняшний день атаки через Интернет лидируют как по количеству, так и по уровню опасности. Достаточно бегло пробежаться по ежемесячным рейтингам вредоносных программ, чтобы убедиться в этом: веб-атак огромное количество, они постоянно совершенствуются. Все наиболее сложные угрозы последнего времени – ZeuS, Sinowal, TDSS – распространяются именно через Интернет. Та же история с регулярно досаждающими пользователям фальшивыми антивирусами и программами-блокерами. Через веб была проведена нашумевшая целевая атака «Operation Aurora». И это только видимая часть киберпреступного айсберга.

Основной целью злоумышленника при атаке в Интернете является загрузка и установка на атакуемый компьютер вредоносного исполняемого файла. Безусловно, существуют такие атаки, как, например, XSS или CSRF, которые не подразумевают загрузки и инсталляции исполняемых файлов на атакуемые компьютеры. Но контроль изнутри над заражённой системой открывает злоумышленникам широкие возможности: при успешном исходе атаки они получают доступ к пользовательским данным и ресурсам системы. Это позволяет злоумышленникам так или иначе нажиться на пользователях.

Атака

В общем случае атака в вебе состоит из двух этапов: переход пользователя на вредоносный ресурс и загрузка на его компьютер вредоносного исполняемого файла.

Злоумышленники используют все возможные каналы для привлечения пользователей на вредоносные ре-

сурсы: электронную почту, системы мгновенного обмена сообщениями, социальные сети, поисковые системы, рекламу – проще говоря, вредоносные ссылки могут быть везде. Иногда злоумышленнику даже не приходится совершать специальных действий по привлечению пользователя, а достаточно лишь взломать легитимные[1] веб-сайты, которые имеют большое количество посетителей. Более того, в последнее время всё чаще злоумышленники используют именно этот метод.

Когда пользователь попал на «нехороший» ресурс, остаётся только загрузить и установить на его компьютер вредоносную программу. Здесь у злоумышленника есть два пути: вынудить пользователя сделать это самостоятельно или произвести скрытую drive-by-загрузку. В первом случае активно применяются методы социальной инженерии, то есть делается ставка на доверчивость и неопытность пользователя, во втором – эксплуатируется уязвимое программное обеспечение, установленное на его компьютере.

Атаку в Интернете, которая подразумевает загрузку и инсталляцию вредоносных файлов, можно представить в виде схемы.

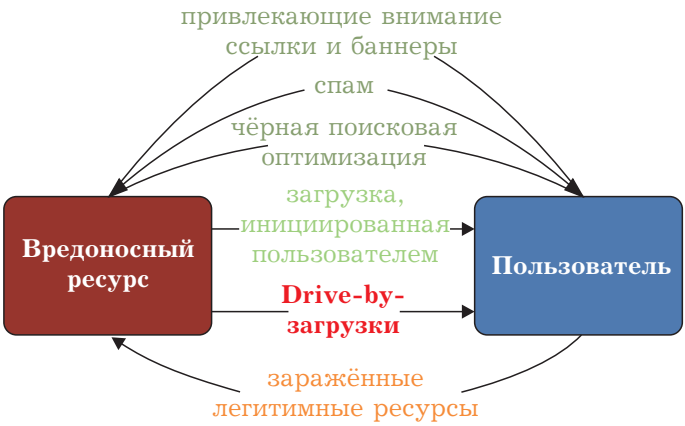

Рис. 1. Схема атаки в Интернете с использованием загрузки исполняемого вредоносного файла

Рассмотрим подробнее, как при повседневном пользовании Интернетом пользователь может попасть на «нехорошую» веб-страницу и заразить свой компьютер.

Спам

Один из наиболее популярных у злоумышленников способов заманивания пользователей на вредоносные страницы – это спам. Ещё несколько лет назад слово «спам» ассоциировалось только с рассылкой

[1] Легитимными называют сайты, которые не просто официально принадлежат какой-то организации, а являются настоящими, неподдельными. В противовес этому в сети встречаются поддельные сайты, внешним видом похожие на известные – скопирован дизайн, стиль и т. п., но в скрипте может находиться вредоносный код.

рекламных писем по электронной почте. Сейчас для распространения спама используется много других каналов: системы мгновенной передачи сообщений, социальные сети, блоги, форумы и даже SMS.

Зачастую спам несёт в себе вредоносный исполняемый файл или ссылку на вредоносный ресурс. Злоумышленники активно используют методы социальной инженерии для того, чтобы заставить пользователя пройти по ссылке и/или загрузить и установить вредоносный файл: начиняют сообщения ссылками якобы на горячие новости, маскируются под популярные интернет-ресурсы и компании. В общем, играют на человеческих слабостях: страхе, любопытстве, азарте. Подробно останавливаться на этом не будем, так как большое количество примеров распространения вредоносных программ таким способом опубликовано у нас на сайте.

Привлекающие внимание ссылки и баннеры

Еще одним актуальным способом привлечения пользователей на вредоносные ресурсы является баннерная реклама и многообещающие ссылки. Как правило, такие методы актуальны для веб-сайтов нелегальной направленности, распространяющих нелицензионное программное обеспечение или другой нежелательный контент.

Рассмотрим пример такой атаки. Задав в строке поиска в Google довольно популярный в мае 2010 года запрос «скачать кряк для Assassin's creed 2», в числе других результатов вы получите адрес некой веб-страницы, при загрузке которой появляется плавающий баннер, рекламирующий ресурс «Forex-Bazar».

Рис. 2. Плавающий баннер на веб-сайте, распространяющем нелицензионное ПО

При попытке закрыть баннер открывается новое окно браузера с веб-сайтом, предлагающим просмотреть видеоролики. При нажатии мышкой на preview-изображение любого видео появляется сообщение о том, что для его просмотра необходимо установить обновление для Adobe Flash Player.

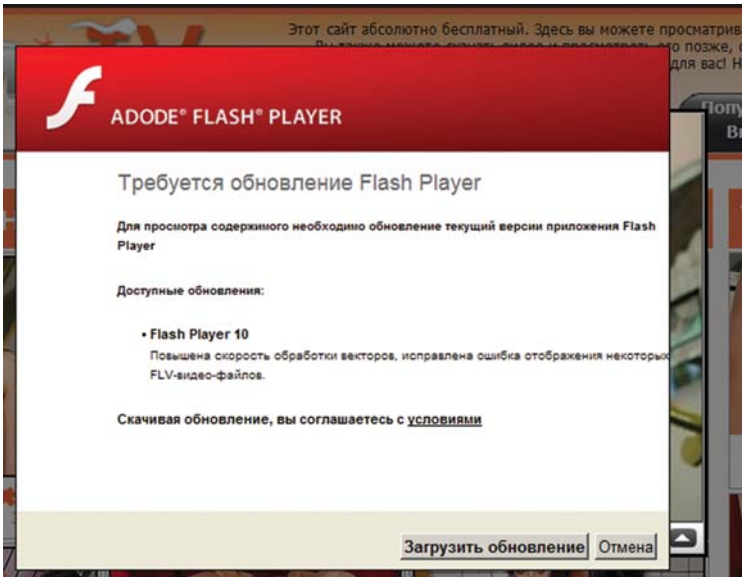

Рис. 3. Сообщение, появляющееся на веб-сайте при попытке просмотреть видеоролик. Программа похожа на настоящую, но является подделкой – обратите внимание на название «ADODE...»

Вы нажимаете на кнопку «Загрузить обновление», затем – «Установить обновление», после чего на ваш компьютер устанавливается одна из последних версий Trojan-Ransom.Win32.XBlocker – и никаких обновлений. Эта программа поверх всех остальных окон открывает окно с предложением отправить платное SMS-сообщение. Пока пользователь этого не сделает и не получит код, чтобы «немедленно деинсталлировать модуль», окно будет продолжать ему надоедать.

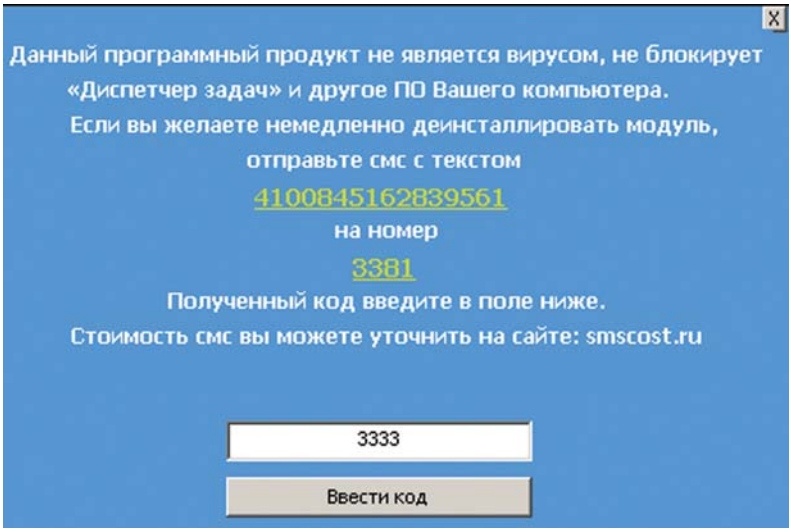

Рис. 4. Окно, появляющееся на экране после установки Trojan-Ransom.Win32.XBlocker

Чёрная поисковая оптимизация

SEO (Search Engine Optimization) – это комплекс мер для поднятия позиций сайта в результатах выдачи поисковых систем по определённым запросам пользователей. В современном информационном мире поисковые системы представляют собой основное средство для получения нужной информации, поэтому чем легче найти тот или иной веб-сайт, тем более востребована будет предлагаемая на нём услуга.

Методов оптимизации существует множество – как разрешённых, легальных, так и запрещённых поисковыми системами. Для нас больший интерес представляют запрещённые методы чёрной оптимизации, которые активно используются злоумышленниками для продвижения вредоносных ресурсов.

Опишем в общем виде, как пользователи попадают на «раскрученные» ресурсы и что для этого делают злоумышленники.

Используя ключевые слова, заданные вручную или полученные автоматически (например, с помощью Google Trends), злоумышленники создают веб-страницы с релевантным (соответствующим поисковым запросам) содержимым. Обычно это осуществляется автоматически: роботы делают запрос к поисковым системам и воруют контент (например, фрагменты текста) со страниц, попавших в топ по результатам поиска.

Далее злоумышленник вручную, с помощью специальных утилит, заставляет поискового робота индексировать веб-страницу. Для этого ссылка на страницу может быть распространена на ресурсах, уже известных поисковым системам, – на различных форумах, в блогах или в социальных сетях. Ссылки на целевую страницу с таких веб-сайтов будут прибавлять ей вес, страница попадёт в верхушку списка выводимых поисковыми системами результатов.

На сформированной веб-странице помещается скрипт, который с помощью обработки HTTP-заголовков может идентифицировать посетителя. Если это робот – то ему будет «показана» страница с содержимым, соответствующая определённым ключевым словам. Как следствие, эта страница будет продвинута вверх в списке выдаваемых пользователю результатов. Если же это пользователь, который нашёл страницу с помощью поисковой системы, то он будет перенаправлен на вредоносный сайт.

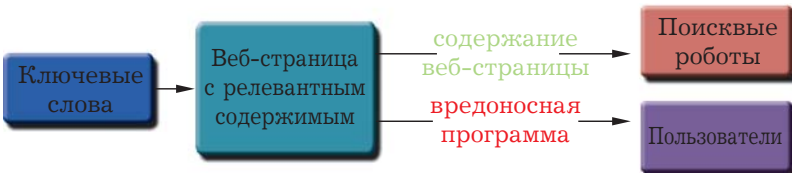

Рис. 5. Схема формирования и отображения данных в процессе чёрной поисковой оптимизации

Веб-сайты, продвинутые «нехорошими» методами, оперативно удаляются поисковыми системами из результатов поиска. Поэтому для их создания и продвижения злоумышленники, как правило, используют автоматизированные средства, которые позволяют ускорить процесс и приумножить количество новых вредоносных веб-ресурсов.

Автоматически сформированные веб-страницы могут располагаться

где угодно: на ресурсах злоумышленников, на заражённых легитимных ресурсах, на бесплатных хостингах или платформах для блогов.

Описанные выше варианты заражения могут произойти только в случае согласия пользователя на загрузку программы. Чаще всего такое поведение обусловлено неопытностью или невнимательностью. Не последнюю роль играют и человеческие слабости. К примеру, окно, информирующее о том, что компьютер заражён, вызывает страх, и неопытный пользователь стремится побыстрее нажать на кнопку «Удалить все угрозы». А окно с предложением скачать «обновление для Adobe Flash Player» или «недостающий кодек» у него не вызывает подозрений – тем более, что оно очень похоже на оригинальное, и прежде пользователю не раз случалось нажимать кнопку «Скачать» в случае реальных обновлений.

Заражённые легитимные ресурсы

Всё большую популярность набирает ещё один способ распространения вредоносных программ – скрытые drive-by-загрузки. В ходе drive-by-атак заражение компьютера происходит незаметно для пользователя и не требует его участия. Подавляющая часть drive-by-атак происходит с помощью заражённых легитимных ресурсов.

Заражение легитимных ресурсов – пожалуй, одна из наиболее серьёзных и актуальных проблем в Интернете на сегодняшний день. Новостные ресурсы пестрят заголовками вроде «Mass hack plants malware on thousands of webpages», «WordPress Security Issues Lead To Mass Hacking. Is Your Blog Next?» и «Lenovo Support Website Infects Visitors with Trojan». Ежедневно «Лаборатория Касперского» регистрирует тысячи заражённых ресурсов, с которых без ведома пользователя загружается вредоносный код. Такие атаки называются drive-by-атаками.

В drive-by-атаках, как правило, не стоит вопрос привлечения пользователя на вредоносную страницу – он приходит на неё сам в процессе серфинга. К примеру, веб-сайт, на который пользователь ежедневно заходит, чтобы прочитать новости или заказать какой-то товар, может подвергнуться заражению.

Заражение ресурса происходит обычно двумя способами: через уязвимости на целевом ресурсе (например, внедрение SQL-кода) и с помощью похищенных ранее конфиденциальных данных для доступа к веб-сайту. Самое простое заражение представляет собой скрытый тэг iframe, дописанный в исходную страницу. В тэге iframe содержится ссылка на вредоносный ресурс, куда пользователь автоматически перенаправляется при посещении заражённого веб-сайта.

На вредоносном ресурсе находится эксплойт[1] или набор эксплойтов, которые при наличии у пользователя уязвимого программного обеспечения успешно срабатывают, и происходит загрузка и запуск исполняемого вредоносного файла.

Общая схема атаки представлена на рисунке ниже (источник: Google).

[1] Эксплойт – фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.

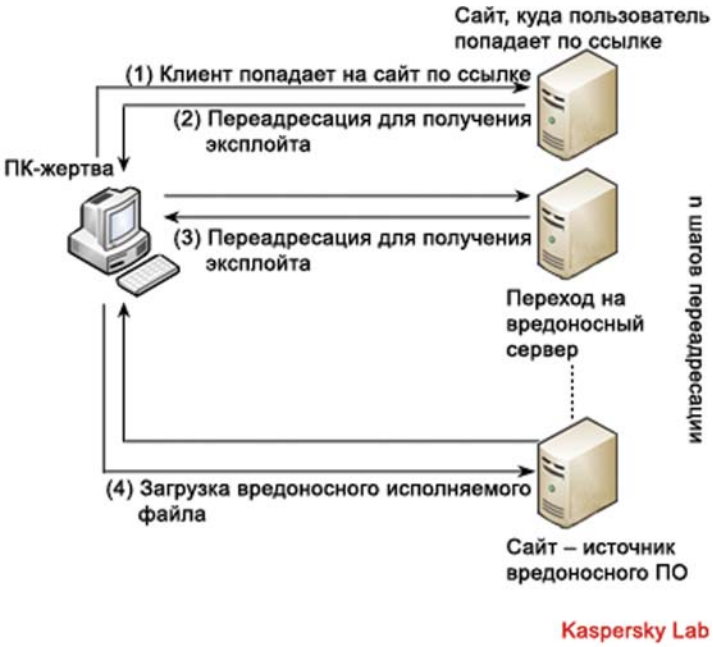

Рис. 6. Общая схема drive-by-атаки

Наборы эксплойтов

Рассмотрим подробнее один из наиболее распространённых сегодня методов drive-by-атак – с использованием набора эксплойтов. Набор эксплойтов – это совокупность программ, эксплуатирующих уязвимости в легитимном ПО на стороне пользователя. Проще говоря, эксплойты открывают чёрный ход, через который вредоносные программы попадают на компьютер. Учитывая, что атаки в вебе происходят через браузер, злоумышленнику необходимо использовать уязвимости либо в браузере, либо в дополнительных модулях к браузеру, либо в стороннем ПО, которое загружается браузером для обработки контента. Конечной целью работы набора эксплойтов является незаметная для пользователя загрузка и запуск на его компьютере исполняемого вредоносного файла.

Наборы эксплойтов плотно заняли свою нишу на рынке киберпреступных услуг. На сегодняшний день на чёрном интернет-рынке продаётся множество таких наборов, которые отличаются ценой, количеством включённых эксплойтов, удобством административного интерфейса, а также качеством предоставляемого сервиса по обслуживанию. Помимо готовых наборов эксплойтов, которые имеются в продаже, есть такие, которые создаются на заказ и используются отдельными киберпреступными группировками.

Среди сделанных на заказ наиболее распространёнными являются наборы эксплойтов, используемые в атаках популярных скриптовых загрузчиков Gumblar и Pegel.

Особенность последней версии Gumblar – это автоматизированный процесс заражения веб-сайтов и компьютеров пользователей, при котором все инструменты атаки – и эксплойты, и исполняемый файл –

располагаются на взломанных легитимных ресурсах. При посещении одного заражённого веб-сайта пользователь перенаправляется на другой заражённый веб-сайт, с которого и происходит заражение.

В атаке Gumblar эксплуатируются уже известные уязвимости в Internet Explorer, Adobe Acrobat/Reader, Adobe Flash Player и Java.

Стоит вспомнить также очень интересного с технологической точки зрения загрузчика Twetti, который формирует несколько запросов к API социальной сети Twitter. Из полученных данных генерируется псевдослучайное имя домена, на который пересылается пользователь. Злоумышленники заранее по аналогичному алгоритму получают имя домена, регистрируют его и размещают на сайте вредоносные объекты для загрузки на компьютеры пользователей.

Деньги

Кто же и как наживается на описанных атаках?

Атака с использованием рекламного баннера выгодна владельцам веб-ресурсов, на которых размещается баннер, – они получают деньги за его размещение. На успешной загрузке и инсталляции XBlocker зарабатывают авторы вредоносной программы – в том случае, если пользователь отправит SMS на платный номер. А неопытные пользователи, как правило, отправляют.

На чёрной оптимизации и атаках с использованием раскрученных таким способом сайтов наживаются те, кто реализовал схему распространения, кто разработал программные средства для автоматизации создания поддельных веб-сайтов, кто связал все части схемы воедино. При успешной загрузке и инсталляции фальшивых антивирусов в прибыли оказываются те, кто организовал атаку. А неопытные пользователи, как правило, соглашаются на установку и платят за «антивирус». Зарабатывают на этом и разработчики самих фальшивых антивирусов.

На drive-by-атаках наживаются разработчики наборов эксплойтов и те, кто пользуются этими наборами. Например, схема «Набор эксплойтов + ZeuS Toolkit» эффективно работает для получения конфиденциальных данных пользователей, которые затем можно продать на чёрном рынке. А в результате регулярных атак Pegel злоумышленникам удалось создать бот-сеть из заражённых Backdoor.Win32.Bredolab компьютеров, используя которую, они могут загружать на заражённые компьютеры другие вредоносные программы.

Выходит так, что зарабатывают даже собственно на загрузках вредоносного ПО? Конечно, зарабатывают. Организуется такой заработок с помощью партнёрских программ (партнёрок), или PPI-схем (Pay-Per-Install).

Партнёрки

Партнёрки появились довольно давно и изначально использовались в основном для распространения рекламных программ, «склеенных» с бесплатными приложениями: пользователь вместе с интересующей его программой в виде «бонуса» получал программу, которая показывала рекламу. Теперь такие схемы активно используются для распространения вредоносных программ.

Чёрная PPI-модель включает в себя следующих действующих лиц (партнёров).

- Заказчики – это киберпреступники, которые обладают опре-

делёнными денежными ресурсами и вредоносной программой, которую им необходимо распространить.

- Исполнители – это люди, которые берутся распространять эту программу и получают за это деньги. Часто случается так, что партнёр не интересуется тем, что именно ему предстоит распространять, и становится пособником киберпреступников, не подозревая об этом (что не умаляет, конечно, его вины).
- PPI-ресурс – это организация, которая связывает заказчиков и исполнителей и получает процент от их сделки.

Рис. 8. Схема работы чёрной PPI-модели

Помимо партнёрских программ, в которых, по сути, может участвовать любой, существует ещё множество «закрытых» партнёрок, куда допускаются только крупные игроки киберпреступного бизнеса, например, владельцы ботнетов[1]. Можно лишь предполагать, какие деньги крутятся при таком сотрудничестве.

Остался один вопрос – кто является источником дохода злоумышленников? Ответ здесь однозначен и очевиден – пользователи. Это их личные деньги, их конфиденциальные данные или вычислительные мощности их компьютеров.

Выводы

Современный Интернет небезопасен: достаточно пройти по ссылке из результатов поисковой системы или зайти на любимый сайт, который незадолго до этого был заражён, чтобы превратить свой компьютер в зомби-машину. Главная цель злоумышленников – это деньги пользователей или конфиденциальные данные, которые, в конечном счёте, дают злоумышленникам возможность обналичить (разными способами) те же деньги. Поэтому киберпреступники используют все имеющиеся в их арсенале методы, чтобы доставить вредоносную программу на компьютер пользователя.

Чувствовать себя безопасно можно лишь при постоянном обновлении активно используемого программного обеспечения, в особенности того, которое работает в связке с интернет-браузером. Важно, чтобы на компьютере было установлено современное комплексное решение по безопасности с базами, поддерживаемыми в актуальном состоянии. А в целом следует быть максимально бдительным по отношению к внешней информации, получаемой из Сети.

[1] Ботнет (ботсеть) – заражённые компьютеры, логически объединённые в сеть с помощью центра управления, позволяющего злоумышленнику централизованно управлять ими и использовать их по собственному усмотрению.