Визитка

ВЛАДИМИР БЕЗМАЛЫЙ, Microsoft Security Trusted Advisor, Certificate Trainer Kaspersky Lab, Consultant UN (Information Security), автор серии книг «Цифровая гигиена», cybercop@outlook.com

Покупаем технику
А думать?

В статье пойдет речь о том, как сделать приобретение новой техники максимально безопасным процессом. Рассматриваются некоторые практические приемы, по которым чужеродное ПО может быть подброшено на компьютер или смартфон пользователя. И, конечно, приводятся рекомендации, как избежать перечисленных неприятностей.

Увы, время идет гораздо быстрее чем хотелось бы. Соответственно время от времени всем нам приходится обновлять технический парк. Как компьютеров, так и мобильных телефонов. Но кто и когда задумывается какие неприятности при этом нас могут подстерегать?

В данной статье мы рассмотрим несколько возможных ситуаций. И дело вовсе не в том, что вы платите за одну комплектность, а получаете другую. Это самый простой и легко проверяемый вариант.

Вначале я хотел бы задать вопрос, который вполне может вызвать ваше недоумение.

Вы доверяете вашему партнеру? Имею в виду вашей жене (любовнице, невесте)? Странный вопрос, не правда ли? Доверите ли вы ему (ей) PIN-код вашего смартфона? Сомневаюсь, ведь у каждого из нас есть свои скелеты в шкафу.

Ну а если вам к празднику или просто чтобы создать вам праздник дарят новый смартфон. Вы довольны? Думаю, что да. И что вы сделаете? Начнете устанавливать приложения, быстренько перенесете туда вашу телефонную книгу. Сделаете это сами либо с помощью вашего друга, который разбирается в этом куда лучше вас самого, верно?

А теперь посмотрим на это глазами специалиста по безопасности.

Итак, представьте себе, вы – простой пользователь. Ну хорошо, не вы, а супруга, сестра, мама Вашего директора. Я согласен, что простой пользователь не читает этот журнал.

И вот такой пользователь приходит в магазин купить себе ноутбук (смартфон). И вроде бы знает, что именно хотел бы купить. Но в магазине менеджер начинает морочить голову дополнительными услугами. Мол, мы вам все настроим, наши специалисты установят приложения, дадут вам дополнительно на некоторое время неограниченный доступ в интернет (да-да, такое бывает). Что же получает покупатель, причем за свои же деньги?

Как правило, неизвестно какими средствами полученную ОС. Далеко не всегда продавец имеет право на продажу того или иного ПО. Например, далеко не все компании имеют право предустанавливать OEM версии Windows. Еще может быть какой-то пакет офиса. Чаще всего пиратский. Но за это сдерут деньги, могут еще добавить бесплатную или триал-версию антивируса. Это, так сказать «базовый» набор.

Проблемы, начнутся, если вдруг правоохранительные органы решат проверить легальность установленного ПО. При это такая скрытая «мина замедленного действия» может годами ожидать, когда кто-то решит проверить на легальность. Но, как любая мина, она может взорваться и принести существенный вред, а может и не принести такого уж вреда. Или быть успешно нейтрализована, например, при установке корпоративного ПО, купленного в рамках корпоративной лицензии. Или при переходе на Linux и другое бесплатное ПО для корпоративного использования.

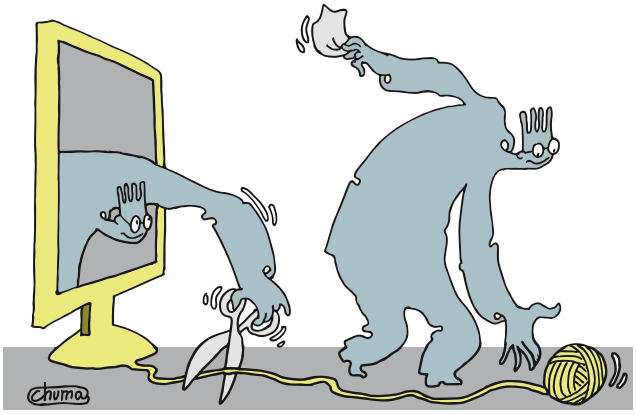
Но гораздо веселее, если установят на ноутбук (планшет) или смартфон так называемое stalkerware. Формально данное ПО не вредоносное. Но, увы, только формально. Давайте подробнее разберемся что ж это такое?

Stalkerware

Данный класс приложений позволяет контролировать телефоны партнеров и отслеживать их местоположение без их ведома. Стоит отметить, что до недавнего времени такие приложения не считались вредоносными и, соответственно, не отслеживались антивирусами. С недавнего времени Kaspersky выделяет их в отдельный вид вредоносного ПО.

Сегодня stalkerware называется «шпионским программным обеспечением для наблюдения за потребителями» или «spousware». Данное ПО позволяет удаленно контролировать активность устройства. То есть не только местоположение, а и читать тексты, просматривать фотографии, получать доступ к GPS-координатам устройства. Так, например, делает приложение под названием PhoneSheriff [1].

По сообщению [2] в прошлом году тысячи людей стали жертвами PhoneSheriff. Анализ файлов бывшего производителя данного ПО, компании Retina-X, показал, что данный продукт использовали чаще обычные люди, а не сотрудники правоохранительных органов. Однако, если вы считаете, что это приложение уникально, вы ошибаетесь. На самом деле их десятки, если не сотни. Это такие приложения как Mobistealth [3], Family Orbit [4], FlexiSPY [5].



Некоторые программы даже удаляют следы своего присутствия на телефоне...

Последнее – одно из наиболее популярных. Сегодня это приложение умеет отправлять поддельные текстовые сообщения, похищать пароли приложений, просматривать и отправлять фотографии, следить за историей веб-поиска, за чатами в Facebook, iMessage и WhatsApp и отслеживать поведение в Tinder.

Сегодня неизвестно сколько народу стало жертвами такого ПО. Однако согласно данным таких организаций, как Национальный центр по борьбе с бытовым и сексуальным насилием [6], наблюдение со стороны партнера является реальностью для многих, кто сообщает о жестоком обращении, и само по себе является серьезной формой жестокого обращения. В 2014 году британская сеть поддержки Refuge сообщила о почти 1000 случаев [7], когда жертвы нуждались в помощи, потому что боялись, что за ними следят с помощью их личных устройств или технологий «умного дома», таких как веб-камеры и термостаты.

Однако после изучения возможностей коммерческих приложений шпионов становится ясно, что различий между коммерческом ПО для слежки (большинством защитных решений оно детектируется как «not-a-virus») и классическим шпионским ПО [8] очень мало.

Так пользовательское ПО для слежки работает:

- Командный сервер (C&C) предоставляется владельцами сервиса;
- Ее легче купить и развернуть, чем классическое шпионское ПО. Нет необходимости посещать сомнительные хакерские форумы и иметь навыки программирования; практически по всех случаях достаточно установить программу вручную.

В большинстве стран коммерческие программы-шпионы не единожды становились объектом публичного обсуждения [9] и критики [10], однако статус его в большинстве стран мира до сих пор не определен.

Возможности этих программ позволяют им без ведома пользователя нарушать его конфиденциальность – иконку приложения можно скрыть в меню приложений, пока программа работает в фоновом режиме, при этом некоторые функции приложения выполняют слежку (например, записывают голос жертвы). Некоторые программы даже удаляют следы своего присутствия на телефоне, а также удаляют установленные защитные решения после того, как атакующая сторона предоставляет приложению root-права.

Продукты «Лаборатории Касперского» детектируют такие программы с вердиктом «not-a-virus:Monitor.*».

Кто-то может возразить, мол, это же персональные шпионы, причем тут корпоративный журнал, да еще и для системных администраторов?

Причина очень проста. Вернее, их две.

1. Кто настраивает корпоративные смартфоны? Да и будем откровенны, кто настраивает руководству и не корпоративные телефоны? Отдел ИТ. А если это небольшая организация, к кому директор отправится настраивать свой смартфон, впрочем, и домашний ноутбук тоже? К системному администратору!
2. Шантаж, увы, до сих пор остается весьма действенным инструментом социальной инженерии.

Ну и как вы думаете? Шантажировать ваше руководство не будут? А? Причем не только конкуренты, а и обманутые супруги (обманутые не супруги)? Или обиженные дети?

А как вы думаете, кого первым будут допрашивать? Задумывайтесь, пока такое будущее еще не наступило.

Методы распространения stalkerware

На самом деле способов заразиться всего два:

1. Фишинговая атака
2. Физический доступ к устройству

В первом случае злоумышленник отправляет вам по электронной почте замаскированную ссылку, которая установит вредоносное ПО к вам на смартфон (компьютер).

Во втором – нужен физический доступ. В частности, доброжелательный продавец, который окажет вам дополнительные услуги по настройке вашего телефона, вено? Кроме того, возможной жертве могут подарить (купить) телефон и установить приложение до передачи устройства жертве.

Существует очень небольшая вероятность, что коммерческие программы с внедренным «шпионом» попадают в App

Store. Гораздо хуже дела обстоят с Google Play. Но стоит помнить, что страницы таких программ со ссылками на скачивание можно без проблем найти в интернете. Естественно, эти программы вынуждают пользователей разрешить установку приложений из сторонних источников, вне официального магазина Google Play, что зачастую подвергает устройства риску. Это разрешение делает Android-устройство уязвимым к вредоносным программам и нарушает политики безопасности Google.

В первую очередь коммерческие приложения-шпионы распространяются через установку вручную, поскольку после установки злоумышленник должен зарегистрировать устройство, введя данные лицензии. После этого быстрого процесса конфигурации программа готова к шпионажу за пользователем, а ее присутствие на устройстве скрыто. Так обстоят дела, например, с программой Mobile Tracker Free [11].

Некоторые программы принимают дополнительные меры к тому, чтобы предотвратить возможность обнаружения со стороны пользователя, например, маскируются под системное приложение в списке установленных приложений:

Такое маскирующееся поведение типично для многих Android-угроз. В отдельных случаях приложения-шпионы скрывают все следы своей деятельности. После установки они удаляют инсталляционный файл и подчищают историю браузера, удаляя в ней веб-страницы, связанные с распространением программы.

Однако если вы простой домашний пользователь, то это плохо, но не страшно. Гораздо интереснее, если вы руководитель в какой-то компании. Вот здесь нужно быть предельно внимательным.

И вариантов может быть тоже несколько:

1. Ваши сотрудники (партнеры) решили подарить вам смартфон на праздник.
2. Вы решили сами себе купить новый смартфон
3. Вы решили обновить мобильную технику для руководящего состава компании

Рассмотрим все три варианта.

Сотрудники (партнеры) решили подарить смартфон на праздник

Откровенно? Самый простой вариант. Лучше сразу вернуть подарок в магазин, но при этом купить себе смартфон той же модели и того же цвета, чтобы не обижать дарившего своим недоверием. А вдруг подозрения напрасны и люди от всего сердца подарили «чистый» смартфон? В идеале будет лучше всего, если это сделает доверенное лицо, в другом городе и за наличные, ведь они оставляют меньше следов в виде записей об информации по карте, при передаче реквизитов и так далее. Разумеется, при этом не нужно сообщать никаких данных, не нужно оформлять скидочных карт, заполнять каких-либо анкет и т.д., то есть покупка должна быть за наличные именно в салоне, без заполнения скидочных анкет и без использования карты покупателя.}

Вы решили сами себе купить новый смартфон

В принципе действия практически те же. Вы заказываете его себе в магазине, но настраиваете его сами. Естественно, PIN-код себе вы настраиваете сами. Не забывайте, что PIN-код от вашего смартфона – это ваша и только ваша тайна.

Вы решили обновить мобильные телефоны руководства компании.

Этот вариант, наверное, встречается наиболее часто. В этом случае смартфоны в первую очередь попадают в отдел ИТ, вернее в службу технической поддержки, в которой и осуществляется собственно настройка.

И вот здесь начинается целый ряд вопросов, на которые очень часто нет ответа:

1. Существует ли у вас список разрешенного к установке программного обеспечения?
2. Прописаны ли настройки соответствующего ПО?
3. Когда в последний раз проверялась защищенность смартфона при соответствующих настройках?
4. И самое главное – НА СКОЛЬКО ВЫ ДОВЕРЯЕТЕ ТЕМ, КТО ПРОИЗВОДИТ НАСТРОЙКУ???

Если не доверяете, а зачем же копании платить зарплату этим специалистам? Если такие «недоверенные лица» работают в компании – необходимо уволить таких «специалистов» немедленно, не взирая на стаж, заслуги и родственные связи! Не забудьте о необходимости сброса корпоративных смартфонов сразу после того, как уволится соответствующий специалист, проводивший настройку. Учтите, сброс в заводские настройки проводится владельцем смартфона в присутствии специалиста отдела ИБ. Или специалистом ИТ, но тоже в присутствии ИБ.

Почему так? Да просто чтобы никто не смог потом обвинить в утечке информации, например, со смартфона руководителя, и последующих махинациях при помощи этих данных.

Странные правила? Наверное. Но все же лучше пусть будут обвинять в странных правилах, чем потом допрашивать в прокуратуре.

А вы как думаете?

Ох уж эти флешки!

Представим себе ситуацию, Вы покупаете смартфон, и Вам продавец предлагает всего-то за ничего, а то и бесплатно, в виде бонуса, MicroSD карту, полную музыки, фильмов, книг (всевозможные акции вроде «Библиотека в кармане»). А что – приятно! Чем качать или оформлять подписку на известные сервисы – все сразу в комплекте, еще и флешка в придачу.

Другой распространенный вариант – карта памяти уже идет в комплекте со смартфоном, хотя в спецификации ее нет. Приятный сюрприз? Конечно! Или продавец сам предлагает установить какую-нибудь карту для проверки нормальной работы телефона с такими носителями. Даже если Вы только что сами купили MicroSD карту, ему ничего не стоит отвлечь покупателя и при установке временно подменить носитель на уже «обработанный», а потом все вернуть обратно.

Иногда компания или спонсор дарит пользователям USB-флешки. Естественно, с рекламными материалами. Что будет делать с такой флешкой неискушенный пользователь? Отнесет ее на проверку в службу информационной безопасности? Хотя бы проверит антивирусом на специально выделенном компьютере под Linux? Сильно сомневаюсь. Скорее всего сразу же воткнет ее в свой компьютер. В лучшем случае домашний, а то и принесет на работу. Только не нужно говорить, что на домашнем компьютере или корпоративном ноутбуке нельзя использовать внешние флешки, что это реализовано

техническими методами. Практика показывает, что пользователи всегда требуют как можно больше «свободы», в том числе и для манипуляций с любыми флешками.

К счастью, бесплатная флешка с презентацией – далеко не самый частый вариант распространения malware и stalkerware. Все-таки фирма переживает за свою репутацию, эти носители в идеале должны проверяться и так далее. Если на фирме работает нормальный вдумчивый системный администратор или специалист по безопасности – он обязательно проверит все носители перед передачей в другие руки.

Гораздо худший вариант, если флешка была взята на прокат у «добренького» коллеги (стоит задуматься, а чего это он такой безотказный, да и флешка зачем-то всегда с собой?). Или еще хуже – это бесхозный предмет, который нашелся, например, в ящике офисной тумбочки, и владелец носителя так и не признался.

Результатом такой «удачной находки» может быть, как минимум, заражение вашего домашнего ПК, а то и корпоративной сети. Если «по доброте душевной» подбросили так называемую «флешку-убийцу» – есть шанс распрощаться с USB-контроллером на компьютере или ноутбуке. Если повезет по максимуму – полное выгорание домашнего или корпоративного компьютера. Особенно «весело», когда незадачливый админ втыкает такую «флешку» в сервер, роутер или USB-порт МФУ. Тут уж, как говорится, без комментариев.

Что делать?

1. Новое (купленное, подаренное) устройство не означает что оно обязательно безопасное. Доверяй, но проверяй! Новый ноутбук подлежит такой же проверке, как и любой другой! В идеале, если вы купили ноутбук под управлением Windows 10, сделайте сброс в заводские настройки и установите драйвера и прикладное ПО заново.

2. Не давайте без крайней необходимости что-либо вставлять в свое устройство. Ни карты памяти, ни USB-носители, ни SIM-карты – ничего. Не важно, компьютер, ноутбук, смартфон, роутер и так далее. Если прямо уж необходимо что-то куда-то подключить чтобы перенести информацию – только через проверку, и лучше не самостоятельно, а силами своей службы безопасности. Чем жестче и консервативнее подход – тем безопасней будет жизнь и тем дольше проработает данное устройство.

3. Никому и никогда не доверять PIN-код от вашего смартфона и, естественно, не доверять доступ к вашему смартфону. То же самое справедливо и для ноутбука, и для стационарного компьютера, и для роутера и так далее.

4. Если вам купили (подарили) смартфон, прежде чем вы начнете им пользоваться, сбросьте его в заводские настройки, а лучше перепрошейте его заново новой прошивкой с сайта производителя или продайте и купите себе сами. Чуть дороже, зато голова не болит!

5. Естественно, ничего нельзя прошивать «кастомными» прошивками из Интернет, которые что-то там улучшают.

6. Что делать с флешкой и прочими носителями информации? Здесь все тоже достаточно просто. Я уверен, что у вас на предприятии есть старый, но работающий ПК, который устарел для актуальных задач. Установите его в службе безопасности, отключив предварительно от сети и проверяйте на нем флешки с помощью RescueDisc. Какой вы при этом будете использовать антивирус – ваше дело. Не забудьте только предварительно каждый раз обновлять базы, лучше скачивая образ носителя целиком.

Внимание! Все те же проблемы могут ожидать, не только когда используют чужую флешку, но и временно передают ее для каких-то целей. Когда носитель вернули, его обязательно нужно проверить на выделенном компьютере, а дальше уже поступать в зависимости от того: нужна эта информация или лучше сразу обнулить носитель (для большей уверенности стоит удалить все разделы и создать их заново).

Заключение

Нет необходимости лишний раз рассказывать, что подобные приложения несут за собой вредные последствия. Исходная их концепция не этична. Однако стоит подчеркнуть, что сегодня для пользователя, у которого они установлены, возникает масса других угроз. Такие приложения вредят безопасности пользователей. Мало того, данные, собранные у пользователей, подвергаются риску утечки в результате взлома. Впоследствии эти данные могут использоваться для различных вредоносных воздействий, начиная от вымогательства денег до кражи цифровой личности.

И несмотря на все это, большинство защитных решений не детектируют коммерческие приложения-шпионы как угрозу из-за неопределенности их юридического статуса.

И если пользователи привыкли что их можно защитить от обычных угроз (как корпоративных, так и нет) с помощью антивирусных технологий, антиспама, пусть частично, но все же, то в данном случае интересно то, что линией обороны выступает сам пользователь. Ведь строгий PIN-код, настройка и регулярная проверка установленного ПО и носителей информации – это в первую очередь задача пользователя. И, конечно же, приветствуется вдумчивый и осторожный подход ко всему, что нас окружает в цифровом мире.

Что вам сказать? Добро пожаловать в новый мир. Вы готовы? Впрочем, вас никто не спрашивает! EOF

[1] Worried about your child's phone or tablet usage? http://www.phonesheriff.com/
[2] How to Tell If Your Partner Is Spying on Your Phone https://www.vice.com/en_us/article/zmdg5e/know-if-someone-is-spying-on-my-phone
[3] How does it Works? https://www.mobistealth.com/how-it-works
[4] The Best Parental Control App to Protect Your Kids https://www.familyorbit.com/
[5] Программа для прослушки компьютера, мобильного телефона или планшета https://www.flexispy.com/ru/
[6] Национальный центр по борьбе с бытовым и сексуальным насилием http://www.ncdsv.org
[7] Abusive partners use home technology to stalk and abuse women, study shows https://www.standard.co.uk/tech/abusive-partners-use-home-technology-to-stalk-and-abuse-women-study-shows-a3921386.html
[8] Бережной А. Создаем ИТ-структуру, устойчивую к вредоносному ПО. Часть 1. // «Системный администратор», № 6, 2010 г. http://samag.ru/archive/article/984
[9] Бережной А. Создаем ИТ-структуру, устойчивую к вредоносному ПО. Часть 2 // «Системный администратор», Спецвыпуск № 2 «Безопасность», 2010 г. http://samag.ru/archive/article/1066

Ключевые слова: вирус, безопасность, stalkerware, malware, virus, IT security, антивирус, шпионское ПО, смартфон, флешка