Опубликовано: 8 февраля 23:20

ИСТОЧНИК: НАРОДНАЯ ГАЗЕТА

Как защитить компьютеры и телефоны от вредоносных программ

Вирусы становятся мобильнее

Каждый день хакеры придумывают новые способы заразить технику. Если раньше вредоносный софт чаще был нацелен на офисные устройства, то в последнее время под особым прицелом — телефоны, веб-камеры, приставки к ТВ. Шпионское или вредительское приложение может украсть личные данные, затормозить работу устройства. При этом вредоносная программа маскируется, и распознать ее порой непросто. Как противостоять угрозам?

PINTEREST.COM

Слабое звено

Раньше вирусы «приносили на дискете». Например, запустившего зараженную компьютерную игру пользователя ждали сюрпризы: пропадали файлы. Приходилось вызывать специалиста, чтобы тот «вылечил» технику. Когда дискеты устарели, вирусы «переехали» на компакт-диски, а потом распространение вредоносных программ подхватил интернет. Притом «паразиты» могут быть занесены даже при производстве смартфона, попадая на девайс через сторонних поставщиков программного обеспечения, к которым обращаются многие компании.

Летом прошлого года пользователей классических сотовых телефонов бренда Digma в России ждал неприятный сюрприз — техника оказалась заражена вредоносным ПО. Что интересно, мобильники не поддерживают установку приложений — опасный софт в них могли интегрировать на одном из этапов производства. В России эти телефоны занимают почти 6 % рынка. На маркетплейсах их продажи в разы выше, чем офлайн. Уязвимость «звонилок» позволяет злоумышленникам в том числе отправлять СМС-сообщения и перехватывать входящие СМС от банка.

Как оказалось, простой кнопочный мобильник в фоновом режиме подключался к удаленному серверу через мобильный интернет. После установки соединения телефон сливал данные об IMEI-номере устройства, названии оператора и идентификаторе сим-карты. А чтобы абонент ничего не заподозрил, входящие и исходящие сообщения, обработанные вирусом, в памяти устройства не сохранялись. Компания заявила, что разбирается с «аномалиями» в прошивке устройства.

Случай из Минска. В столичной прокуратуре рассказали, что направили в суд уголовное дело в отношении 28-летнего минчанина, который разрабатывал и распространял вредоносные компьютерные программы. Обвиняемый на веб-сайте и в Telegram подыскивал клиентов и предлагал им услуги по защите их систем, а на самом деле вносил в данные заказчиков конкретный набор скрытых предписаний. В результате — получение несанкционированного доступа к компьютерам жертв.

Технику, зараженную вирусами, киберпреступники могут продавать на маркетплейсах. За хитрыми схемами скрываются как отдельные хакеры, так и организованные группы, использующие популярные площадки для распространения вредоносного ПО. Низкая цена и кажущаяся

выгодность предложения зачастую служат крючком для ничего не подозревающих покупателей. Мотивы у злоумышленников различные: от кражи финансовой информации и личных данных до использования зараженных устройств для DDoS-атак или майнинга криптовалюты.

Буткиты проникают в прошивку

В смартфоне хранятся наша переписка, номера карт, паспортные данные и другая информация, которую может использовать злоумышленник. Борьба со шпионскими программами — задача со звездочкой, ведь многие приложения на девайсе устанавливаются производителем еще на заводе. Да и обычному пользователю довольно сложно разобраться, какую опасность представляет программа, которая под видом безобидного значка «попросила» обновиться.

Ольга Бойправ, кандидат технических наук, и.о. заведующего кафедрой защиты информации БГУИР, выделяет около 20 видов вредоносного ПО, отличающихся друг от друга алгоритмом функционирования и задачами, которые преследуют киберпреступники:

— Коды вредоносного программного обеспечения могут содержаться в кодах веб-страниц и нелицензионных играх, обработчиках фото, медиапроигрывателях, прошивках различных устройств (флешек, веб-камер, клавиатур, подключаемых к USB-разъемам, TV Box и других). Вредоносное ПО, коды которого включаются в прошивку устройств, называют буткитами. Заражению вирусами подвержены программные средства и устройства, выпускаемые как неизвестными, так и проверенными вендорами (поставщиками). При установке, обновлениях, покупке нового устройства обязательно анализируйте, не были ли они скомпрометированы. Один из ключевых способов защитить свой компьютер от буткитов — установить в UEFI режим Secure Boot (UEFI от англ. Unified Extensible Firmware Interface — «унифицированный расширяемый интерфейс прошивки»).

Эксперт советует при выборе нового устройства обращать внимание на его стоимость. Насторожить должны такие подозрительные моменты, как чересчур низкая цена той же флешки, жесткого диска, смартфона, отсутствие контактов продавца и истории магазина, доставки и самовывоза.

— Даже если такое дешевое устройство не заражено вредоносным ПО, оно может содержать уязвимости, которые потом помогут

киберпреступникам внедрить опасное программное обеспечение, — обращает внимание Ольга Бойправ. — *Как правило, устройство, продаваемое по цене ниже рыночной, не обладает заявленным функционалом. Часто эта особенность прослеживается у дешевых флешек.*

ДОСЛОВНО

Светлана Костевич, адвокат Минской городской коллегии адвокатов:

— *По законодательству любой товар должен иметь соответствующее качество. Это понятие включает совокупность свойств и характеристик, определяющих соответствие товара установленным и (или) обычно предъявляемым к нему требованиям (безопасность, функциональная пригодность, эксплуатационные характеристики, надежность, экономические, информационные и эстетические требования и др.). Например, покупатель приобрел изделие с зараженным ПО. Если из-за этого пропадет возможность использовать технику по назначению, функционально она непригодна, то такое изделие будет являться товаром ненадлежащего качества. Также отмечу, что недостатком товара считается его несоответствие нормативным документам, устанавливающим требования к качеству изделия (технические нормативные правовые акты, санитарные нормы и правила, гигиенические нормативы, а также технические регламенты Таможенного союза, Евразийского экономического союза и т.д.), иному законодательству или условиям договора. При наличии разногласий по качеству изделия экспертиза проводится за счет продавца. Также доказательствами правоты покупателя могут служить переписка, текст размещенного в интернете объявления о продаже техники, заключение специалиста на предмет соответствия товара техническим нормативам.*

В ТЕМУ

Для того чтобы защититься от угроз, связанных с покупкой зараженной электроники, важно соблюдать определенные правила кибербезопасности: изучить рейтинг продавца, а также тщательно прочитать отзывы других покупателей.

— Советую поискать на ресурсах информацию о том, компрометировалась ли когда-нибудь продукция вендора этого устройства. Кроме того, старайтесь не подключать к своему компьютеру незнакомые девайсы. Можно отдать гаджет на диагностику. Но следует понимать, что не всякое вредоносное программное обеспечение можно удалить. Известны случаи, когда сброс до заводских настроек не помог убрать с мобильных телефонов трояна, код которого был встроен в код мобильного приложения для редактирования изображений, — говорит Ольга Бойправ.

Пользователь должен быть уверен, что в специализированном центре работники действительно удалят вирус, а не добавят что-то свое вредоносное. «Гаражный сервис» тут точно не подойдет, следует искать профессионалов с хорошими отзывами.

Кристина ХИЛЬКО