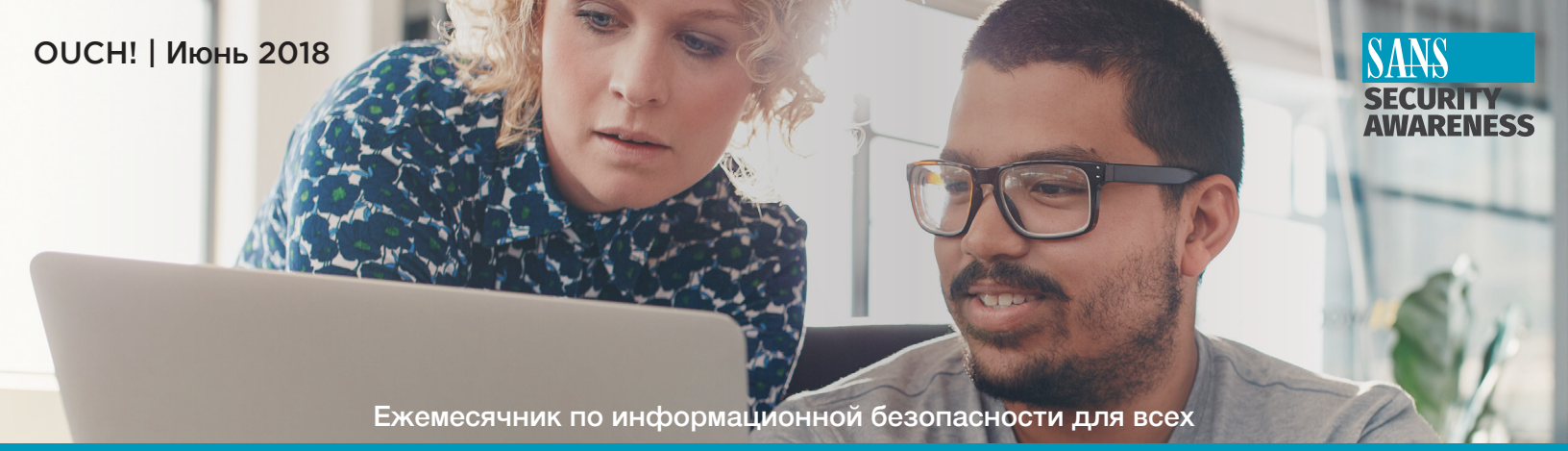

Ежемесячник по информационной безопасности для всех

Защита от вирусов

Обзор

Скорее всего, вы не раз слышали такие термины как вирус, Троян, программы-вымогатели или руткит при обсуждении компьютерной безопасности. Все эти термины обозначают специфические виды вредоносных программ, с помощью которых злоумышленники пытаются инфицировать компьютер или мобильные устройства. После установки, вредоносные программы позволяют получают полный контроль над компьютером или мобильным устройством. Сегодня мы поговорим о вредоносных программах, об опасностях, которые они представляют и, самое главное, как себя от них защитить.

Что такое вредоносные программы?

Вредоносные программы – компьютерные программы, осуществляющие вредоносные действия. Английский термин malware образован из слов malicious (вредоносная) и software (программа). Злоумышленники устанавливают вредоносные программы на ваши компьютеры или гаджеты для того, чтобы их контролировать. Будучи установленной, вредоносная программа позволяет мошенникам следить за вашей онлайн активностью, красть ваши пароли или файлы, или использовать вашу систему для атак на другие системы. Вредоносные программы могут даже взять под контроль все ваши файлы и требовать за них выкуп. Многие люди думают, что проблема вредоносных программ актуальна только для пользователей Windows. К сожалению, вредоносные программы могут атаковать абсолютно любое устройство, от компьютеров Mac и смартфонов, до камер безопасности и цифровых видеорегистраторов. Чем больше компьютеров или устройств мошенникам удаётся инфицировать, тем больше денег они могут заработать. Поэтому их целью является любой человек, в том числе и вы.

Защитите себя от вирусов

Может сложиться впечатление, что установки антивирусных программ достаточно для защиты от вирусов. К сожалению, антивирус не может обнаружить и обезвредить все вредоносные программы. Кибер мошенники постоянно разрабатывают новые продвинутые программы, способные обойти антивирус. С другой стороны, производители антивирусных программ тоже постоянно совершенствуют свои продукты, разрабатывая новые методы обнаружения вредоносных программ. Это соревнование никогда не заканчивается, и плохие парни обычно всегда на шаг впереди. Вот почему нельзя полагаться только на антивирус, а следует предпринять дополнительные шаги для своей защиты:

Кибер мошенники пытаются атаковать ваш компьютер или устройство через уязвимость в системе. Чем более новой версией программного обеспечения вы пользуетесь, тем меньше у них шансов её инфицировать. Поэтому регулярно обновляйте операционную систему, приложения, браузер и его дополнительные модули. Самый простой способ – настроить автоматическое обновление.

Чаще всего кибер преступники инфицируют систему или мобильное устройство с помощью фальшивых программ или мобильных приложений, размещая их в интернете и обманным путём вынуждают их загрузить или установить. Поэтому следует загружать программы или устанавливать приложения только из проверенных онлайн магазинов. С осторожностью относитесь к совершенно новым программам или приложениям, по которым есть только небольшое количество положительных отзывов, их редко обновляют или загрузило небольшое количество пользователей. Если больше не пользуетесь программами или приложениями, то их нужно удалить.

Мошенники часто пытаются установить вирус с помощью обмана. Например, вам могут прислать электронное письмо, которое выглядит очень правдоподобно, и содержит вложение, которое нужно открыть, или ссылку, по которой нужно перейти. Письмо может быть якобы из банка или от вашего друга. В любом случае, если вы откроете вложение или перейдёте по ссылке, то активируете вредоносный код, который загрузит вирус в вашу систему. Если в письме создаётся иллюзия срочности, его содержание слишком хорошо, чтобы быть правдой, то, скорее всего, это атака. Проявляйте бдительность, здравый смысл – ваша лучшая защита.

Регулярно создавайте резервные копии системы и файлов, размещайте на облачных сервисах или храните на съёмных дисках, которые не подключаются к сети. Это поможет сохранить и восстановить данные, если вирусы их удалят или зашифруют. Резервные копии очень важны, во многих случаях это единственный способ восстановить данные в случае атаки.

Таким образом, лучшая защита от вредоносных программ – использование последних версий программ и их регулярное обновление, установка надёжной антивирусной программы и внимание к различным уловкам, с помощью которых вам пытаются загрузить вирусы. Регулярное создание резервных копий является единственным гарантированным способом восстановления данных в случае заражения вашей системы.

Об авторе

Ленни Зельцер *борется с вредоносными программами, разрабатывая продукты безопасности в компании Minerva Labs и преподавая в Институте SANS. Ленни ведёт страничку в Twitter @lennyzeltser и блог информационной безопасности на zeltser.com.*

Ресурсы

Программы-вымогатели:	https://www.sans.org/u/EdI
Резервное копирование и восстановление:	https://www.sans.org/u/EdN
Осторожно, фишинг!:	https://www.sans.org/u/EdS
Классификация вредоносных программ:	https://www.kaspersky.ru/blog/klassifikaciya-vredonosnyx-programm/2200/

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: www.sans.org/security-awareness/ouch-newsletter. Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова