Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Что такое вредоносные программы
- Кто создает вредоносные программы
- Как защититься от вредоносных программ

Что такое вредоносные программы

Обзор

Скорее всего, в контексте компьютерной безопасности вы слышали такие термины, как вирус, троян, программы-вымогатели или руткит. Все эти слова обозначают типы программ, используемых мошенниками для инфицирования компьютера или мобильного устройства. Универсальный термин для всех этих типов программ – вредоносные программы. В этом выпуске мы расскажем, что такое вредоносные программы, кто их создает и зачем, и, самое важное, научим, как защитить себя от них.

Об авторе

Ленни Зельцер специализируется на защите информационной безопасности клиентов корпорации NCR Corp. Он также преподает курс по защите от вредоносных программ в Институте SANS. Ленни публикует записи в Twitter **@lennyeltser** и ведёт блог **zeltser.com**.

Что такое вредоносные программы

Вкратце, вредоносные программы - это компьютерные программы, которые используются для осуществления вредного воздействия. Этот термин состоит из двух слов: «вредоносный» и «программа». Кибер мошенники устанавливают вредоносные программы на ваш компьютер или устройство, чтобы получить контроль над ним или получить доступ к информации на них. После установки, вредоносная программа позволяет отслеживать ваши действия в интернете, похищать пароли или файлы, или использовать вашу систему для атаки других пользователей. Вредоносная программа даже может заблокировать вам доступ к вашим собственным файлам и вам придется заплатить за возобновление доступа к ним.

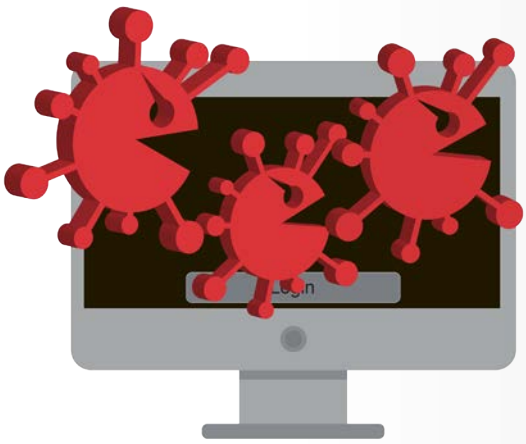
Многие ошибочно считают, что вредоносные программы могут угрожать только пользователям системы Windows. На самом деле, система Windows просто самая распространённая, вредоносные программы могут заразить абсолютно любую систему и любое устройство, включая компьютеры Mac, смартфоны и планшеты. Чем больше компьютеров или устройств мошенники могут заразить, тем больше денег они получат. Таким образом, любой может стать жертвой, включая вас.

Кто создает вредоносные программы

Вредоносные программы создают не только любители или дилетанты, но и профессиональные киберпреступники. Их цель – получить деньги с каждого инфицированного компьютера или устройства путем

Что такое вредоносные программы

кражи данных, рассылки спама по электронной почте, запуска атак отказа обслуживания или осуществления вымогательства. Люди, создающие, распространяющие и получающие выгоду от вредоносных программ могут быть как отдельными личностями, так и хорошо организованными криминальными группами и даже целыми компаниями. Люди, создающие современные сложные вредоносные программы, работают полную рабочую неделю. Кроме того, однажды создав вредоносную программу, они не только продают её другим людям или организациям, но и поддерживают своих «клиентов» с помощью регулярных обновлений и техподдержки.



Чтобы защитить свою систему, нужно скептически относиться к подозрительным сообщениям, регулярно обновлять устройства и стараться использовать самые последние антивирусные программы.

Как защититься от вредоносных программ

Самым простым способом защиты является установка антивирусных программ от надёжного производителя. Антивирусные программы специально разработаны для предотвращения и обнаружения вредоносных программ. Но помните, что даже самый современный антивирус не может обнаружить или остановить абсолютно все вредоносные программы. Киберпреступники регулярно создают новые, всё более сложные программы, которые всё трудней обнаружить. Получается бесконечная гонка производителей антивирусов и злоумышленников. К сожалению, плохие парни всегда на шаг впереди. Следовательно, нужно обеспечить себя дополнительной защитой, не полагаться только на антивирус.

- Кибер мошенники чаще всего используют слабые места в системе для заражения компьютера или устройства. Поэтому, чем современней система, тем меньше у неё слабых мест и злоумышленникам сложнее заразить вирусом вашу систему. Учитывая это, следует установить автоматическое обновление всех операционных систем, приложений и устройств.
- Чаще всего мошенники распространяют вирусы под видом приложений, публикаций в Интернете, или обманом вынуждают людей загрузить или установить программу. Поэтому следует загружать приложения только из надёжных источников. Кроме того, устанавливайте приложения, давно существующие в онлайн магазинах с большим количеством положительных отзывов других пользователей.
- На компьютере следует использовать обычную, непривелигированную учётную запись, а не учетную запись администратора. Это предоставляет дополнительную защиту от вирусов, которые могут автоматически устанавливаться.

Что такое вредоносные программы

- Злоумышленники обманным путем заставляют людей устанавливать вредоносные программы. Например, они могут прислать письмо по электронной почте с инфицированным вложением или ссылкой. Причем, письмо может выглядеть достоверно, например, от имени банка или вашего друга. Если вы откроете вложение или перейдёте по ссылке, вы активируете код вредоносной программы, и она попадёт в вашу систему. Если в письме создается ситуация срочности, вас что-то настораживает или содержание слишком хорошо, чтобы быть правдой, скорее всего, это атака. Будьте внимательны, зачастую осторожность и есть лучшая защита.
- Регулярно делайте резервные копии системы и данных на облачные сервисы или храните данные на съёмных дисках. Это поможет защитить информацию, если вирус её зашифрует или повредит. Резервные копии очень важны, в некоторых случаях это единственный способ восстановить данные.

Следовательно, лучшие способы защиты: регулярное обновление системы, установка надёжного антивируса от известных производителей и осторожность - всё это обеспечит наилучшую защиту вашей системы.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Ресурсы

Фишинг:	https://securingthehuman.sans.org/ouch/2015#december2015
Социальная инженерия:	https://securingthehuman.sans.org/ouch/2014#november2014
Безопасное использование мобильных приложений:	https://securingthehuman.sans.org/ouch/2015#january2015
Безопасность планшета:	https://securingthehuman.sans.org/ouch/2016#january2016
Резервное копирование и восстановление данных:	https://securingthehuman.sans.org/ouch/2015#august2015

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова

