Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Почему вы цель для мошенников
- Способы защиты

Да, Вы действительно цель для мошенников

Обзор

Многие люди ошибочно считают, что их компьютер или они не могут быть целью кибер преступников: они сами или их компьютеры не могут интересовать мошенников. Это абсолютно не так. Если у вас есть компьютер, мобильное устройство, онлайн счета, электронная почта, кредитная карта или вы занимаетесь другой деятельностью в Интернет, то вы можете стать источником доходов для мошенников. В этом выпуске мы поговорим о том, чем вы можете заинтересовать мошенников, какие могут быть атаки и как себя защитить.

Об авторе

Эрик Конрад – Президент и CTO компании Backshore Communications и один из ведущих авторов книг CISSP Study Guide, Second Edition и the Eleventh Hour CISSP, Second Edition. Также, он соавтор шестидневного курса SANS Continuous Monitoring and Security Operations (SEC511).

Почему вы цель для мошенников

Преступления, такие, как кража личных данных, существуют с момента существования цивилизации и стали частью нашей жизни. Цели преступников всегда одинаковы: получить как можно больше денег с минимальными затратами и рисками. Раньше это было не так легко, так как преступнику нужно было караулить жертву и физически с ней взаимодействовать. Далеко не все преступления совершались подобным образом, но преступники подвергались большому риску. Всё кардинально изменилось с появлением Интернет и онлайн технологий. Теперь преступники могут находить жертву по всему миру абсолютно бесплатно или с небольшими затратами. Кроме того, кибер преступники стали весьма организованными, что позволяет им быть эффективными как никогда.

Прежде всего, преступники знают, что чем больше они украдут номеров кредитных карт, тем больше банковских счетов они могут взломать, или чем больше паролей они взломают, тем больше денег смогут заработать. Они в буквальном смысле пытаются взломать абсолютно всех, кто подключен к Интернет, в том числе и вас. Процесс взлома миллионов людей по всему миру не так трудоёмок, как кажется, ведь часть работы автоматизирована. Например, преступники могут создать базу данных из миллионов адресов электронной почты и использовать автоматическую рассылку для фишинг атак. Отправка писем не стоит ничего для преступников: они могут отправлять письма со

Да, Вы действительно цель для мошенников

взломанных компьютеров, включая ваш, таким образом и проделывают грязную работу. Это ещё один пример того, чем ваш компьютер может заинтересовать злоумышленников, если не получается его взломать или навредить другим. В конечном счёте, преступники не знают, кто может стать их жертвой, но они знают, что чем больше писем разошлют, тем выше вероятность получить жертву. Большая вероятность того, что преступники могут сканировать абсолютно любой компьютер или устройство, подключенное к Интернет, с помощью уже взломанных компьютеров для сканирования. Поэтому не стоит думать, что вы особенные и не интересуете мошенников, ведь преступникам интересны абсолютно все, включая вас.

Вы можете не сознавать этого, но ваши гаджеты и ваша информация очень ценятся преступниками всего мира.

Способы защиты

Как правило, кибер преступники пытаются взломать миллионы людей по всему миру с помощью относительно простых методов. Следуя некоторым простым рекомендациям, вы сможете себя защитить.

- **Вы сами**. Прежде всего, вы и есть первая линия обороны от атак. Многие атаки начинаются с попыток обмануть или одурачить вас, например, заставить открыть инфицированное вложение в письме электронной почты или пытаются получить ваш пароль от почты по телефону. Лучшей защитой является здравый смысл: если что-то слишком подозрительно или хорошо, чтобы быть правдой, значит, так оно и есть и это может быть атакой.

- **Обновления**. Убедитесь, что ваш компьютер или устройство регулярно обновляется, и вы работаете с последними версиями. Это важно не только для системы, но и для всех приложений, которыми вы пользуетесь. Продолжайте регулярно обновлять систему и приложения, чтобы избежать атак.

- **Пароли**. Всегда используйте сильный, уникальный пароль для каждого аккаунта. Если один из сайтов взломают, то все другие пароли от других учётных записей по-прежнему будут в безопасности. Также, сильным и уникальным паролем, ПИН-кодом или другим механизмом

Да, Вы действительно цель для мошенников

блокировки следует защитить все устройства, которыми вы пользуетесь. Чтобы надёжно оперировать всеми паролями следует использовать Менеджер паролей (Password Manager).

- **Кредитные карты**. Проверяйте свои выписки по счетам как минимум еженедельно, ежемесячно не всегда достаточно. Как только вы заметите несанкционированное использование карты, немедленно свяжитесь с банком. Если банк предоставляет услугу оповещения о подозрительно больших тратах или превышении лимита по электронной почте или смс, следует ей воспользоваться.

- **Ваша сеть**. Обеспечьте безопасность домашней сети Wi-Fi с помощью надежного пароля администратора и настройки запроса пароля для всех, кто пытается к ней подключиться. Также убедитесь, что все подключенные к сети устройства регулярно обновляются.

- **Социальные сети**. Чем больше информации о себе вы размещаете на различных сайтах, тем больше рисков для вас. Кроме того, что любая информация упрощает возможность вас обмануть, но и позволяет распознать в вас более интересную цель для мошенников.

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

OUCH! Менеджер паролей:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Защита Домашней Сети:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Фишинг: атаки по электронной почте:	http://www.securingthehuman.org/ouch/2013#february2013
Плакат «Вы-Цель!»:	http://www.securingthehuman.org/resources/posters

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 3.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

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