Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Что такое вредоносные программы
- Кто и зачем их распространяет
- Как защитить себя

Что такое вредоносные программы

Обзор

Наверное, вы слышали такие термины компьютерной безопасности, как вирус, червь, троян или руткит (набор утилит или специальный модуль ядра для маскировки объектов, контроля событий и сбора данных). Все эти термины относятся к различным видам программ, используемых преступниками для контроля компьютеров и мобильных устройств. Все эти программы относятся к категории вредоносных программ. В данном выпуске мы поговорим о том, что такое вредоносные программы, кто и зачем их разрабатывает и как защитить себя от них.

Об авторе

Ленни Зельцер – автор февральского выпуска OUCH! Ленни специализируется на защите IT операций клиентов корпорации NCR и читает лекции по борьбе с вирусами в Институте SANS. У Ленни есть страничка в Twitter **@lennyzeltser** и блог **blog.zeltser.com**.

Что такое вредоносные программы

Прежде всего, смысл термина заключен в названии: «вредоносные» и «программы». Конечной целью мошенников является установка вредоносной программы на ваш компьютер или мобильное устройство. Если это произойдет, то хакер получит полный контроль над ними. Многие ошибочно считают, что вредоносные программы могут угрожать только компьютерам с Windows. Windows очень широко используется, поэтому и является заметной мишенью; вредоносные программы могут заразить любое компьютерное устройство, включая планшет или смартфон. На самом деле количество вредоносных программ для смартфонов растет все больше. И помните, любой может стать жертвой, даже вы. Чем больше компьютерных устройств будут заражены, тем больше денег могут получить мошенники. Обычно кибер мошенникам безразлично кого заразить, им нужно как можно большее количество заражений.

Кто распространяет и зачем

Вирусы не создаются хакерами из любопытства или дилетантами; они создаются кибер преступниками для достижения определенных целей. Такими целями является кража конфиденциальной информации, сбор логинов и паролей, рассылка спама по электронной почте, запуск атак отказов сервиса, кража или вымогательство в обмен на личные данные. Например, хорошо известный вирус Cryptolocker используется мошенниками для инфицирования и шифровки всех данных на компьютере. Если удается заразить компьютер и зашифровать все данные, кибер преступники требуют выкуп за расшифровку.

Что такое вредоносные программы

Люди, которые разрабатывают, применяют и получают прибыль от вредоносных программ, могут быть одиночками, а могут состоять в организованной группе или даже работать в государственной компании. Люди, которые разрабатывают современные сложные вредоносные программы, часто посвящают этому всё свое время. Случается, что однажды продав вредоносную программу человеку или компании, они предоставляют регулярные обновления и поддержку своим так называемым «клиентам». Купив программу всего лишь раз, преступники зарабатывают деньги на установке миллионам ничего не подозревающих жертв, создавая ботнет инфицированных систем. Ботнет становится удаленно контролируемой армией, которую кибер преступники могут использовать в своих целях или продать инфицированные компьютеры другим преступникам.

лучшим способом защиты от вредоносных программ являются регулярные обновления, использование последней версии антивируса и осторожность.

Как защитить себя

Основным шагом для защиты компьютера и мобильных устройств является установка антивирусного программного обеспечения от надёжных провайдеров. Антивирус – это специальная программа, созданная для обнаружения и защиты от вредоносных программ. Но антивирус не может обнаружить или удалить абсолютно все вредоносные программы. Кибер преступники постоянно изобретают, разрабатывают новые и более сложные атаки, которые могут преодолеть антивирус. С другой стороны, производители антивирусных программ постоянно обновляют свои продукты для борьбы с новыми вирусами. Обе стороны пытаются различными способами перехитрить друг друга. К сожалению, кибер преступники часто побеждают. Например, следует помнить, что антивирус может обнаружить и заблокировать большую часть вредоносных программ, но мошенники безостановочно создают новые версии, которые пройдут через защиту. В результате чего не следует полагаться только на антивирус, следует предпринять следующие дополнительные шаги для защиты.

Прежде всего, следует настроить автоматическое обновление операционной системы и приложений. Самая последняя версия наиболее сложна для взлома преступниками.

Во-вторых, помните, вы сами лучшая защита от вредоносных программ. Эти программы часто распространяются с помощью социальной инженерии, которая представляет собой установку программы обманным путём. Примером может являться фишинг атака, когда рассылаются поддельные письма электронной почты, созданные для обмана. Например, преступники отправляют письмо от имени вашего банка, в котором просят вас перейти по ссылке. Если вы перейдёте по

Что такое вредоносные программы

ссылке, то попадёте на сайт, который автоматически попытается взломать ваш компьютер и инфицировать его. Или в письме говорится о том, что ваша посылка не может быть доставлена и вам нужно открыть накладную во вложении, которая при открытии заразит ваш компьютер.

Атаки с помощью социальной инженерии могут использовать и другие технологии, в частности, ваш телефон. Например, хакеры могут позвонить вам от имени службы поддержки Microsoft и сообщить о заражении компьютера. Это неправда и ваш компьютер на самом деле в порядке. Целью этого звонка является получение удалённого доступа к вашей системе или установка вредоносной программы. Прислушивайтесь к интуиции. Если телефонный звонок или сообщение кажется странным, подозрительным или слишком хорошим, чтобы быть правдой, то, скорее всего, так и есть.

Таким образом, использование последних версий программного обеспечения, установка надёжного антивируса от известного производителя и осторожность помогут избежать заражения вашего компьютера.

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 - Фишинг: атаки по электронной почте:

www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

OUCH - Семь простых шагов для защиты компьютера:

www.securingthehuman.org/resources/newsletters/ouch/2012#december2012

Вы – Цель (плакат):

http://www.securingthehuman.org/resources/posters

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