Безопасность в Интернете

Отформатировано Нагаевой Марией

Оглавление

Введение.

Тему безопасности в интернете можно разделить на две части. Первая - это, собственно, обеспечение безопасности сайтов, защита сайтов и серверов, на которых они расположены, от взлома и атак хакеров. Но вначале, безусловно, ещё не начиная создания своего сайта, вопросами безопасности своего компьютера должен озаботиться каждый пользователь, выходящий в интернет. И этой второй части - вопросам безопасности пользователя интернета будет посвящена данная статья.

В настоящее время наблюдается массовый приток в интернет слабо подготовленных в области информационных технологий пользователей, которые имеют весьма туманное представление о потенциальных угрозах, которые могут подстерегать их в сети, и в результате их компьютеры оказываются заражёными различными вирусами и троянами, которые занимаются кражей паролей, участвуют в распределённых атаках (DDoS) на различные сайты, используются спамерами для организации масовых рассылок. В результате провайдеры вынуждены идти даже на меры по принудительному отключению таких пользователей. Ниже мы постараемся дать обзор основных сведений по безопасности для начинающих пользователей сети интернет.

Для чего кому-то нужно взламывать ваш компьютер?

Даже если вы самый что ни на есть обыкновенный пользователь и на вашем компьютере нет какой-либо ценной и секретной информации, не нужно пребывать в иллюзии, что ваш компьютер никому (в плане его взлома) не интересен. С точки зрения хакеров и людей, распространяющих вредоносные программы, он всё равно будет представлять ценность. Времена, когда вирусы писали ради спортивного интереса, уже прошли и сегодня весь хакерский инструментарий используется ради получения коммерческой выгоды. В отличие от вирусов прошлого, которые могли отформатировать ваш винчестер или порадовать ничего не подозревающего владельца компьютера всякими неожиданными эффектами, сегодня вредоносные программы стараются маскироваться и скрывать свою деятельность, чтобы втайне выполнять заложенные в них функции. Такими функциями могут быть:

- ✓ кража паролей от ваших электронных кошельков, почтовых ящиков, icq, сайтов, аккаунтов в различных сервисах и т. д. К сожалению, случаи, когда открыв в один прекрасный день свой кошелёк webmoney, пользователь обнаруживает в нём ноль, не редкость, причём установить, куда и кем были переведены деньги, в таких случаях весьма затруднительно. Украв пароль от почтового ящика, вредоносная программа может от вашего имени разослать по имеющимся в вашей адресной книге адресам письма с вложенными в них троянами или вирусами и т. д.
- ✓ достаточно прибыльным "бизнесом" в наше время является организация DDoS-атак, которые могут направляться на любой сайт или сервер, даже не имеющий каких-либо существенных уязвимостей. В результате таких атак сервер перегружается запросами, идущими с многочисленных компьютеров в разных регионах мира и сайт, на который направлена атака, таким образом отключается. Многочисленные случаи DDoS-атак на различные сайты были бы невозможны, если бы в распоряжении организаторов этих атак не находилось большое количество компьютеров обычных ничего не подозревающих пользователей, заражённых троянами, которые по сигналу извне начинают все вместе посылать запросы на сервер, выбранный в качестве жертвы.
- ✓ организация массовых рекламных рассылок такж является, к сожалению, прибыльным бизнесом, и для таких целей также практикуется заражение компьютеров обычных пользователей троянами.
- ✓ перечисленные цели являются наиболее типичными, но, в принципе, цели могут быть ограничены лишь фантазией автора троянов и вирусов. Троян может зашифровать, например, некоторые из имеющихся на вашем компьютере файлов и затем требовать плату за восстановление информации, заставлять ваш модем звонить на платные телефонные номера и т. д. Последние 2 года были отмечены эпидемией т. н.

"блокировщиков" Windows, когда попавшие на компьютер вирусы блокировали работу компьютера и требовали отправить платную смс для его разблокировки.

Источники опасностей.

Подхватить вредоносную программу, к сожалению, значительно легче, чем многие себе представляют. Для взлома компьютеров пользователей сети и кражи важных данных, например, паролей электронных платёжных систем, применяются следующие методы:
1) социальная инженерия - метод основанный на психологических приёмах, который существует и эффективно используется с самого начала развития компьютерных сетей и которому не грозит исчезновение. Список уловок, придуманных хакерами в расчёте на доверчивость пользователей, огромен. Вам могут прислать письмо от имени администрации сервиса с просьбой выслать им якобы утерянный пароль или письмо, содержащее безобидный, якобы файл, в который на самом деле спрятан троян, в расчёте на то, что из любопытства вы сами его откроете и запустите вредоносную программу.
2) трояны и вирусы могут быть спрятаны в различных бесплатных, доступных для скачивания из интернета программах, которых огромное множество или на пиратских дисках, имеющихся в свободной продаже.
3) взлом вашего компьютера может быть произведён через дыры в распространённом программном обеспечении, которых, к сожалению, довольно много и всё новые уязвимости появляются регулярно. Хакеры, в отличие от большинства пользователей, не следящих за уязвимостями и часто не скачивающих устраняющие их патчи, за обнаружением новых уязвимостей следят и используют их в своих целях. Для того, чтобы компьютер, имеющий уязвимости, был заражён, достаточно, например, всего лишь зайти на определённую страничку (ссылку на эту страничку хакер может прислать в письме, оставить на форуме и т. д.).
4) в последнее время получил распространение фишинг - создание поддельных сайтов, копирующих сайты известных фирм, сервисов, банков и т. д. Заманить вас на такой поддельный сайт могут разными способами, а цель - украсть данные вашего аккаунта (т. е. логин и пароль), которые вы обычно вводите на странице настоящего сайта.

Меры по защите.

- Установите файрволл (firewall). Хотя в Windows, начиная с версии XP и появился встроенный файрволл, его функциональность оставляет желать лучшего. Поэтому установите надёжный файрволл, выбрать который вам поможет актуальный рейтинг файрволлов. Некоторые из подобных программ можно скачать бесплатно или за небольшую сумму.
- Установите антивирусное и антишпионское ПО. Антивирусные программы должны быть свежими и регулярно скачивать базы с обновлениями через интернет. Антивирусное ПО должно запускаться автоматически при загрузке Windows и работать постоянно, проверяя запускаемые вами программы, в фоновом режиме. Обязательно проверяйте на вирусы перед первым запуском любые программы, которые вы где-либо скачиваете или покупаете.
- Своевременно скачивайте и устанавливайте все критические обновления для Windows, Internet Explorer и т. п.
- Не устанавливайте или удалите лишние ненужные службы Windows, которые не используете, например, службу доступа к файлам и принтерам и т. п. Это ограничит возможности хакеров по доступу к вашему компьютеру.
- Не открывайте подозрительные письма странного происхождения, не поддавайтесь на содержащиеся в них сомнительные предложения лёгкого заработка, не высылайте никому пароли от ваших аккаунтов, не открывайте прикреплённые к письмам подозрительные файлы и не переходите по содержащимся в них подозрительным ссылкам.
- Не используйте простые пароли. Нельзя в качестве паролей использовать простые комбинации символов, вроде "qwerty" или "9999". Такой пароль будет взломан программой для перебора паролей за считанные секунды. Не используйте короткие пароли (меньше 6 символов), не используйте в качестве паролей слова, которые есть в словаре. Не используйте один и тот же пароль на все случаи жизни.
- Будьте осторожны при выходе в интернет из мест общего пользования (например, интернет-кафе), а также при использовании прокси-серверов. Пароли, который вы вводите, в этом случае, с большей вероятностью могут быть украдены.
- При использовании электронных платёжных систем типа webmoney или яндекс-деньги, работа с ними через веб-интерфейс является менее безопасной, чем если вы скачаете и установите специальную программу (WebMoney Keeper или интернет-кошелёк для Яндекса)
- Даже если у вас безлимитный доступ, всё равно следите за траффиком - его непонятное возрастание может быть свидетельством активности вредоносной программы, а также отключайте соединение с интернетом тогда, когда оно не используется.

Источник: http://wseweb.ru/diz/obzor7.