Справочник угроз

В прошлом компьютерам угрожали преимущественно вирусы и черви. Основной целью этих программ было самораспространение; некоторые программы также причиняли вред файлам и самим компьютерам. Такие вредоносные программы - типичные проявления кибервандализма.

В чем разница между вирусом и червем?

Вирус – это саморазмножающаяся программа: она распространяется с файла на файл и с компьютера на компьютер. Кроме того, вирус может быть запрограммирован на уничтожение или повреждение данных.

Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы. Он внедряется один раз на конкретный компьютер и ищет способы распространиться далее на другие компьютеры.

Вирус заражает тем большее количество файлов, чем дольше он находится на компьютере необнаруженным. Червь создает единственную копию своего кода. В отличие от вируса, код червя самостоятелен. Другими словами, червь – это отдельный файл, в то время как вирус – это код, который внедряется в существующие файлы.

Что такое DoS- (DDoS-) атака?

DoS-атака (сетевая атака, Denial of Service – отказ в обслуживании пользователей) производится с целью срыва или затруднения нормальной работы веб-сайта, сервера или другого сетевого ресурса. Хакеры осуществляют такие атаки разными способами. Один из них – это отправка на сервер многочисленных запросов, которая может привести к затруднению или срыву работы, если ресурсов сервера окажется недостаточно для их обработки.

DDoS-атака (Distributed Denial of Service – распределенная сетевая атака) отличается от DoS-атаки тем, что запросы на атакуемый ресурс производятся с большого количества машин. Одна зараженная машина часто используется хакерами как «ведущая», и управляет атакой, производимой с других, так называемых зомби-машин.

Что такое фишинг?

Фишинг – это особый вид кибермошенничества, направленный на то, чтобы обманным путем заставить вас раскрыть персональные данные, как правило финансового характера. Мошенники создают поддельный веб-сайт, который выглядит как сайт банка (или как любой другой сайт, через который производятся финансовые операции, например eBay). Затем преступники пытаются завлечь вас на этот сайт, чтобы вы ввели на нем конфиденциальные данные, такие как логин, пароль или PIN-код. Часто для этого мошенники с помощью спама распространяют ссылку на этот сайт.

Что такое руткит?

Руткит (rootkit) – это набор программ, используемый хакерами для сокрытия своего присутствия в системе при попытках неавторизованного доступа к компьютеру. Термин пришел из Unix-систем и обозначает методы, которые авторы троянских программ, работающих под Windows, используют для маскировки вредоносной активности своих зловредов. Установленные в системе руткиты не только не видны пользователям, но и избегают обнаружения антивирусным ПО. За счет того, что многие пользователи входят в систему как администраторы, не создавая отдельной учетной записи с ограниченными правами для ежедневной работы, для злоумышленников задача внедрения руткитов упрощается.

Что такое вредоносные программы?

Понятие “вредоносные программы” (malware) объединяет все программы, создаваемые и используемые для осуществления несанкционированных и зачастую вредоносных действий. Вирусы, backdoor-программы (создаваемые для незаконного удаленного администрирования), клавиатурные шпионы, программы для кражи паролей и другие типы троянцев, макровирусы для Word и Excel, вирусы сектора загрузки, скриптовые вирусы (BAT-вирусы, windows shell-вирусы, java-вирусы и т.д.) и скриптовые троянцы, мошенническое ПО, шпионские и рекламные программы – это далеко неполный список того, что классифицируется как вредоносные программы.

Когда-то для описания всех вредоносных программ хватало понятий “вирус” и “троянец”. Однако технологии и методы заражения компьютеров с тех пор ушли вперед, и этих двух понятий стало недостаточно для описания всего существующего многообразия вредоносных программ.

Что такое троянская программа и почему она так называется?

В античной мифологии Троянский конь – это деревянная конструкция соответствующей формы, внутри которой греки проникли в Трою и таким образом смогли покорить и разрушить город. По классическому определению, троянец – это программа, которая внешне выглядит как легальный программный продукт, но при запуске совершает вредоносные действия. Троянские программы не могут распространяться сами по себе, и этим они отличаются от вирусов и червей.

Обычно троянцы скрытно устанавливаются на компьютер и выполняют вредоносные действия без ведома пользователя. Трояны разных видов составляют большую часть современных вредоносных программ; все они пишутся специально для выполнения конкретной зловредной функции. Чаще всего встречаются backdoor-троянцы (утилиты удаленного администрирования, часто включают в себя клавиатурные шпионы), троянцы-шпионы, троянцы для кражи паролей и троянцы-прокси, превращающие ваш компьютер в машину для рассылки спама.

Что такое drive-by (попутная) загрузка?

При drive-by загрузке, компьютер заражается при посещении веб-сайта, содержащего вредоносный код. Кибермошенники ищут в Интернете веб-серверы, уязвимые для взлома, чтобы вписать вредоносный код на веб-страницы (часто в виде вредоносного скрипта). Если в операционной системе или на приложениях не установлены обновления безопасности, то при посещении зараженного веб-сайта вредоносный код загружается на ваш компьютер автоматически.

Что такое клавиатурный шпион?

Клавиатурный шпион – это программа, отслеживающая нажатия кнопок на клавиатуре. При помощи нее злоумышленник может получить доступ к конфиденциальным данным (логины, пароли, номера кредитных карт, PIN-коды и т.п.) Клавиатурные шпионы часто входят в состав backdoor-троянцев.

Что такое рекламные системы (adware)?

Понятие “adware” включает в себя программы, запускающие рекламу (часто в виде всплывающих окон) или перенаправляющие поисковые запросы на рекламные веб-сайты. Рекламное ПО часто бывает встроено в бесплатные или условно-бесплатные программы и устанавливается на компьютер пользователя одновременно с основным приложением без ведома и согласия пользователя. В некоторых случаях рекламное ПО может тайно загрузить и установить на ваш компьютер троянская программа.

Устаревшие, не обновленные вовремя версии веб-браузеров могут быть уязвимыми для хакерских инструментов, скачивающих рекламные программы на ваш компьютер. Существуют также «программы-угонщики браузеров», способные менять настройки интернет-обозревателей, переадресовывать неправильно набранные или неполные URL-адреса на конкретные веб-сайты или менять заданную вами домашнюю страницу. Они также могут перенаправлять поисковые запросы на платные (часто порнографические) веб-сайты.

Рекламные программы, как правило, никак не проявляют себя в системе: их не видно в списке программ на вкладке Пуск -> Программы, нет соответствующих иконок в области уведомлений системы и в списке задач. Для них редко предусмотрена процедура деинсталляции (удаления); попытка удалить их вручную может привести к неполадкам в работе программы-носителя (в составе которой была установлена рекламная программа).

Что такое ботнеты (бот-сети)?

Ботнеты (или так называемые зомби-сети) создаются троянцами или другими специальными вредоносными программами и централизованно управляются хозяином, который получает доступ к ресурсам всех зараженных компьютеров и использует их в своих интересах.

Что такое шпионские программы?

Как следует из названия, эти программы предназначены для сбора данных и отправки их третьей стороне без вашего ведома и согласия. Такие программы могут отслеживать нажатия клавиш (клавиатурные шпионы), собирать конфиденциальную информацию (пароли, номера кредитных карт, PIN-коды и т.д.), отслеживать адреса электронной почты в почтовом ящике или особенности вашей работы в Интернете. Кроме того, шпионские программы неизбежно снижают производительность компьютера.