**Доклад по теме «Информационная безопасность»**

Сегодня огромное количество информации обрабатывают с помощью персональных или рабочих компьютеров, поэтому атаки на компьютерные системы получили большую распространенность. С каждым годом число активных пользователей Интернета растет в геометрической прогрессии, следовательно, проблема безопасности при работе в сети все более актуальна.

К сожалению, знания пользователей об основах компьютерной безопасности при использовании Интернет отстают от темпов развития сети и лавинообразного роста угроз безопасности. Как программное обеспечение может представлять угрозу информационной безопасности в сети Интернет? К таким угрозам мы можем отнести:

* вредоносное программное обеспечение (вирусы);
* интернет-мошенничество;
* атаки на отказ в обслуживании;
* кражи денежных средств; кражи персональных данных;
* несанкционированный доступ к информационным ресурсам и систем;
* распространение заведомо недостоверной информации.

Кроме того, вам уже известны основные угрозы информационной безопасности пользователя Интернета, которые идут от авторизованных пользователей и электронных методов воздействия. От авторизованных пользователей: Умышленные повреждения или похищения данных хакерами Повреждения данных в результате неосторожных действий Электронные методы воздействия: Компьютерные вирусы Спам Фишинг.

Рассмотрим влияние на безопасность со стороны различного вредоносного программного обеспечения, которое распространяется по сети Интернет. Вредоносное программное обеспечение (англ. Malware, malicious software — вредоносная программа, вредоносное) — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самого компьютера или к информационным ресурсам, которые хранятся на нем, предназначенное для несанкционированного владельцем их использования или причинение вреда (нанесение ущерба) владельцу компьютера, информации или компьютерной сети путем копирования, искажения данных, удаление или подмены информации.

Термин «вредоносная программа» (malware — это сокращение от «malicious software») с трактовкой корпорации Microsoft обычно используется как общепринятый термин для обозначения любого программного обеспечения, специально созданного для того, чтобы причинять ущерб отдельному компьютеру, серверу или компьютерной сети, независимо от того, является ли оно вирусом, шпионской программой и тому подобное. Вредоносные программы по виду нанесенного ущерба можно отнести к нескольким категориям. Вредоносные программы:

* создают помехи в работе системы;
* уменьшают ресурсы компьютера;
* выполняют несанкционированные действия с данными;
* дестабилизируют работу пользователя с компьютером.

Препятствиями в работе зараженного компьютера могут быть различные вредоносные действия: начиная от открытия-закрытия лотка CD-ROM и заканчивая уничтожением данных и поломкой аппаратного обеспечения; блокирование антивирусных сайтов, антивирусного программного обеспечения и административных функций операционной системы с целью усложнения их лечения; саботаж производственных процессов, управляемых компьютером (этим занимался известный червь Stuxnet).

Часто зараженный файл выполняет установку другого вредоносного программного обеспечения: загрузка из сети и распаковки другой, еще более вредоносной программы, либо вредоносный код уже содержится внутри файла (dropper), часто вредоносное программное обеспечение занимает почти все ресурсы компьютера.

К несанкционированным действиям с данными относят: кражу, мошенничество, вымогательство и шпионаж за пользователем.

Для кражи может применяться сканирование жесткого диска, регистрация нажатий клавиш (Keylogger) и перенаправление пользователя на поддельные сайты, в точности повторяющие исходные ресурсы; похищения данных, представляющих ценность или тайну; кража аккаунтов различных служб (электронной почты, мессенджеров, игровых серверов, платежных систем).

Аккаунты при этом применяются для рассылки спама, а через электронную почту можно заполучить пароли от других аккаунтов, в то время как виртуальное игровое имущество можно продать в MMOG (Massively multiplayer online game). Вредоносное программное обеспечение вызывает блокировку компьютера, шифрование файлов пользователя с целью шантажа и вымогательства денежных средств. Зачастую после оплаты компьютер либо не разблокируется, либо вскоре блокируется во второй раз. Вредоносная программа использует телефонный модуль для осуществления дорогостоящих звонков на платные номера, зарегистрированные злоумышленниками, что вызывает значительные суммы в телефонных счетах.

Возможно также создание платного программного обеспечения, которое имитирует, например, антивирус, но ничего полезного при этом не делает (fraudware или scareware). Вредоносные программы также выполняют другую незаконную деятельность: получение несанкционированного доступа к ресурсам самого компьютера или третьих ресурсов, доступных через него, в т.ч. прямое управление компьютером (так называемый backdoor), осуществляют организацию на компьютере открытых vpn-туннелей и общедоступных прокси-серверов.

Зараженный компьютер (в составе ботнета) может быть использован для проведения DDoS-атак, сбор адресов электронной почты и распространение спама, в т.ч. в составе ботнета. К такой деятельности относится также накручивания электронных голосований, кликов по рекламным баннерам; генерирования монет платежной системы Bitcoin, и даже использование эффекта 25-го кадра для зомбирования человека. Rootkit (руткит, от англ. Root kit, то есть «набор root’a») программа или набор программ, предназначенный для скрытия следов присутствия злоумышленника или вредоносного программного обеспечения от посторонних глаз.

Ransomware (от англ. Ransom — выкуп и software — программное обеспечение) — это вредоносное программное обеспечение, которое работает как вымогатель.

Ботнет (англ. Botnet от robot и network) — это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, которая скрыто устанавливается на компьютере жертвы и позволяет злоумышленнику выполнять определенные действия с использованием ресурсов зараженного компьютера.

Нежелательное программное обеспечение может записывать файлы, которые не являются истинно вредными, но в основном нежелательными: шутливое программное обеспечение, то есть которое делает какие-либо вещи, которые беспокоят пользователя.

Например, программа Adware показывает рекламу, а программа Spyware посылает через сеть Интернет информацию, несанкционированную пользователем. Создается так называемое «отравления» документов, дестабилизирующее программное обеспечение, которое открывает их (например, архив размером менее мегабайта может содержать многие гигабайты данных, а при его распаковке может надолго «зависнуть» архиватор, или даже переполниться жесткий диск).

Программы удаленного администрирования могут применяться как для того, чтобы дистанционно решать проблемы с компьютером, так и для вредоносных целей. Иногда вредоносное программное обеспечение для собственного «жизнеобеспечения» устанавливает дополнительные утилиты: IRC-клиенты, программные маршрутизаторы, открытые библиотеки перехвата клавиатуры.

Такое программное обеспечение не является вредным, но вместе с ним устанавливается более вредоносная программа, которая определяется антивирусами. Бывает даже, что вредоносен только скрипт из одной строки, а остальная часть программы вполне легитимна.

Классификация вредоносных программ по методу размножения: эксплойт — теоретически безвредный набор данных (например, графический файл или сетевой пакет), который некорректно воспринимается программой, которая работает с такими данными. Здесь вред наносит не один файл, а неадекватное поведение программного обеспечения с ошибкой.

Также эксплойтами называют программы для генерирования так называемых «отравленных» данных; логическая бомба в программе срабатывает при определенном условии, является неотъемлемой от полезной программы-носителя; троянская программа не имеет собственного механизма размножения; компьютерный вирус размножается в пределах компьютера и через сменные диски.

Размножение через локальную сеть возможно, если пользователь сам выложит зараженный файл в сеть. Вирусы одновременно делятся по типу файлов, которые заражаются (файловые, скриптовые, загрузочные), по способу прикрепления к файлам (паразитные, сопутствующие и перезаписывающие исходный файл) и т.д.; сетевой червь способен самостоятельно размножаться с сети. Делятся на IRC, почтовые, такие, которые размножаются с помощью эксплойтов и т.д.

Вредоносное программное обеспечение может образовывать цепочки: например, с помощью эксплойта на компьютере жертвы разворачивается загрузчик, который устанавливает из сети Интернет основное тело (программный код) червя. Подробнее о программах, заражающих компьютер можно прочитать в статье Компьютерные вирусы.

Безопасное использование публичного Wi-Fi Сегодня многие из нас пользуется Интернетом с помощью ноутбуков или смартфонов. Для удобства во многих общественных местах (кафе, барах, гостиницах, торговых центрах и даже трамваях) есть возможность воспользоваться Wi-Fi и без проблем посмотреть прогноз погоды, проверить электронную почту, или послать сообщение в социальную сеть. Однако в общедоступных Wi-Fi сетях пользователя может ожидать ряд угроз. При подключении к Wi-Fi устройства (ноутбук, планшет или смартфон) начинают передавать и получать информацию в Wi-Fi сети.

Злоумышленник, используя специальные программы, может собрать различную информацию через сеть: какие устройства подключены, есть ли общедоступные ресурсы (файлы, папки, принтеры) на подключенных устройствах, на какие сайты заходят пользователи этих устройств. Некоторые из этих программ (Zenmap, Inssider, WiFi Analyzer) можно без проблем свободно найти в Интернете.

При более серьезном подходе злоумышленники также могут получить информацию о введенных логинах и паролях. При использовании сети Wi-Fi в общественных местах нужно соблюдать следующие правила: Отключите доступ к своим данным, иначе устройство и информация на нем может стать легкой добычей для злоумышленников.

На компьютере под управлением Windows в настройке общего доступа (Панель управления / Сеть и интернет) следует выключить общий доступ к файлам, а также запретить нахождения компьютера другими пользователями сети. Используйте VPN. Безопаснее пользоваться общественным Интернетом через VPN (эта аббревиатура расшифровывается как virtual private network — частная виртуальная сеть).

VPN перенаправляет трафик через так называемую безопасную сеть, даже при подключении к бесплатному Wi-Fi. VPN будет уместным, если часто пользоваться незащищенными и публичными сетями. Сделать это можно как бесплатно, так и с использованием платных, еще более надежных, сервисов.

Последние, например, позволяют выбирать, через какие страны будет проходить трафик данных, и они не ограничивают объем и скорость передачи данных.

Нежелательно автоматически подключаться к Wi-Fi сетям. Современные ноутбуки, смартфоны и планшеты умеют автоматически подключаться к открытым Wi-Fi-точек, однако это может быть опасно. Устройство может «подцепить» сеть, созданную злоумышленниками специально для того, чтобы воровать информацию.

В большинстве современных мобильных устройств автоматическое подключение к сетям выключено по умолчанию, но лучше потратить несколько секунд, чтобы проверить это лишний раз в разделе «Настройка Wi-Fi». Используйте SSL. Многие сайты используют криптографический протокол SSL, обеспечивающий обмен данными между сервером и пользователями в зашифрованном виде. Все происходит автоматически, нужно только в настройках безопасности браузера поставить галочку напротив пункта «SSL». Обычно этот протокол включен по умолчанию, при установке браузера.

Не пренебрегайте двухэтапной (двухфакторной) аутентификацией (авторизация на сайте). Чаще всего двухэтапная аутентификация сводится к тому, что сайт просит заранее установленный пароль, а также код, присланный по SMS на введенный пользователем номер мобильного телефона. Таким образом, если кто-то украдет пароль, его одного будет недостаточно для того, чтобы использовать чужой аккаунт.

Двухступенчатая аутентификация занимает немного больше времени, может раздражать (такую ​​схему использует большинство интернет-банков. Иногда хочется ее отключить, но часто сделать это невозможно, ведь это одно из главных условий авторизации на сайте).

Важно подключить двойную проверку доступа там, где это можно сделать добровольно, например, в Google аккаунте, где связаны вместе почта, видеохостинг, документы и многие другие сервисы, которыми пользуются миллионы людей. Google предложит ввести номер мобильного и пришлет SMS-кой шестизначный код, который потребуется для того, чтобы связать аккаунт с телефоном.

Подобный код нужно вводить каждый раз дополнительно к паролю при попытке войти в учетную запись. Уточняйте название сети. Иногда мошенники могут создать сеть для кражи данных, которая по названию похожа на настоящую. Например, кроме официальной сети THOMSON можно увидеть «THOMPSON», что может быть сетью, созданной злоумышленником для кражи личных данных и несанкционированного доступа к мобильному устройству.

Если обнаруженный в кафе Wi-Fi вызывает хоть малейшее сомнение, нужно обязательно обратиться к работникам заведения и уточнять у них, как должна называться их сеть. Защищайте свои пароли. Главное и очень простое и важное правило: не устанавливать один и тот же пароль для зарегистрированных на разных сайтах аккаунтов. Также важно не лениться и придумывать сложные пароли: использовать цифры вперемешку с большими и маленькими буквами и символами. Если паролей много, то в них можно запутаться.

Для этого можно использовать менеджер паролей, вроде KeePass или LastPass. Эти программы — бесплатные, обе шифруют данные, но делают это различным образом: KeePass сохраняет зашифрованные данные на компьютере, a LastPass — на облачном сервере. У каждого из способов есть свои за и против, но в целом оба сервиса обеспечивают высокий уровень защиты. Включите «файервол» (сетевой экран). Некоторые операционные системы имеют встроенный файервол, который отслеживает входящие и исходящие интернет-соединения и предотвращает проникновения или отправку с компьютера конфиденциальных данных. Существует много программ-файерволов — как платных, так и бесплатных.

Файервол не гарантирует стопроцентную безопасность, но это полезная защитная опция, которую следует держать включенной. В Windows она включается в секции Система и безопасность (System And Security) в панели управления.