Опасности, связанные с использованием программного обеспечения

Далеко на каждая компьютерная программа полезна, и далеко не каждая программа безопасна. Существует целый класс программного обеспечения (ПО), цель которого – причинение вреда устройствам (компьютерам, планшетам, смартфонам) и кража данных пользователя.

Вирусы и вредоносное программное обеспечение

Вредоносное программное обеспечение – программы, предназначенные для несанкционированного доступа к информации или ресурсам информационной системы или воздействия на них.

Компьютерный вирус – это программа, написанная специально для причинения вреда программам и устройствам или для криминальной активности. Способна распространяться в Интернете и заражать другие устройства.

Троянская вирусная программа (троян) – это разновидность вирусов, маскирующаяся под полезные программы. Трояны позволяют решать противоправные задачи:

- хищение данных;
- внесение изменений в конфигурацию компьютера (например, для захвата устройства, создания трафика на сайте, рассылки спама).

> *Троян обязан своим названием троянскому коню. Во время осады Трои греки, видя неприступность стен города, пошли на хитрость: имитировав отступление, оставили в жертву богам у стен города статую коня. Троянцы втащили статую в город. Ночью лучшие воины греков, прятавшиеся в статуе, перебили городскую стражу и открыли ворота вернувшимся греческим отрядам. Так пала Троя.*

Руткит (Rootkit) – вредоносное ПО для получения скрытого удалённого доступа к компьютеру. Руткиты позволяют злоумышленнику удалённо управлять компьютером.

Шпионское ПО (Spyware) – программное обеспечение для сбора данных пользователя и сведений о его действиях. Данное ПО используется для сбора пользовательских паролей, реквизитов от банковских карт и прочей конфиденциальной информации.

Вирусы-вымогатели блокируют возможность работы за компьютером пользователю, как правило устанавливая на экран баннер, предлагающий пользователю заплатить злоумышленникам за разблокировку устройства. Разновидность вымогателей – **вирусы-шифровальщики.** Как следует из названия, эти вирусы шифруют содержимое жёсткого диска, предлагая за выкуп восстановить доступ к файлам.

> *Обоснование концепции компьютерных вирусов было дано одним из создателей информатики как науки Джоном фон Нейманом, рассмотревшим возможность существования машины, которая могла бы повреждать машину-носитель, производить собственные копии и заражать другие машины.*
>
> *Теория превратилась в практику в 1971г. – это была программа Greeper, созданная для проверки возможности существования самовоспроизводящейся программы и не выполнявшая каких-либо вредных функций.*
>
> *Первый вирус в полном смысле слова появился в 1974г. – программа Rabbit (она же Wabbit) не только умела самовоспроизводиться, но и изначально была создана с вредоносной целью. Огромное количество копий вируса замедляло работу компьютера и в конечном счёте приводило к отказу всей системы.*

В следующем году появился первый троян – он не преследовал какие-либо опасные цели, но умел всё, что положено уметь трояну: прятаться внутри других программ и выполнять действия без ведома и разрешения пользователя.

Первая глобальная эпидемия компьютерного вируса произошла в 1986г. – это был вирус Brain, заражавший загрузочный сектор дискет. Изначально созданный для отслеживания нелегального распространения ПО, вирус быстро вышел из-под контроля.

С развитием цифровой среды и распространением доступа в Интернет вирусам и вредоносному ПО перестали требоваться физические носители, а количество «точек контроля» (т.е. действий пользователя, при каждом из которых он мог бы заметить что-то неладное и вмешаться) сильно уменьшилось. Начались эпидемии компьютерных вирусов. Одновременно с этим произошла окончательная криминализация: наибольшая часть вирусов и вредоносного ПО создаётся не для того, чтобы навредить «из любви к искусству», а для атак на компании и для вымогательства и кражи денег, данных пользователей.

В настоящий момент создание вредоносных программ во многом автоматизировано, постоянно, в большом количестве появляются и новые разновидности, и мутации старых вирусов.

Как вирусы и вредоносное программное обеспечение проникают на пользовательские устройства?

Для выполнения своей «боевой задачи» вирусу или вредоносной программе необходимо попасть на устройство жертвы. В арсенале злоумышленников есть много способов «доставки», однако все эти способы можно разделить на две основные категории в зависимости от того, какая уязвимость используется – психологическая или технологическая.

1. Социальная инженерия: злоумышленник при помощи манипуляций и психологического давления заставляет пользователя запустить инфицированный файл или перейти по опасной ссылке.
2. Технические приёмы, незаметные для жертвы: использование уязвимостей операционных систем и оборудования (включая как компоненты самого устройства, например процессор, так и сетевое оборудование – немалое количество вирусных атак производится с использование «брешей» в ПО роутеров), антивирусного ПО и отдельных распространённых программ и приложений.

На практике эти способы используются одновременно, и человеческий фактор (см. п.1) является одной из главных уязвимостей, которыми пользуются злоумышленники.

Зачем это нужно?

В основе деятельности авторов и распространителей вирусов и вредоносных программ – полулегальное или откровенно криминальное получение дохода. Это может быть:

- установка программ для принудительного просмотра рекламы. Чаще всего таким видом вирусов заражаются браузеры, начиная после этого открывать всплывающие окна с рекламными объявлениями при посещениях интернет-страниц;
- «зомбирование» заражённого устройства и создание ботнетов – сетей из захваченных машин с предоставлением злоумышленнику возможности управления этой сетью. Чаще всего ботнеты используются для рассылки спама и для использования захваченного, «зомбированного» компьютера как дополнительного оборудования для майнинга криптовалют;

► кража личной информации и персональных данных (паролей, от различных интернет-сервисов, регистрационных данных программных продуктов, ФИО, адресов, номеров телефонов и т.д.);
► кража банковской информации;
► кража электронных денег.

Вирусные атаки могут быть ориентированы не только на конечных пользователей: они могут быть организованы в том числе для вывода из строя важных инфраструктурных объектов (электростанций, заводов и пр.). Порой подобные атаки могут иметь политический подтекст, например взлом почты известного политика.

Как обезопасить себя от вредоносного программного обеспечения?

Основное правило: используйте антивирусное программное обеспечение, регулярно обновляйте антивирусные базы и саму программу (все современные антивирусные программы имеют функцию автоматического обновления, убедитесь, что она включена и программа установила актуальные обновления).

При работе с приложениями и программами:

► скачивайте только те программы, приложения и файлы, которые вам действительно нужны;
► скачивайте только проверенные программы, приложения, файлы и только из надёжных источников. Под надёжными источниками мы понимаем официальные сайты производителей ПО или специализированные торговые площадки в Интернете с многолетним опытом работы и подтверждённой репутацией;
► не скачивайте ПО из сомнительных источников, не связанных с производителем программного обеспечения. как правило, практически любое ПО или игра, скачанные из подобных источников, содержат в себе вредоносный код. Это один из самых популярных способов распространения вредоносного ПО.

Примените рискориентированный подход

1. При установке программ:
► с подозрением относитесь к предложениям «улучшить» или «расширить» функционал распространённых и популярных программ. Соглашаясь на них, вы рискуете: подобные «улучшатели», используя популярность чужого бренда, либо окажутся пустышкой, либо попытаются внедрить в ваше устройство вредоносный код;
► обновляйте операционную систему (ОС) – разработчики ОС, в зависимости от семейства ОС, каждую неделю выпускают обновления, в том числе направленные на устранение уязвимостей ОС;
► если при установке программное обеспечение требует внести какие-то изменения в системные файлы операционной системы, то лучше не устанавливать эту программу;
► следите за разрешениями, которые запрашивает программа при установке. Чем больше разрешений запрашивается и чем меньше они относятся к ожидаемому функционалу, том больше причин не устанавливать её. Например, приложению для работы с архивированными файлами вряд ли нужен доступ к камере, а фонарику – к адресной книге.

2. При посещениях интернет-страниц:
► в настройках всех браузеров включите функцию переходя на веб-страницы, поддерживающие протокол https. Этот протокол позволяет в шифрованном виде

передавать данные между вашим компьютером и сервисом (сайтом) и таки образом защищает вас от перехвата вашего интернет-трафика. Кроме того, в современные браузеры уже встроены функции повышенной защиты от типовых угроз, поэтому обязательно выбирайте опцию максимальной защиты;

- будьте аккуратны с вашим аккаунтом для синхронизации в браузере. Если злоумышленник получит доступ к вашему аккаунту, то ему будут доступны все синхронизируемые данные. Поэтому рекомендуем либо убирать из синхронизации сохранённые логины и пароли, либо включать двухфакторную аутентификацию для входа в аккаунт;

> ***Двухфакторная аутентификация пользователя*** *– дополнительный способ защиты аккаунта от взлома, при котором производится не только стандартная проверка прав доступа (проще говоря, указание логина и пароля для доступа к сайту или сервису), но и запрашивается подтверждение: в самом ли деле доступ стремится получить именно тот пользователь, который имеет на это право? На практике это выглядит как требование ввода одноразового кода, отправляемого по электронной почте или SMS.*

- в настройке браузера необходимо отключить доступ к камере, микрофону, всплывающим окнам и геоданным;
- по возможности выбирайте программные и сервисные решения, которые работают в браузере и не требуют установки на компьютер (например, Яндекс.Телемост);
- устанавливайте расширения браузера для блокирования рекламы. Злоумышленники могут встроить в рекламный баннер код перехода на поддельный сайт или инициировать загрузку вредоносного файла;
- обращайте внимание на уведомления: большинство современных браузеров уведомляет о попытке перейти на сайт, внесённый в чёрные списки. При посещении такой сайт сможет установить вредоносную программу;
- избегайте подписки на push-уведомления сайтов в браузерах (это наделит владельцев этих сайтов обширными возможностями внедрения вредоносного кода).

3. При работе с электронной почтой:

- не открывайте письма, попавшую в папку «Спам», кроме тех случаев, когда почтовый сервер ошибочно пометил туда письмо от известного вам отправителя. Вероятность такой ошибки мала: современные антиспам-фильтры имеют довольно высокую точность;
- не открывайте вложения в письмах от неизвестных вам отправителей. Скорее всего, эти вложения заражены вредоносным кодом, активирующимся при попытке открытия;
- не загружайте картинки из писем от неизвестных отправителей. В них может быть и следящий пиксель, по данным которого авторы письма пометят ваше устройство как активную цель, а может быть и вредоносный исполняемый код;
- не переходите по ссылкам в письмах от неизвестных отправителей и в рекламных рассылках. В лучшем случае такой переход увеличит поток спама в вашу почту, в худшем – активирует механизм установки вредоносного кода;
- не открывайте архивы, прилагающиеся к письмам. «Упаковка» вируса в архив – стандартный способ обойти сканирование антивирусной программой. Часто вирус захватывает почтовую программу и рассылает архив со своей копией по всей адресной книге владельца заражённого устройства. Открытие подобного архива, по сути, означает самостоятельный запуск установки вируса. Если такое письмо отправлено известным

вам человеком, уточните у него, на самом ли деле он отправлял вам этот архив и что в нём находится;

► лучше всего вообще не открывать приложения от неизвестных отправителей.

4. Для мобильных устройств есть несколько дополнительных правил, связанных со спецификой мобильных платформ:

► избегайте установки приложений, требующих заведомо больше прав и разрешений, чем необходимо для их работы;

► проверьте права уже установленных приложений и при необходимости отмените разрешение излишних прав доступа;

► не загружайте сообщения MMS, присланные с неизвестного номера.

Пароли

1. Обязательно устанавливайте пароли на все свои цифровые устройства.
2. Проводите собственный аудит паролей от всех почт, аккаунтов и сервисов хотя бы раз в несколько месяцев – проверяйте, достаточно ли они сложны, не используется ли один и тот же пароль в разных учётных записях. Проверить данные своих аккаунтов на утечку можно при помощи службы строенной функции браузера, например в браузере Яндекс нужно открыть меню (три горизонтальные полоски в правом верхнем углу), выбрать «Пароли и карты» и запустить «Проверка паролей».
3. Оптимальный вариант – использовать специализированное приложение для хранения всех паролей (например, Kaspersky Password Manager). База данных таких приложений, как правило, тоже шифруется, что обеспечивает дополнительную сохранность паролей.
4. По возможности проверяйте новости специализированных ИТ-сайтов об утечках данных – это позволит вам выиграть время на смену пароля, пока злоумышленники не воспользуются вашими украденными данными.
5. Создавайте уникальные и сложные пароли, не включающие распространённые слова или числа. Не используйте в паролях телефонные номера, даты дней рождений, имена родных, клички домашних животных, обычные слова (их легко автоматически подобрать по словарю).
6. Никогда не записывайте пароли в текстовый файл, хранимый на компьютере или смартфоне, - его может найти и украсть вирус.
7. Используйте двухфакторную аутентификацию.
8. Не используйте очевидные проверочные вопросы для смены или восстановления забытого пароля.
9. Не используйте набор русских слов во включённом латинском регистре (русских букв может не оказаться на клавиатуре чужого компьютера, например во время путешествия).

Фишинг

Фишинг *– это использование поддельных писем и сайтов для получения конфиденциальных данных пользователя. Объектом атаки при фишинге является не устройство, а сам пользователь, поэтому главным элементом защиты будет разумная осторожность, внимательность и критичное отношение к входящим сообщениям.*

Фишинг может быть не только компьютерный, но и телефонный; так, распространённые звонки от «служб безопасности банка» также являются фишингом, цель которого – завладеть реквизитами банковской карты жертвы и украсть деньги со счёта.

Как обезопасить документы и банковские карты?

1. Не переходите по ссылкам и не заполняйте формы, в которых необходимо указывать личные данные. Если вам надо выполнить какие-либо операции с банковской картой, сделайте это самостоятельно с помощью официального сайта банка.
2. Номер и пин-код банковской карты, логины и пароли от личных кабинетов должны знать только вы и на всякий случай ваши родители (на письма, сообщения или звонки с просьбой уточнить /перепроверить/ подтвердить личные данные отвечайте отказом, а о поступившем предложении сообщите взрослым).
3. Не разрешайте фотографировать ваши документы и банковские карты; если кто-то пытался это сделать, сообщите об этом взрослым.
4. Если вам на почту или в мессенджер пришло письмо или сообщение от имени финансового учреждения с просьбой перейти по определённой ссылке и заполнить некую форму, перенаправьте это письмо в службу безопасности финансового учреждения (как правило, контакты таких учреждений находятся в открытом доступе); таким образом вы поможете предотвратить мошеннические действия.
5. Не храните финансовые данные и сканы документов на компьютере (лучше сохраните их на отдельную флешку или внешний диск) и обращайтесь к ним по необходимости. Однако если такой возможности нет, то лучше использовать ПО для создания надёжных шифрованных папок с личными данными, например Kaspersky Password Manager.
6. Не присылайте своим друзьям и знакомым фото своего паспорта, банковских карт и прочих документов – нет никаких гарантий, что получатель будет столь бережно относиться к сохранности этих данных, как вы (или что эти данные не будут выкрадены уже с его устройства).

Чтобы обезопаситься от **фишинговых звонков,** надо выполнять следующие правила:

- с недоверием относится к звонкам с неизвестных номеров;
- не поддерживать разговоры с незнакомцами, кем бы они ни представлялись;
- не перезванивать на пропущенные звонки с неизвестных номеров. С большой вероятностью это спамеры или мошенники;
- не отвечать на задаваемые незнакомцами вопросы и не предоставлять личные данные – имя, фамилию, адрес и т.д.;
- использовать специальные приложения – определители номера. Эти приложения ведут собственные базы спамеров, мошенников и нежелательных звонков. Подобные приложения требуют разрешения на доступ к телефонной книге, поэтому нельзя использовать определители номера от малоизвестных или совсем неизвестных производителей. Для защиты достаточно продуктов от Яндекса, лаборатории Касперского и 2ГИС. А вот от использования приложений, обещающих показать, как вы записаны у других пользователей (например, GetContakt), стоит воздержаться – сама суть подобных приложений опасна: предполагает «выкачивание» вашей адресной книги, хранение её внешних серверах и сравнение с адресными книгами других пользователей;
- иметь семейные пароли (проверочное слово или словосочетание, известное только членам семьи). Это может пригодиться не только для проверки звонящих под видом знакомых, но и для рискованных ситуаций общения с незнакомцами на улице или в общественных местах;
- одна из самых главных и одновременно непростых рекомендаций – подключение отдельного телефонного номера для банковских приложений. В идеале SIM-карта, привязанная к этому номеру, должна быть установлена в телефон, не

поддерживающий установку каких-либо приложений. В этом случае никто, кроме вас и родителей, не будет знать этот номер, привязанный к вашей банковской карте. А следовательно, любой звонок не от банка автоматически можно воспринимать как спам.

Спам

> ***Спам*** *– это не запрошенные массовые анонимные рассылки электронных писем, SMS-сообщений в мессенджерах. Содержание спама может быть различно – от непрошеной рекламы, до уже рассмотренных фишинговых писем.*

Большая часть спама уничтожается спам-фильтрами почтовых служб, но некоторая доля проходит через фильтры и попадает во «Входящие». Это происходит потому, что инструментарий спамеров, как и вирусописателей, постоянно совершенствуется, сами спам-письма всё больше маскируются под личную и деловую переписку.

Наиболее распространённая цель спама – заставить получателя совершить переход по ссылке в фишинговом письме, используя социальную инженерию

Большинство спам-писем содержит следящий пиксель, срабатывающий при открытии письма и уведомляющий спамера о том, что почтовый ящик активен, письма в нём читаются.

Несмотря на то, что в целях мимикрии большая часть спам-писем содержит ссылку «Отписаться», пользоваться ею нельзя – переход по такой ссылке передаст спамерам много личной информации о вас (от самого факта открытия письма до индивидуальных настроек браузера и т.д.) и не приведёт к уменьшению потока спама – на «той стороне» нет живых людей, есть автоматизированный сервер рассылок, уже пометивший вас как «живую» цель.

Советы по управлению аккаунтами в социальных сетях/сервисах и др.

1. Заведите себе отдельные почтовые ящики для регистрации на разных площадках:
   - ► в социальных сетях;
   - ► для получения банковских рассылок;
   - ► на игровых платформах и т.д.;
   - ► на маркетплейсах.

Таким образом вы будете заранее насторожены, если на почту, предназначенную только для банковских рассылок, придёт письмо, что вам кто-то написал в социальной сети.

2. Для учебных целей и общения с одноклассниками должна быть создана отдельная почта: используйте только её, не делитесь без необходимости другими своими почтовыми ящиками.

3. Каждый свой аккаунт необходимо ограничить для просмотра другими пользователями. Добавляйте только тех пользователей, с которыми вы действительно знакомы.

4. Указывайте как можно меньше персональных данных в своих аккаунтах. Очень часто злоумышленники используют указанные в социальных сетях персональные данные, чтобы убедить вас в том, что это действительно сотрудник, например банка, ведь только у него могут быть такие сведения.

Литература:

Основы безопасности жизнедеятельности: базовый уровень: учебное пособие для образовательных организаций, реализующих образовательные программы среднего профессионального образования: в 2 частях/ под ред. Ю.С.Шойгу. – Москва: Просвещение, 2024. – (Учебник СПО).

Ч.2. Модуль 8. Безопасность в информационном пространстве. Тема 2. Опасности, связанные с использованием программного обеспечения. с 117.