Чернов А.Ю, Клочков Д.А.
Интернет-угрозы и способы защиты от них

doi: 10.18411/lj-04-2019-262

idsp: ljournal-04-2019-262

Научный руководитель: Ермолаева В.В

Аннотация

В данном тексте поднимаются самые основные угрозы, на которые может наткнуться обычный пользователь сети интернет и компьютера в частности

Ключевые слова: вирусы, интернет, вредоносные программы, технические угрозы, социальная инженерия, черви, Трояны, DDoS атаки, фишинг, способы защиты в интернете

Abstract

This text raises the most basic threats that may come across an ordinary user of the Internet and computer in particular

Keywords: viruses, Internet, malware, technical threats, social engineering, worms, Trojans, DDoS attacks, phishing, methods of protection on the Internet

Сейчас уже сложно представить человека без компьютера и интернета, каждый день человек делает покупки в сети интернет, общается с родными и друзьями, листает новостную ленту и даже работает, не вставая с дивана, но не задумывается о том, что ежедневно компьютер, телефон, планшетный компьютер подвергается угрозам. Важные Документы, фотографии, переписки и личные данные — вся эта информация может исчезнуть в один клик из-за очередного вируса. Сеть интернет является огромным складом информации. Интернет предлагает огромные возможности для обучения, работы и отдыха и в то же время это огромная база данных, пополняемая каждую секунду, которая содержит полезную информацию для хакеров и других мошенников. Существует множество видов угроз, но два основных вида, которым могут подвергаться обычные пользователи сети это социальная инженерия (получение информации путем обмана) и технические (с помощью различных вредоносных программ). Вредоносные программы с каждым днем становятся все продуманнее и с более сложным кодом. Самые лучшие варианты программ — это хорошо скрытые для простого человека и способные обмануть даже самую современную и защищенную систему. Сейчас можно встретить огромные системы с большим количеством модулей, в которой каждый отвечает за свою задачу. Например, первый модуль проникает в систему и взламывает ее, второй модуль закрепляется в ней и загружает еще модули, которые уже делают то, что задумал владелец данного программного обеспечения.

Задача вредоносных программ — это нанести повреждения вашему компьютеру, сети интернет или просто украсть ваши данные. Существуют вирусы, которые могут удалить информацию, хранящуюся на любом диске, тормозить или прекратить совсем работу вашего устройства. Вредоносные программы чаще всего «скрываются» в письмах или сообщениях с "интересными" предложениями от незнакомых людей, в страницах различных новостных или других популярных сайтов, которые содержат те или иные недочеты. Пользователь заходит на сайт чтобы получить нужную информацию, а вредоносные программы в этот момент проникают на компьютер, пользователь даже не подозревает об этом.

Рассмотрим основные виды Технических угроз для обычного пользователя — Компьютерные вирусы, черви, трояны, Ddos атаки.

Компьютерные вирусы

Компьютерный вирус —

один из самых опасных видов ПО, распространяется по компьютеру путем попадания своей копии в другие программы. Получается, что вирус становится частью программы

, которую он заразил. Вирус передается от одного компьютера к другому, заражая все устройства на своем пути. Это может быть как легкое подвисание устройства, как и полная потеря данных и прекращение работы компьютера. Чаще всего вирус существует в системе, но он не может распространяться,

пока человек не запустит зараженную программу. Во время основной работы программы так же выполняется работа вируса, который перезаписывает код других программ уже своим зараженным кодом, что делает программу неисправной.

Так же вирусы могут передаваться от одного компьютера к другому, используя сеть или флеш-накопитель

Черви

Компьютерные черви очень схожи с вирусами, потому что они делают свои копии в рабочие программы и вызывают такие же повреждения. Самое главное отличие червей от вирусов это то, что вирус требует распространения, а червь делает это в автономном режиме и не требует вмешательства человека. Чтобы распространяться в системе черви используют или уязвимости системы, или обман человека, для запуска. Червь попадает в компьютер через уязвимости в системе, это позволяет перемещаться ему по устройству без помощи человека.

Черви -

это один из самых опасных классов ПО с точки зрения проникновения в компьютер, потому что для перемещения червей по компьютеру не требуется вмешательство человека. Например, если подключить флеш-накопитель к компьютеру зараженному червем, он самостоятельно распространится и заразит другие программы.

Трояны

Троян (trojan)

еще один тип вредоносного ПО, который назвали в честь большого коня из дерева, который древние греки использовали для проникновения на территорию противника. Пользователь путем обмана самостоятельно загружает его и это выглядит как запуск какой-то программы, которую искал пользователь. Файл может быть замаскирован под видео или изображение. Троян может отображаться как video.avi, а на деле это будет video.avi.exe. Часто троян имеет иконку проигрывателя видео дорожек, это сбивает владельца компьютера и он по невнимательности запускает файл.

После запуска, он может использовать различные функции компьютера: открывать файлы и программы, изменять вид рабочего стола, удалять и воровать данные, так же распространять другие вирусы. В последние годы большой популярностью пользуются трояны-

винлокеры, которые блокирующие рабочий стол компьютера с целью вымогательства денег у пользователя.

DDoS атаки

DDoS-атака –

это атака, которая приводит сервер к сбоям или полной остановке работы компьютера из-за огромного количества запросов, с огромной скоростью.

Суть DDoS-

атаки в том, что мошенник пытается временно отключить определенный сервер, перегрузить сеть или процессор. Цель DDoS атаки –

это выведение компьютера из работы, чтобы пользователь временно не имел доступа к информации. DDoS атака может воздействовать на такие ресурсы как: память компьютера, сетевые ресурсы и т.д

Осуществить DDoS-атаку можно несколькими способами.

В первом случае используются недочеты отдельных программ, которые установлены на компьютере. Эти уязвимости позволяют вызвать ошибку системы.

Во втором случае атака происходит при помощи массовой рассылки пакетов информации на компьютер, это вызывает перегрузку сети и появление ошибок.

Для данной атаки злоумышленники используют сеть компьютеров зараженных вирусом. Каждым компьютером злоумышленник управляет удаленно, владелец даже не подозревает об этом. При помощи вируса на компьютер-жертву незаметно устанавливается зараженный программный код, который антивирус не может найти и работает не мешая пользователю. В нужный момент по команде программа активируется и начинает отправлять большое количество запросов на атакуемый сервер или компьютер, в результате сервер перегружается и перестает работать.

Социальная инженерия

Фишинг

Фишинг один из самых популярных способов атаки на пользователей, это один из методов социальной инженерии. Цель фишинга – получить личную информацию пользователя. Например номер кредитной карты, логин и пароль от социальной сети, путем поддельных страниц в интернете. Самый распространенный метод фишинга это : на электронную почту приходит сообщение от вашего банка, что срочно требуется вход. Текст письма обычно провоцирует пользователя сразу выполнить действия из письма. Но даже если информация кажется надёжной, следует связаться со службой поддержки и уточнить у них все, чтобы не попасться на уловки мошенников. В письме находится ссылка на сайт, который полностью копирует настоящий сайт банка. После ввода данных на этом сайте мошенник сразу же получает их. И как только он получает данные для входа, он может, использовать их в своих целях, например, вывести деньги с счета или расплатиться в каком нибудь интернет магазине, или создать копию пластиковой карты и снять деньги в любой точке мира.

Большинство мошенников пользуется не только технологиями, но и человеческой невнимательностью или слабостью, используя для этого социальную инженерию. Это термин подразумевает получение информации путем обмана или хитрости, без использования вредоносных программ. Специалисты используют психологические методы воздействия на человека через социальные сети, почту или мессенджеры . В результате чего, человек самостоятельно раскрывает всю нужную информацию не подозревая этого

Сообщения от мошенников чаще всего содержат смс с угрозами, например они могут обещать огромный выигрыш с минимальными вложениями, а то и вовсе без них . Так же могут приходить сообщения от банков и социальных сетей с текстом : «Ваш аккаунт заблокирован. Чтобы получить доступ и разморозить аккаунт, необходимо подтвердить свои личные данные: это номер телефона, электронную почту и пароль. После того как жертва отправляет свои данные, мошенники начинают шантажировать жертву и вымогать деньги.

Так же злоумышленники используют личную информацию (фото, видео, переписки) личного характера для вымогательства денежных средств, шантажируют распространить полученную информацию в сети интернет.

Например вы заходите в свой профиль Вконтакте или другой сети и видите сообщение от незнакомого человека, который пишет вам о том, что на ваша страница была взломана и у вымогателя есть ваши фотографии интимного характера. Чтобы фотографии не были разосланы по всем друзьям, вы должны отправить на веб-кошелек некоторую сумму денег. На таких вымогателей чаще всего попадают девушки, которые в свое время записывали «домашнее видео» или делала фотографии интимного характера .

Способы защиты в интернете.

Будьте осторожны и бдительны в интернете в Интернете

Если ваш телефон или компьютер подвергся заражению, то скорее всего вскоре произойдет кража информации. Либо информация может просто удалиться . Основным способом защиты в данном случае - это хороший антивирус.

Лучшие антивирусы на сегодняшний день это:

- Kaspersky
- Avast
- 360 Total Security

К тому же их можно установить совершенно бесплатно!

Антивирус Касперского на данный момент является одним из лучших антивирусов на рынке, по исследованиям. На втором месте идет простой и бесплатный антивирус Avast. Для любителей все настроить под себя подойдет 360 Total Security. Последний антивирус имеет сложную настройку, поэтому не подойдет для новичков.

Если есть финансовые возможности, то можно оплатить платную версию антивируса с дополнительной защитой от кражи личной информации.

Чтобы избежать фишинговых атак в интернете:

Не оставляйте почту и номер телефона в открытом доступе на сайтах и в комментариях.

Не отвечайте на спам, а лучше сразу добавляйте в черный список такие сообщения.

Чтобы не попасться на мошенничество с банковскими картами нужно соблюдать эти правила:

Нельзя сообщать незнакомым людям информацию, размещенную на вашей карте.

Чтобы совершить оплату, достаточно номера карты и фамилии или номера телефона к которому привязана карта.

В случае, если вы заметили подозрительные действия, которые происходят с вашей картой, немедленно обратитесь в поддержку и заблокируйте карту.

Чтобы избежать попадания вирусов на ваше устройство загружайте файлы только из проверенных источников.

Остерегайтесь подозрительных ссылок на форумах, в социальных сетях и на досках объявлений.

Так же будьте внимательны на сайтах социальных сетей

Facebook, Twitter, ВКонтакте и другие социальные сети чаще всего используют злоумышленники. Бывает, что опасные сообщения приходят от друзей и знакомых. Если вы видите подозрительное сообщение от друга, свяжитесь с ним и убедитесь, что это именно его ссылка, или просьба. Не переходите по ссылкам, пока не убедитесь, что это безопасно.

1. <https://safe-surf.ru/users-of/article/212/>
2. <https://moluch.ru/archive/91/19771/>
3. <https://camafon.ru/internet>
4. <https://lifehacker.ru/10-luchshix-antivirusov/>

Юдин А.О.¹, Козырева Л.В.²

Способы повышения экологической безопасности автотранспортных потоков с использованием имитационного моделирования

¹ФГБОУ ВО «Национальный исследовательский Московский государственный строительный университет»
(Россия, г. Москва)

²ФГБОУ ВО «Тверской государственный технический университет»
(Россия, Тверь)

doi: 10.18411/lj-04-2019-263

idsp: ljjournal-04-2019-263

Аннотация

В статье рассмотрены способы повышения экологической безопасности автотранспортных потоков посредством применения метода имитационного моделирования. На основе исследований разработаны мероприятия планировочного и организационно-технического характера, которые повышают экологическую безопасность дорожного движения. Полученные результаты могут быть использованы для решения комплекса научных и практических задач по организации дорожного