4. Elena Doynikova, Igor Kotenko. Approach for determination of cyber attack goals based on the ontology of security metrics // Proceedings of the International Workshop "Advanced Technologies in Aerospace, Mechanical and Automation Engineering" (MIST: Aerospace-2018). October 20, 2018, Krasnoyarsk, Russia. IOP Conference Series: Materials Science and Engineering (MSE), IOP Publishing, Vol.450. 2018. 7 p. <https://doi.org/10.1088/1757-899X/450/5/052006>.
5. Common Weakness Enumeration schema. Режим доступа: <https://cwe.mitre.org/documents/schema/> (дата доступа: 12.10.2019).
6. Elena Doynikova, Andrey Fedorchenko and Igor Kotenko. Ontology of metrics for cyber security assessment // Proceedings of the 14th International Conference on Availability, Reliability and Security. August 26–29, 2019, Canterbury, United Kingdom. ACM, New York, NY, USA, 8 p. <https://doi.org/10.1145/3339252.3341496>.

Ермолаева В.В., Москвин А.С., Бредихин В.М.
Угрозы "всемирной паутины"

*Саратовский Государственный технический университет имени Ю.А.Гагарина
(Россия, Саратов)*

doi: 10.18411/lj-11-2019-34

idsp: ljjournal-11-2019-34

Аннотация

В наши дни интернет является неотъемлемой частью быта людей. Огромное количество людей ежеминутно заходят во «Всемирную паутину», дабы узнать о самых свежих новостях из разных новостных сайтов. Для людей, чья деятельность, так или иначе, связана с компьютером и информационными технологиями, Интернет является одним из основных источников дохода. Для большинства учащихся, в частности, школьников и студентов, это источник неисчерпаемого количества знаний и информации, возможность весело провести время и отдохнуть, играя в игры с друзьями, возможность удовлетворения потребности в общении посредством использования социальных сетей. Таким образом, каждый человек, который регулярно использует Интернет, может столкнуться с рядом угроз. Основными видами интернет – угроз являются социальная инженерия и технические угрозы. Самыми распространёнными техническими угрозами для нас, это вредоносные программы, DoS и ботнеты и DDoS-атаки. Эти программы выводят из строя ПК, сервер или компьютерную сеть. Такие программы могут удалять, изменять или красть наши данные компьютера, безусловно, это чревато плохими последствиями для дальнейшей работы компьютера. Вредоносные программы в большинстве случаев находятся на различных новостных сайтах и подобных популярных ресурсах, незаметно устанавливаются на компьютер пользователя, использующего данный сайт. Различные портативные носители данных, такие как USB или CD также могут быть источниками и распространителями вредоносных (вирусных) программ, а скачанные с Интернета файлы, необходимо проверять с помощью специальных программ, разработанных для поиска и уничтожения вредоносных программ. Все вирусные программы можно подразделить на троянские программы, черви и вирусы.

Ключевые слова: Сетевой червь, ботнет, компьютерный вирус, троянская программа, социальная инженерия, фишинг, DoS.

Abstract

Nowadays, the Internet is an integral part of people's lives. A huge number of people every minute go to the World Wide Web in order to learn about the latest news from various news sites. For people whose activities, one way or another, are connected with computers and information technologies, the Internet is one of the main sources of income. For most students, in particular, schoolchildren and students, this is a source of an inexhaustible amount of knowledge and information, the opportunity to have fun and relax, playing games with

friends, the ability to satisfy the need for communication through the use of social networks. Thus, each person who regularly uses the Internet can face a number of threats. The main types of Internet threats are social engineering and technical threats. The most common technical threats for us are malware, DoS and botnets, and DDoS attacks. These programs disable a PC, server, or computer network. Such programs can delete, modify or steal our computer data, of course, this is fraught with bad consequences for the further operation of the computer. Malicious programs in most cases are located on various news sites and similar popular resources, and they are quietly installed on the computer of the user using this site. Various portable storage media, such as USB or CD, can also be sources and distributors of malicious (virus) programs, and files downloaded from the Internet must be checked with the help of special programs designed to search for and destroy malicious programs. All virus programs can be divided into trojans, worms and viruses.

Keywords: Network worm, botnet, computer virus, trojan, social engineering, phishing, DoS.

Компьютерный вирус—это один из множества видов вирусных ПО, который может производить свои копии и попадать в коды других программ, загрузочные отделы, пользовательские области памяти, а также распространять свои копии по различным каналам связи с целью нарушения работы программного комплексов, изменению файлов, приведения в неисправность структур размещения данных, ограничению доступа пользователей или же приведения в негодность технических составляющих компьютера.

Рис. 1. Диаграмма. Тенденция роста Интернет-угроз (апрель 2017) (Источник: КЦ RU РФ)

Хранящийся на диске вирус не опасен, но лишь до тех пор, пока его не открыть. Он активизируется только в случаях, когда человек сам его запускает. Вирусы разработаны с целью копирования, заражения компьютеров, что обычно сопровождается уничтожением данных. Компьютерные вирусы названы вирусами, так как они способны, словно биологические вирусы, самопроизвольно размножаться в теле хозяина, только для компьютерных вирусов этим телом является операционная система.

Топ-10 самых знаменитых компьютерных вирусов : «Storm», «Sasser», «Nimda», «Melissa», вирусы семейства «Code Red», «Morris», «ILOVEYOU», «Brain», «Conficker», «Elk».

Сетевой червь — это один из видов вредоносных программ, самостоятельно распространяющейся через домашние и глобальные компьютерные сети. **Троянская вирус** — разновидность вредоносной программы, попадающая в компьютер (ПК) под видом легального программного обеспечения, контролируемая человеком. «Трояны» — самый простой вид вирусам, сложность которых зависит исключительно от сложности истинной задачи и средств маскировки. Самые простые «трояны» (например, способные стереть уничтожить личные данные) могут иметь очень короткий исходный код. Примеры троянских программ: TDL-4, Back Orifice, Pinch, Winlock.

Зачастую злоумышленники заражают ПК ради того, чтобы сделать его частью **ботнета** — единой сети из зараженных устройств во всех точках мира.

Ботнет представляет из себя сеть компьютеров, заражённых вредоносным программным обеспечением, которое даёт злоумышленникам возможность удалённого контроля за ними, рассылки разного рода спама, вирусов, осуществления DDoS-атаки. Все эти действия могут происходить без ведома хозяев ПК. Современные боты могут распространяться, как черви, скрываясь от ОС. Одна из самых серьёзных проблем ботнета, что при создании ботов работают несколько человек, то есть появляются несколько вариантов одного и того же бота. Это существенно затрудняет их распознавание антивирусными программами.

Рис. 2. Схема работы ботнета

DoS и DDoS-атаки

DoS — атака злоумышленников на систему направленная на выведение её из работы. Чаще всего с помощью данного действия производится финансовое давление: обычной службы, приносящей прибыль, счета от провайдера и меры по уходу от атаки ощутимо бьют «цель» по карману. В настоящий момент DoS и DDoS-атаки наиболее популярны, ведь они могут довести до отказа практически любую систему, не оставляя юридически значимых улик. Для атаки используется незащищённость программного обеспечения, используемого на ПК пользователя. С помощью уязвимости вызывается определенная критическая ошибка, ведущая к нарушению работоспособности системы.

Существует второй способ, при котором атака производится с использованием одновременной отсылки большого количества пакетов информации на ПК «жертвы», что приводит к сбою сети.

Рис. 3. Статистика DoS-атак за 2018 год

DDoS-атака — это вид DoS-атаки, организованной несколькими компьютерами, что позволяет вывести из строя большую сеть.

Для DDoS-атак хакер применяет ботнет — организованная сеть устройств, с пред загруженным специальным вирусом. Хакер может управлять устройством удаленно из любой точки мира, без ведома пользователя. При использовании вредоносной программы, создающей вид легального софта, на ПК - пользователя загружается вирус, который не распознается систем как угроза и работает незаметно для пользователя (фоновом режиме). По команде хакера вирус активируется и начинает делать запросы на сервер жертвы, по итогу канал связи перегружается, и провайдером и сервер выходят из строя.

Социальная инженерия — способ несанкционированного доступа к данным, полагающийся на человеческий фактор. Задачей таких хакеров, как и у обычных злоумышленников и взломщиков, взлом доступа к данным для кражи персональных данных. Все методики и технологии социальных инженеров предполагают использовании человеческого фактора, хакер получает данные, например, с помощью обычного разговора по телефону.

Фишинг — это вид мошенничества, целью которого является получение доступа к персональным данным пользователей — данным авторизации. Целью для фишинга является кража персональных данных. Самым наглядным примером такой атаки, это сообщение, отправленное пользователю по электронной почте, и изменённое под официальное письмо, заращающей информацию или требующей совершить некоторые действия. Повод бывают абсолютно разные. Запрос восстановления личных данных, неисправность и т.п. Эти сообщения чаще всего содержат в себе ссылку на поддельную веб-страницу, не отличающуюся от официальной, и содержащую анкету, запрашивающую конфиденциальную информацию.

Способы защиты от угроз в Интернете

Существует много видов и способов атак, но также есть и достаточное количество способов защиты от них. При работе в Интернете рекомендуется выполнять следующие требования:

1. Применяйте разные пароли
2. Используйте на ПК с учетной записью с ограниченным доступом к данным
3. Применяйте шифровку данных
4. Стабильно меняйте антивирусные программы
5. Применяйте межсетевой экран

Биометрические системы защиты — это способ идентификация личности. Используя параметры лица, голоса и жестов для более точной идентификации, и авторизации. Используется для создания многоуровневой системы информационной безопасности, основанной на индивидуальной биометрической информации.

1. Википедия
2. <http://safe-surf.ru/users-of/article/212/>
3. <http://elhow.ru/programmnoe-obespechenie/antivirusnye-programmy/kak-udalit-win32>
4. <http://biz.liga.net/all/all/novosti/2030737-top-5-osnovnykh-internet-ugroz-itogi-iyulya.htm>
5. Молодой учёный №11 (91)/2015
6. newcorediary.com/2011/02/почему-компьютерные-вирусы-называют/
7. <http://www.star-force.ru/press/articles/?news=2955>
8. <https://www.avast.ru/c-botnet>
9. <https://www.rif.ru>