Вредоносные утилиты–это вредоносныепрограммы, предназначенныедляавтоматизациисозданиявирусов,червей или троянских программ, DoS-атакна удалённые серверы, взлома других компьютеров ит.п. В отличие от вирусов, червей и троянских программ, вредоносные утилиты сами не представляютугрозы для компьютера, на котором исполняются, авредоносные действия выполняются приложением только по прямому указаниюзлоумышленника.

Подкласс вредоносных утилит в соответствии ссовершаемыми действиямиделится на следующие типы:

Программы-конструкторы, предназначенные для создания новых вирусов, червей итроянских программ и способные генерировать исходный код вредоносных программ, объектные модули и/или вредоносные файлы;

DoS,предназначенные для осуществления атак типа «отказ в обслуживании» на компьютер-жертву;

Email-Flooder, используемые для того, чтобы переполнять каналы электронной почты бессмысленными сообщениями;

Программы SMS-Flooder, используемые для переполнения бесполезными сообщениями каналы передачи текстовых сообщений [2].

Таким образом, в настоящее время существует множество компьютерных вирусов и вредоносных программ, которые способны наносить значительный ущерб компьютеру, а также нарушать целостность, конфиденциальность и доступность информации. Вирусы были и остаются серьёзной проблемой в компьютерном мире, поэтому очень важно установить и поддерживать на своём компьютереантивирусную программудля защиты от вредоносных программ.

Список использованных источников

Информационная безопасность в таможенных органах: учебно-методическое пособие для студентов специальности 1-96 01 01 «Таможенное дело» / Г. М. Бровка, И. А. Ковалькова, А. Н. Шавель. – Минск: БНТУ, 2019. – 118 с.

Студенческая электронная библиотека [Электронный ресурс]. – Режим доступа: https://www.avast.ru/c-malware-all2-105752.html./–Дата доступа: 10.03.2020.

Методы обнаружения и удаления вирусов.Антивирусные программы и комплексы

Савастюк О.Ю., Тишкова Е.О. Научный
руководитель: Ковалькова И.А. Белорусский
национальный технический университет

Компьютерные вирусы были и остаются одной из наиболее распространённых причин потери информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий.

Основным средством борьбы с вирусами остаются антивирусные программы. В настоящее время используется множество антивирусных программных средств, которые могут реализовывать не только некоторые определённые методики обнаружения компьютерных вирусов, но и их комбинации [1].

Существует несколько основополагающих методик обнаружения и защиты от вирусов:

Сканирование

Сканирование –этосамая простая методика поиска вирусов.Заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Антивирусные программы-сканеры могут обнаружить только уже известные вирусы, которые были предварительно изучены и для которых была определена сигнатура. Таким образом, использование программ-сканеров не защищает компьютер пользователя от проникновения новых вирусов.

Обнаружение изменений

При внедрении вируса в компьютерную систему обязательно происходят изменения в системе (которые некоторые вирусы успешно маскируют). Это изменение объёма доступной оперативной памяти, изменение загрузочных секторов дисков и изменения самих файлов.

Достаточно запомнить характеристики, которые подвергаются изменениям в результате внедрения вируса, а затем периодически сравнивать эти эталонные характеристики с действующими.

Эвристический анализ

Эвристический анализ является относительно новым методом в обнаружении вирусов. Он позволяет обнаруживать ранее неизвестные вирусы, причём для этого не надо предварительно собирать данные о файловой системе, как этого требует метод обнаружения изменений. Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов.

Резидентные мониторы (сторожа)

Резидентные мониторы– это программы, которые постоянно находятся оперативной памяти компьютера, и отслеживают все подозрительные действия, выполняемые другими программами. Они выдают сообщение пользователю, если какая-либо программа попытается изменить загрузочный сектор жёсткого диска,компакт-диска или выполняемый файл. К сожалению, резидентные мониторы имеют очень много недостатков, которые делают этот класс программ малопригодными для использования.

Многие программы, даже не содержащие вирусов, могут выполнять действия, на которые реагируют резидентные мониторы. Например, обычная команда LABEL изменяет данные в загрузочном секторе и вызывает срабатывание монитора.

Вакцинирование программ

Существует способ защиты программ от вирусов, при котором к защищаемой программе присоединяется специальный модуль контроля, следящий за её целостностью. При этом может проверяться контрольная сумма программы или какие-либо другие характеристики. Когда вирус заражает вакцинированный файл, модуль контроля обнаруживает изменение контрольной суммы файла и сообщает об этом пользователю.

Однако stealth-вирусы легко обманывают вакцину. Заражённые файлы могут работать как обычные файлы и вакцина при этом не обнаружит заражения.

Аппаратная защита от вирусов

Аппаратно-программные средства представляют собой специальный контроллер, вставляемый в один из разъёмов расширения компьютера и программное обеспечение, управляющее работой этого контроллера. Если аппаратно-программный комплекс обнаружит, что какая-либо программа пытается нарушить установленную защиту, он может сообщить об этом пользователю и заблокировать дальнейшею работу компьютера.

После обнаружения вируса, его необходимо удалить. Существуют две основные методики, используемые антивирусными программами для удаления вирусов.

Первая, наиболее распространённая методика предусматривает, что антивирусная программа удаляет уже известный вирус. Чтобы вирус мог быть правильно удалён, необходимо чтобы он был изучен, разработан алгоритм его лечения и этот алгоритм был реализован в новой версии антивируса.

Вторая методика позволяет восстанавливать файлы и загрузочные секторы, заражённые ранее неизвестными вирусами. Для этого антивирусная программа заранее, до появления вирусов, должна проанали-

зировать все выполняемые файлы и сохранить о них много разнообразной информации [2].

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы, хотя они и не гарантируют стопроцентную защиту от вирусов.

На сегодняшний день наиболее популярными антивирусными программами являются:

Антивирус Касперского– это продукт для защиты ПК, чья эффективность проверена миллионами пользователей во всём мире. Программа включает в себя основные инструменты для защиты ПК.

*ESET NOD32*обеспечивает обнаружение и блокировку вирусов, троянских программ, червей, шпионских программ, рекламного ПО, фишинг-атак, руткитов и других интернет-угроз, представляющих опасность для компаний. Несмотря на минимальную потребность в ресурсах, обеспечивает непревзойдённый уровень проактивной защиты, практически не снижая производительность компьютера.

Symantec Norton Anti-Virus – это программа, которая автоматически удаляет вирусы, интернет-червей и троянские компоненты, не создавая помех работе пользователя. Norton AntiVirus позволяет противостоять угрозам самых современных spyware- и adware-программ и блокирует работу таких программ ещё до того момента, как пользователь перенаправляется на другой сайт.

Dr. Web – это антивирус, который проводит полную антивирусную проверку Windows-памяти компьютера и способен остановить вирусный процесс. Важным показателем качества работы этой антивирусной программы является не только её способность находить вирусы, но и лечить их, не просто удалять инфицированные файлы вместе с важной для пользователя информацией, но и возвращать их в первоначальное «здоровое» состояние[3].

У каждого типа антивирусных программ имеются свои плюсы, а также недостатки. Однако применение определенных типов антивирусных программ может привести к желаемому результату.

Литература

Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов. – М.: «СОЛОН-Р», 2001.

Что такое компьютерные вирусы [Электронный ресурс]. – Режим доступа:http://www.frolov-lib.ru/books/step/v05/ch2.htm – Дата доступа: 06.03.2020.

Наиболее популярные антивирусные программы [Электронный ресурс]. – Режим доступа: http://www.tagac.ru/270– Дата доступа: 07.03.2020.

Маскировка IP-адреса. Использование специализированных программ и сервисов

Хацкевич К.С.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

IP-адрес(*Internet ProtocolAddress, айпи адрес*) – это уникальный числовой идентификатор конкретного устройства в составе компьютерной сети, построенной на основе протокола TCP/IP. Для работы в Интернете требуется его глобальная уникальность. Для частной сети достаточно, чтобы были исключены совпадения в локальном пространстве.

настоящее время тема анонимности в интернете очень актуальна. Причин для этого много,но основная – это безопасность, так как существует очень много способов узнать личную информацию о пользователе по его IP-адресу или другим характеристикам интернет-соединения. На какой бы сайт не зашёл пользователь в интернете, он везде оставляет свои «следы», в виде информации о типе операционной системы, обозревателя исамое главное, свой IP и MAC адрес. При совокупности всех этих данных, определить его месторасположение очень просто. Также возможно проследить все его действия, совершённые, например, с домашнего компьютера. Владелец любого удалённого сервера или сайта в Интернете может точно определить, что пользователь делал на его сайте.

Существуют следующие способы маскировки (скрытия) IP-адреса:

1. *VPN-технологии* (*VirtualPrivateNetwork*) – технологии, позволяющей подменить IP-адрес без использования прокси-сервера. Внешне VPN-соединение мало чем отличается от подключения к обычной локальной сети: приложения вообще не почувствуют разницы и поэтому без какой-либо настройки будут использовать его для доступа в интернет. Когда одно из них захочет обратиться к удалённому ресурсу, на компьютере будет создан специальный GRE-пакет (GenericRoutingEncapsulation, общая инкапсуляция маршрутов), который в зашифрованном виде будет отправлен VPN-серверу. VPN-сервер, в свою очередь, этот пакет расшифрует, разберётся, в чём его суть (запрос на закачку какой-либо HTTP-страницы, просто передача данных и т.д.), и выполнит от своего лица (то есть «засветит» свой IP) соответствующее действие. Далее,