их защите и формированию интеграционных шлюзов. Все необходимые программно-технические средства в НАСЭД для этого предусмотрены.

Таким образом, функционирование Национальной автоматизированной системы электронного декларирования имеет большой потенциал для дальнейшего развития и будет способствовать результативной работе таможенных органов.

Вредоносные программы и их классификация. Основные каналы распространения компьютерных вирусов и других вредоносных программ

Русак А.В., Саульченко Д.С.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

Существует класс программ, которые были изначально написаны с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов и т.д. или же приобрели такие свойства вследствие каких-либо причин. Такиепрограммы несут вредоносную нагрузку и соответственно называются вредоносными.

Вредоносная программа–это программа, наносящая какой-либо вред компьютеру, на котором она запускается, или другим компьютерам в сети.

вредоносным программам относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, которые наносят заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети [2].

Для распространения вредоносные программы используют следующие объекты и каналы [1]:

- файлы исполняемых программ;
- файлы офисных документов; •файлы интерпретируемых программ;
- загрузочные секторы дисков и дискет;
- сообщения электронной почты;
- пиринговые (файлообменные) сети;
- интрасеть или Интернет;
- драйверы ОС;
- флеш-накопители.

Вредоносные программы подразделяются на: *компьютерные вирусы, сетевые черви, троянские программы и вредоносные утилиты.*

Компьютерный вирус – это программа, способная создавать свои дубликаты и внедрять их в вычислительные сети и файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликатысохраняютспособностькдальнейшемураспространению [1].

Жизненный цикл любого компьютерного вируса можно разделить на пятьстадий:

- проникновение на чужой компьютер;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- внедрение копий.

Вирусы делятся на *загрузочные* и *файловые* вирусы.

Загрузочный вирус заражает загрузочный сектор винчестера или дискеты и загружается каждый раз при начальной загрузке операционной системы.

Файловый вирус записывает свой код в тело программного файла или офисного документа. При этом во время запуска программы вирус получает управление. Файловые, в свою очередь, подразделяются на *классические файловые вирусы, макровирусы и скрипт-вирусы*[1].

Червь(сетевойчервь)–
этовредоноснаяпрограмма,распространяющаясяпосетевымканалам,которая способнаксамостоятельному преодолению систем защиты компьютерных сетей, атакжек созданиюидальнейшемураспространению своихкопий.

Жизненный цикл червей состоит из следующих стадий:

- проникновение в систему;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- распространение копий.

зависимости от способа проникновения в систему черви делятся на:

- *Сетевые черви*, которые для своего распространения используют локальные сети и Интернет;
- *Почтовые черви*, которые распространяются с помощью почтовыхпрограмм;
- *IM-черви*,которыеиспользуютсистемымгновенногообменасообщениями;
- *IRC-черви*, распространяющиеся по каналам IRC;
- *P2P-черви*,распространяющиесяпripомощипиринговых (файлообменных) сетей.

Троянская программа – это вредоносная программа, выполняющая несанкционированные пользователем действия [2]. Такие действия могут включать:

- удаление данных;
- блокирование данных;
- изменение данных;
- копирование данных;
- замедление работы компьютеров и компьютерных сетей.

отличие откомпьютерных вирусов и червейтроянские программы неспособны к самовоспроизведению. Жизненный цикл троянов состоит из трех стадий:

- проникновение в систему;
- активация; •выполнение вредоносных действий.

Троянские программы в соответствии с типом действий, выполняемыхиминакомпьютере, классифицируются следующим образом:

- *Бэкдор*– это троянская программа, которая предоставляет злоумышленникам возможность удалённого управления заражёнными компьютерами. Такие программы позволяют автору выполнять на заражённом компьютере любые действия, включая отправку, получение, открытие и удаление файлов, отображение данных и перезагрузку компьютера [1].
- *Эксплойты* – это программы с данными или кодом, использующие уязвимость в работающих на компьютере приложениях.
- *Руткиты* – это программы, предназначенные для сокрытия в системе определённых объектов или действий.
- *Банковские троянцы* (Trojan-Banker) предназначены для кражи учётных данных систем интернет-банкинга, систем электронных платежей кредитных или дебетовых карт.
- *Программы Trojan-Downloader* способны загружать и устанавливать на компьютер-жертву новые версии вредоносных программ, включая троянские ирекламные программы.
- *Игровые троянцы* крадут информацию об учётных записях участников сетевых игр.
- *Программы Trojan-IM* крадут логины и пароли к программам мгновенного обмена сообщениями.
- *SMS-троянцы* отправляют текстовые сообщения с мобильного устройства на платные телефонные номера с повышенным тарифом, тратя ваши деньги.

Также существует ещё множество других видов троянских программ.

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