1. Технические средства интроскопии объектов таможенного контроля [Электронный ресурс] – Режим доступа: https://docplayer.com/147338246-Tehnicheskie-sredstva-introskopii-obektov-tamozhennogo-kontrolya.html – Дата доступа: 22.04.2022.
2. Взаимодействие рентгеновского излучения с веществом [Электронный ресурс] – Режим доступа: https://studopedia.net/12_32167_vzaimodeystvie-rentgenovskogo-izlucheniya-s-veshchestvom.html – Дата доступа: 01.05.2022.

ВРЕДОНОСНЫЕ ПРОГРАММЫ И ИХ КЛАССИФИКАЦИЯ, ОСНОВНЫЕ КАНАЛЫ РАСПРОСТРАНЕНИЯ

Гвоздь Е.С., Синицына В.С.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

По мере развития компьютерных технологий совершенствуются и развиваются вредоносные программы. Последние становятся всё более усложнёнными и способными наносить комплексный вред не только одному (целевому) пользователю, но и воздействовать на сторонние (взаимосвязанные с целевым). Исходя из этого, вредоносные программы посредством новых алгоритмов и кодов, способны нанести непоправимый ущерб целым корпорациям. Следует отметить, что такие программы часто используются в качестве дестабилизирующего инструмента некоторыми корпорациями, с целью нанести вред конкурентам.

Итак, рассмотрим данные программы подробнее. Изначально, важно отметить, что компьютерные вирусы и программы часто отождествляют, однако это не совсем так. Вирусы бывают разных видов, и один из них – ***вредоносные программы***, целью которых является нанесение ущерба пользователю, посредством заражения файлов (либо иных пользовательских данных), их удаление, кражи и т. п.

Приведём классификацию вредоносных программ:

1. *Сетевые черви*. Как видно из названия, данный тип программ распространяется по всем пользовательским данным, начиная с документов формата .doc до электронных писем. Аналогично с одноимёнными физическими червями, такой вид программ паразитирует и распространяется с огромной скоростью, и, впоследствии уничтожает их (что является их целью).

2. *Троянские программы*. Такой тип программ, аналогично предшественнику, объясняет свою сущность исходя из названия. То есть выступает посредником между пользователем и реализатором (наносящий вред). Суть заключается в том, что троянская программа несанкционированно, без ведома пользователя, проникает в систему и, непосредственно, наносит вред. Целью злоумышленника (то есть реализатора программы) является кража паролей, либо другой конфиденциальной информации пользователя.

3. *Бекдоры*. Еще один вид вредоносных программ, который не сразу заявляет о себе (пользователь не замечает его непосредственной работы). Принципы работы такого вида программ нацелены на управление (удаление, перемещение, копирование, размножение), либо установку новых (зловредных, либо не нужных) программ и файлов. Такой вид также является одним из опаснейших, поскольку способен нанести непоправимый вред.

4. *Логическая бомба*. Такой вид программы срабатывает при определённом алгоритме действий, (можно сравнить с миной). То есть, если пользователь совершил определённый механизм действий, либо наступило определённо заданное время (заданное злоумышленником, хакером), то программа начинает срабатывать и способна блокировать, уничтожать или модифицировать данные пользователя, то есть наносить вред.

5. *Программная закладка*. Принцип работы схожий с предыдущей, но срабатывание программы может начаться только при случайном попадании в систему (то есть чаще всего не целенаправленно).

6. *Программы шпионы*. Название говорит само за себя – принципы работы программы направлены на сбор и передачу информации пользователя, посредством шпионажа. [1]

Для того чтобы вредоносная программа сработала её необходимо внедрить в систему. Это может совершаться по различным каналам связи различными методами. Наиболее распространёнными являются – спам-рассылки на e-mail и заражённые веб-страницы. Так, обмен мгновенными сообщениями с другом в виде непроверенных ссылок может представлять собой угрозу заражения вредоносными программами. Ведь эти ссылки могут быть оформлены обыкновенно, но переходя по ним в Интернете, вы оказываетесь на заражённых веб-страницах.

Существуют и иные формы заражения вредоносными программами, например – фишинг. Это вид интернет-мошенничества, который используется для того, чтобы получить идентификационные данные пользователей. Например, кража паролей, номеров карт, банковских счетов и другой конфиденциальной информации.

Для поддержания работы вредоносных программ существуют ряд принципов. Например, нарушение работы антивирусных программ для

предотвращения обнаружения вредоносного программного обеспечения и продления его существования на компьютере. Также, это может делаться для того, чтобы сохранять работу вредоносной программы необнаруженной как можно дольше: «Чем менее видима программа для антивирусных программ, тем дольше её можно будет использовать для получения доступа к заражённым компьютерам и сбора информации». [2]

Таким образом, исходя из выше сказанного, можно сделать вывод о том, что вредоносные программы (в качестве вида компьютерных вирусов) способны наносить значительный ущерб, реализуя любые угрозы информации, нарушая целостность, конфиденциальность, доступность. Поэтому специалисты по информационной безопасности настойчиво рекомендуют владельцам компьютеров использовать комплексные системы защиты информации, выявления угроз, блокирования известных и неизвестных вредоносных программ, а также мониторинга работы пользователей и предотвращения инсайдерских атак.

Литература

1. Безруков, Н.Н. Классификация компьютерных вирусов MS-DOS и методы защиты от них : учеб. пособие / Н. Н. Безруков. – М.: СП "ICE", 1990.
2. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях : учеб. пособие / В.Ф. Шаньгин. – М.: ДМК, 2012. – 592 с.