УДК 004.056

АНАЛИЗ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ ОТКРЫТОГО СТЕГАНОГРАФИЧЕСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СКРЫТОГО ОБМЕНА ДАННЫМИ И РЕАЛИЗАЦИИ КОМПЬЮТЕРНЫХ АТАК

Федосенко М.Ю. (ИТМО)
Научный руководитель – доктор технических наук, профессор Беззатеев С.В. (ИТМО)

Введение. В настоящее время Интернет играет большую роль в обществе, в том числе и при осуществлении противоправной деятельности и реализации компьютерных атак [1]. Глобальная сеть содержит в себе огромные объёмы различных данных, которые включают в себя как взаимодействие между пользователями и системами, так и различное программное обеспечение [2]. Эти данные могут иметь полезный, нейтральный и вредоносный характер. К последней категории несомненно относятся вирусное программное обеспечения и информация, имеющая противоправный (преступный) характер. К нейтральной категории можно отнести как информационный «мусор» или развлекательный контент (например, игровые приложения), так и данные, характер которых зависит от ситуации и конечной цели их применения. Одним из примеров является программное обеспечения для сокрытия данных методами стеганографии [3]. Его можно применять в полезных для государства и общества целях, таких как сокрытие тайной информации за счёт реализации скрытых каналов связи, подтверждения авторства за счёт цифровых водяных знаков, выявления скрытого злонамеренного характера информации. Однако, в руках злоумышленников, данное ПО может быть использовано для осуществления обмена противоправными данными и реализации компьютерных атак.

Основная часть. Проведённые ранее исследования в области практического применения стеганографии указывают на возможность проведения хакерских атак за счёт сокрытия вредоносного кода внутри легитимных файлов [4]. В цифровой криминалистике имеются случаи использования стеганографии для проведения атак, направленных на получение персональных и платёжных данных пользователей, доставку вредоносного кода, нарушение отказоустойчивости компьютерных систем предприятий. В большинстве случаев, в качестве покрывающего объекта выступали графические изображения и низкоуровневый код файлов в силу простоты и доступности способов реализации [5]. Также, результаты исследований устойчивости интернет-ресурсов показывают, что веб-ресурсы не имеют достаточной защиты от возможности их использования в качестве среды реализации скрытых каналов связи и обмена данными, имеющими вложения [1]. Это в свою очередь не только допускает стеганографические атаки злоумышленников, но и позволяет «обходить» предпринятые Роскомнадзором меры, направленные на деанонимизацию пользователей, анализ и мониторинг информации, распространяющейся в сети Интернет [6].

В работе представлен сравнительный анализ возможностей использования программного обеспечения для сокрытия данных из свободного доступа. В качестве описания вектора атаки злоумышленника представлена следующая теория [5]:

1. Есть необходимость передать данные противоправного характера через открытый канал связи, чтобы не привлекать при этом внимания к конкретным информационным потокам.
2. При этом, злоумышленник не обладает высоким уровнем знаний в области информационной безопасности, стеганографии, математики и программировании.
3. В таком случае, он воспользуется готовыми решениями, искать которые будет в открытом доступе

Имеющееся множество готовых решений включает в себя следующие такие программные продукты: Jsteg, Hallucinate, JHide, DarkJPEG OpenPuff, Steghide, SilentEye, QuickStego, OpenStego, Anubis, DeEggerEmbedder, Steganogaphy Online [5]. В основе их работы имеются следующие способы вложения информации:

- программы, полностью записывающие вложение в начало или конец покрывающего объекта;
- программы, распределяющие вложение внутри файла-контейнера равномерно или согласно конкретным алгоритмам, заложенным в основу их реализации;
- программы, реализующие фундаментальные методы стеганографии и цифровых водяных знаков (например, LSB - least significant bit) [3] [5].

Данные программные продукты также различаются в зависимости от следующих характеристик:

- поддерживаемых форматов файлов – покрывающих объектов;
- возможности дополнительного шифрования вложения методами криптографии;
- возможности распределять вложение в несколько контейнеров;
- возможности автоматического извлечения вложения и осуществления атак на стегосистемы.

Выводы. Рассмотренные в рамках исследования программные продукты были квалифицированы в зависимости от особенностей работы и программной реализации. На основе представленной классификации выявлены достоинства и недостатки их применения для конкретных целей и конкретных покрывающих объектов. Также, программы были классифицированы по степени удобства эксплуатации и обширности функционала.

Выборка показала, что наиболее простые программы, в большинстве своём, оказывались и наиболее удобными в использовании. Большим преимуществом также является наличие графического интерфейса и англоязычного функционала. Подавляющая часть продуктов написаны на языке Java и являются кроссплатформенными. Всё это делает возможным их использование в качестве инструмента применения стеганографии злоумышленниками в ходе противоправных действий и реализации кибератак [7].

Список использованных источников:

1. Ахрамеева К.А., Федосенко М.Ю., Герлинг Е.Ю., Юркин Д.В. Анализ средств обмена скрытыми данными злоумышленниками в сети Интернет посредством методов стеганографии // Телекоммуникации - 2020. - № 8. - С. 14-20.
2. Менщиков А.А., Перфильев В.Э., Федосенко М.Ю., Фабзиев И.Р. Основные проблемы использования больших данных в современных информационных системах // Столыпинский вестник - 2022. - Т. 4. - № 1. - С. 30.
3. Федосенко М.Ю., Бочаров М.В. Анализ используемых алгоритмов сокрытия информации в современном стеганографическом программном обеспечении // Студенческий научно-образовательный журнал «StudNet» - 2022. - Т. 5. - № 2. - С. 29.
4. Федосенко М.Ю., Беззатеев С.В. Анализ проблематики применения методов стеганографии при осуществлении противоправных действий и её роли в цифровой криминалистике // Проблемы информационной безопасности. Компьютерные системы - 2023. - № 3(56). - С. 33-57.
5. Ахрамеева К.А., Федосенко М.Ю. Сравнительный анализ возможностей использования стеганографического программного обеспечения для скрытого обмена данными в сети интернет // Вестник Санкт-Петербургского государственного университета

технологии и дизайна. Серия 1: Естественные и технические науки - 2022. - № 1. - С. 37-43.

6. Ахрамеева К.А., Федосенко М.Ю. Защита информации методами криптографии в современной России // Студенческий научно-образовательный журнал «StudNet» - 2020. - Т. 3. - № 9.

7. Федосенко М.Ю. Социологическое исследование осведомлённости выпускников образовательных учреждений в возможностях скрытого обмена данными в интернете // Скиф. Вопросы студенческой науки - 2022. - № 1(65). - С. 287-295.