ПРИМЕНЕНИЕ СТЕГАНОГРАФИИ ПРИ ОСУЩЕСТВЛЕНИИ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ ПРЕДПРИЯТИЙ

Д.В. Клишин, *Национальный исследовательский университет ИТМО, Danil.Klishin2021@yandex.ru;*
М.Ю. Федосенко, *Национальный исследовательский университет ИТМО, fedosenkomaksim98@gmail.com.*

УДК 004.056

Аннотация. В работе представлено описание тактик компьютерных атак на информационную инфраструктуру предприятий с применением стеганографии. Описаны основные типы стеганографии, а также представлены технологии и процедуры, используемые в реальных компьютерных атаках. В результате исследования выявлены основные тенденции применения стеганографии в компьютерных атаках: алгоритмы вложения и форматы стеганоконтейнеров, вектора атак, используемое программное обеспечение, реальные случаи успешной реализации атак.

Ключевые слова: стеганография; тактики компьютерных атак; техники компьютерных атак; процедуры компьютерных атак; виды стеганографии.

THE USE OF STEGANOGRAPHY IN THE IMPLEMENTATION OF COMPUTER ATTACKS ON THE INFORMATION INFRASTRUCTURE OF ENTERPRISES

D. Klishin, *National Research University ITMO;*
M. Fedosenko, *National Research University ITMO.*

Annotation. The paper describes the tactics of computer attacks on the information infrastructure of enterprises using steganography methods. The main methods of steganography are described, as well as technologies and procedures used in real computer attacks. The study revealed the main trends in the use of steganography in computer attacks: nesting algorithms and formats of steganocontainers, attack vectors, software used, real cases of successful implementation of attacks.

Keywords: steganography; tactics of computer attacks; techniques of computer attacks; procedures of computer attacks; types of steganography.

Введение

В современном мире постиндустриального общества, развитие которого сопровождается наличием информационной революции, появляется острая необходимость в защите информации от ее подмены, наличия в ней ложного содержания и использования в корыстных целях. Современные технологии и эволюционное развитие человеческого мозга приводит к тому, что и абсолютно верная (в рамках рассматриваемой информационной системы) информация может быть атакована недоброжелателями, при этом приносить вред как конкретному индивиду, так и обществу в целом. Другими словами, в качественном информационном контенте может быть спрятан другой контент.

Исследованием данного явления занимается такой раздел науки как Стеганография. Данный раздел изучает способы передачи и/или хранения информации при условии сохранения в тайне самого факта использования такого способа.

Толковый словарь Ушакова дает следующее определение данному термину:

Стенография (от греч. *steganos*-скрытый и *grapho*-пишу) – Тайнопись, письмо условными, шифрованными знаками [1]. Несмотря на схожее определение с понятием криптография, стеганография не занимается шифрованием самого информационного объекта, а определяет методы сокрытия самого факта присутствия этого объекта. Переходя на более простой язык, шифрование при стеганографии заключается в том, что мы встраиваем один информационный объект в другой информационный объект, как вирус встраивается в клетку живого организма, не изменяя внешней структуры самой клетки, в то время как при использовании криптографии сразу будет понятен факт шифрования в виду совсем другой, отличной от обычной, структуры клетки.

Отсюда следуют следующие преимущества стеганографии над криптографией [2]:

- Отсутствие сложных математических моделей (при классической стеганографии) для шифрования информации.
- Отсутствие очевидного факта наличия скрытой информации, при котором злоумышленник даже не подозревает о наличие данной информации, тем самым вероятность обнаружения без специальных знаний и аналитических данных сводится к нулю.
- Возможность использования стеганографии как альтернативы криптографии в условиях, когда использование криптографии невозможно.

В качестве примера к последнему пункту из списка преимуществ можно привести страну Китай, в которой 1 января 2020 г. вступил в силу закон «О Криптографии» [3]. В рамках действия данного законодательного акта, государственный аппарат будет регулировать криптографические методы и протоколы, использующиеся на территории страны. Конкретнее, будет контролироваться допустимость/недопустимость использования криптографии для каждого конкретного случая, а также сложность криптоключей и наличие возможности дешифровки всех криптографических методов у органов государственной власти. Согласно данному закону, государство не планирует полный отказ от использования криптографии. Наоборот, государство будет поощрять и поддерживать научно-технические исследования в сфере шифрования данных и защищать интеллектуальную собственность на криптографические методы и технологии [4].

Данный пример демонстрирует тенденцию вывода практического применения стеганографии на новый уровень, поскольку потребность в обмене скрытыми данными может возникнуть не только среди нарушителей, но и среди обычных пользователей, не желающих мониторинга своей информации [5]. Но поскольку именно «нежелательные» данные нарушителей, а именно, несвоевременная реакция на них, способны нанести большой ущерб и понести огромные убытки, то необходимо исследовать возможность применения стеганографии в реализации компьютерных атак.

В связи с этим, целью данной статьи является выявление тактик и векторов компьютерных атак на информационную инфраструктуру предприятий с использованием стеганографии на основе информации о реальных случаях реализации подобного рода атак. Для выполнения поставленной цели требуется решить следующие задачи:

- Выявить основные типы и особенности стеганографических контейнеров в зависимости от формата покрывающего объекта.
- Проанализировать реальные случаи осуществления компьютерных атак с использованием стеганографии, выделить особенности реализации.

- Установить результаты практического применения стеганографии в компьютерных атаках для определения особенностей мер защиты от них.
- Выявить основные техники компьютерных атак с использованием стеганографии и сопоставить их с тактиками компьютерных атак.

Методы стеганографии

В изученных источниках информации [6-8] можно выделить шесть основных типов контейнеров, используемых в стеганографии:

- в тексте;
- в изображении;
- в аудио;
- в видео;
- в метаданных;
- в сетевых протоколах.

В случае с текстовым стеганографическим контейнером, стеганография скрывает секретное сообщение внутри фрагмента текста. Простая версия текстовой стеганографии использует первую букву в каждом предложении для формирования скрытого сообщения.

При использовании в качестве контейнера изображения стеганография кодирует секретную информацию, изменяя биты в цветовой гамме. При этом простым примером стеганографии в изображении является использование младших разрядов каждого пикселя изображения.

Для стеганографического контейнера в аудио может использоваться метод изменения младших разрядов каждого байта в аудиофайле, аналогично стеганографии изображений.

При использовании стеганографического контейнера в видео секретное сообщение может быть как в каждом видеокадре, так и в аудиодорожке.

Также возможно сокрытие информации в полях метаданных различных файлов.

Помимо вышеперечисленных методов сокрытия информации возможно использование в качестве стеганографического контейнера сетевого трафика различных сетевых протоколов. Например, данные могут быть скрыты в заголовках *TCP/IP* или полезной нагрузке сетевых пакетов или в *DNS*-запросах, также отправитель может скрыть информацию за счет времени между отправкой различных пакетов.

Основная сложность обнаружения использования стеганографии заключается в установлении факта передачи секретного сообщения, что в совокупности с разнообразными типами стеганографических контейнеров предоставляет злоумышленнику инструмент для компьютерных атак.

Тактики компьютерных атак с использованием стеганографии

Стеганография рассматривается в нормативно-правовых актах РФ в области информационной безопасности от ФСТЭК России [6, 7]. В документе [6] приведена классификация методов стеганографической передачи информации, а также дана сравнительная характеристика стеганографических методов преобразования информации. В документе [7] стеганография упоминается в перечне основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации.

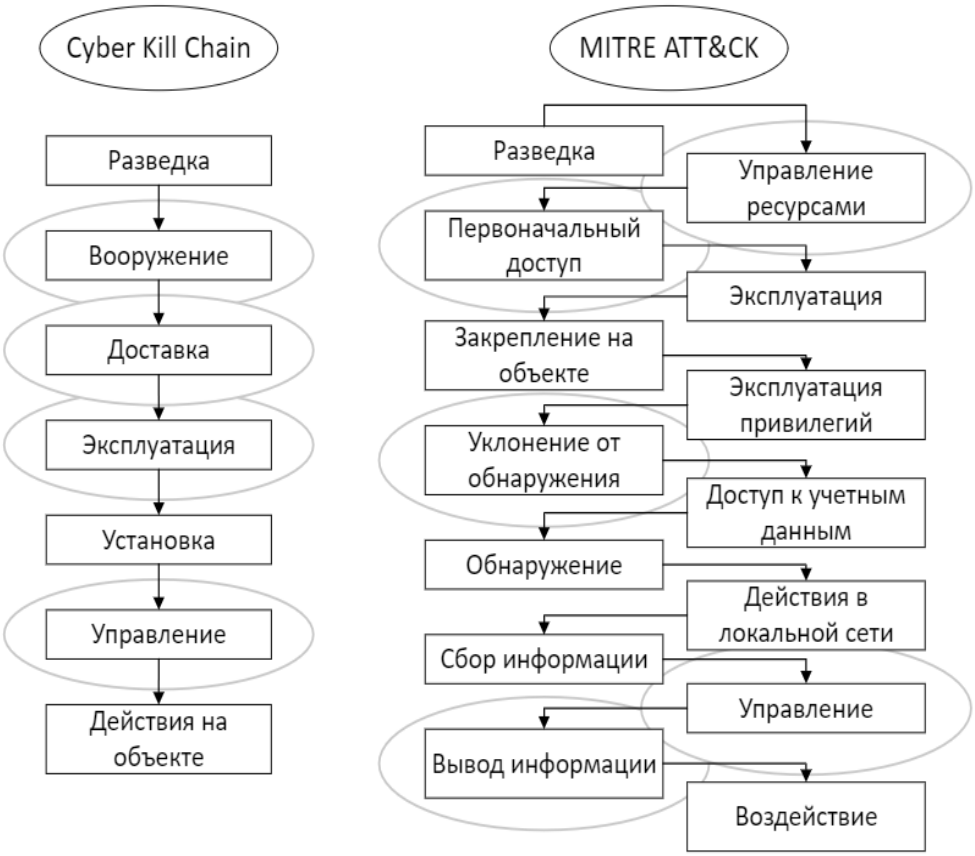

Рисунок 1

Тактики компьютерных атак, в которых используются техники стеганографии можно продемонстрировать на фреймворках *Cyber Kill Chain* [9] и *MITRE ATT&CK* [10]. При анализе базы знаний *MITRE ATT&CK* было выявлено рассмотрение техник стеганографии в таких тактиках компьютерных атак, как управление вредоносным программным обеспечением и в тактике избежания обнаружения. При этом в методике ФСТЭК России [7] также рассматривается применение стеганографии в тактике вывода информации из целевой информационной инфраструктуры. Данное отличие объясняется тем, что для других тактик, например, таких как разработка вредоносного программного обеспечения, получение доступа и вывод данных, процедуры стеганографии идентичны процедурам, описанным в тактике избегания обнаружения. На рис. 1 выделены основные тактики компьютерных атак, в которых может применяться стеганография.

Использование стеганографии в реальных компьютерных атаках

Основной из тактик компьютерных атак, в которой может использоваться стеганография, является предотвращение обнаружения информации, которая доставляется или выводится с целевого объекта в информационной инфраструктуре.

По версии *MITRE* первым вредоносным программным обеспечением, в котором зафиксировано применение стеганографии, является *Duqu*. Вредоносное программное обеспечение *Duqu* было впервые обнаружено в 2011 г., оно использовало стеганографию для скрытного вывода собранной информации из целевой информационной инфраструктуры в изображениях [11].

На данный момент существует большое количество вредоносного программного обеспечения, используемого для скрытой доставки или вывода информации. В табл. 1 перечислено вредоносное программное обеспечение, хакерские группировки, а также каким образом использовалась стеганография в атаках по версии [10, 12].

Таблица 1.

Наименование	**Описание использования стеганографии**
Вредоносное программное обеспечение	
ABK	Может извлечь вредоносный переносимый исполняемый файл из фотографии.
Diavol	Запутывает свои основные процедуры кода в растровых изображениях.
ProLock	Может использовать файлы *JPG* и *BMP* для хранения своей полезной нагрузки.
ObliqueRAT	Может скрывать свою полезную нагрузку в изображениях *BMP*, размещенных на скомпрометированных веб-сайтах.
Raindrop	Использует стеганографию, чтобы определить начало своей закодированной полезной нагрузки в пределах легитимной *zip* кодировки.
PolyglotDuke	Может использовать стеганографию, чтобы скрыть передаваемую информацию в изображениях.
LiteDuke	Использует файлы изображений, чтобы скрыть свой компонент загрузки.
RegDuke	Может скрывать данные в изображениях, включая использование младших разрядов.
RDAT	Может встраивать данные в *BMP* изображение перед выводом.
IcedID	Имеет встроенные двоичные файлы в зашифрованных *RC*4 файлах *PNG*.
Avenger	Может извлекать вредоносные программы-бэкдоры из загруженных изображений.
build_downer	Может извлекать вредоносное ПО из загруженного файла *JPEG*.
BBK	Может извлечь вредоносный исполняемый файл из фотографии.
Ramsay	Извлекает вредоносный исполняемый файл, встроенный в файлы JPEG, содержащиеся в документах *Word*.
Okrum	Полезная нагрузка зашифрована и встроена в *PNG*-файл.
Bandook	Использует изображения в формате *PNG* в *zip*-файле для создания исполняемого файла.
Invoke-PSImage	Может использовать скрипт *PowerShell* в пикселях файла *PNG*.
PowerDuke	Использует стеганографию для скрытия бэкдоров в *PNG*-файлах, которые также шифруются с использованием алгоритма шифрования *Tiny*.
Хакерские группировки	
Earth Lusca	Использует стеганографию, чтобы скрыть шелл-код в файле изображения *BMP*.
Andariel	Скрывает вредоносные исполняемые файлы в файлах *PNG*.
*TA*551	Скрывает закодированные данные для библиотек *DLL* вредоносных программ в формате *PNG*.
Tropic Trooper	Использует файлы *JPG* с зашифрованной полезной нагрузкой.
MuddyWater	Сохранят запутанный код *JavaScript* в файле изображения с именем *temp.jpg*.
*APT*37	Использует стеганографию для отправки изображений пользователям, в которые встроен шелл-код.

Наименование	Описание использования стеганографии
Leviathan	Использует стеганографию, чтобы скрыть украденные данные внутри других файлов, хранящихся на *GitHub*.
BRONZE BUTLER	Использует стеганографию в нескольких операциях, чтобы скрыть вредоносную полезную нагрузку.
Operation Ghost	Во время операции использовалась стеганография, чтобы скрыть полезную нагрузку внутри допустимых изображений.
Компьютерные атаки	
Operation Spalax	Для операции исполнители использовали упаковщики, которые считывают пиксельные данные из изображений, содержащих в себе вредоносные файлы, и создают следующий уровень выполнения на основе этих данных.
ABK	Может извлечь вредоносный переносимый исполняемый файл из фотографии.

Из приведенной выше таблицы можно выделить следующие основные методы использования стеганографии в тактике скрытого ввода и вывода информации:

- Хранение бэкдоров и шелл-кодов.
- Хранение и извлечение компонентов вредоносного программного обеспечения из контейнеров-изображений.
- Обфускация вредоносного кода.
- Скрытие информации в изображении для последующей передачи на сервер злоумышленника [13].

Помимо этого, злоумышленники могут использовать стеганографию в тактике сокрытия трафика управления между сервером атакующего и атакуемым объектом. Как правило, для этого используется стеганография в сетевом трафике, но также может применяться стеганография в изображении. В табл. 2 перечислено вредоносное программное обеспечение, хакерские группировки, а также каким образом использовалась стеганография в атаках по версии [9].

Таблица 2.

Наименование	Описание использования стеганографии
Вредоносное программное обеспечение	
Zox	Использует формат файла *PNG* для обмена данными с сервером атакующего.
Sliver	Может кодировать двоичные данные в *PNG*-файл для связи с сервером атакующего.
SUNBURST	Данные передаются как легитимный *XML*, связанный со сборками *.NET*, или как поддельный большой двоичный объект *JSON*.
RDAT	Может обрабатывать стеганографические изображения, прикрепленные к сообщениям электронной почты, для отправки и получения команд с сервера атакующего. Также может встраивать дополнительные сообщения в изображения формата *BMP* для связи с оператором *RDAT*.
LightNeuron	Управляется с помощью команд, которые встроены в *PDF*-файлы и *JPG*-файлы с использованием стеганографических методов.
Duqu	Когда команда и управление Duqu работают по протоколу *HTTP* или *HTTPS*, *Duqu* загружает данные на сервер атакующего, добавляя их в пустой файл *JPG*.
HAMMERTOSS	Управление осуществляется с помощью команд, которые добавляются к файлам изображений.

Наименование	Описание использования стеганографии
Хакерские группировки	
Axiom	Использует стеганографию, чтобы скрыть свои сообщения серверу атакующего.
Компьютерные атаки	
Operation Ghost	Во время атаки используется стеганография, чтобы скрыть связь между целевым объектом и сервером атакующего.

В фреймворке [9] для тактики сокрытия трафика управления между сервером атакующего и атакуемым объектом, в основном, перечислено применение стеганографии в медиафайлах, но к данной тактике также можно отнести применение стеганографии при осуществлении внеполосных атак, например, таких как *DNS-tunneling.*

Как правило, на внешних веб-серверах, находящихся в демилитаризованной зоне, разрешен обмен информации на 53 порту для протокола *DNS*. В результате чего, атакующий может использовать данный протокол как для проведения внеполосных атак на веб-приложения, так и для контроля сервера в случае, если он уже захвачен. Для этого атакующий отправляет *DNS*-запросы с веб-сервера на подконтрольный ему *DNS*-сервер и фиксирует пришедшие на него запросы. При этом информация передается в запрашиваемом поддомене, например: *base64({whoami}).evel.attack.com.*

Данную технику применения стеганографии в компьютерных атаках можно считать наиболее распространенной, так как она используется при эксплуатации таких уязвимостей как *SSRF, SQLi, Command injection* и *XSS*, а эксплуатация данных уязвимостей осуществляется часто из-за большого количества уязвимых веб-приложений согласно [14].

Заключение

Согласно изученным при проведении данного исследования источникам, можно сделать вывод, что в среде разработчиков вредоносного программного обеспечения наблюдается тенденция использования методов стеганографии не только для вывода информации из информационной инфраструктуры предприятий и сокрытия коммуникации с командным центром, но и для доставки модулей вредоносного программного обеспечения на целевой объект [15]. Иными словами, основные подходы, используемые злоумышленниками, заключаются в обфускации (сокрытии) вредоносных компонентов и их последующей доставки на атакуемую систему в «обход» средств защиты информации (СЗИ).

В настоящий момент уже имеются случаи успешной реализации атак с применением стеганографии, в связи с чем в сообществе специалистов компьютерной безопасности выделяются конкретные атаки, реализующие их группировки, программное обеспечение, тактики и техники, отражающие подходы и вектора атак злоумышленников (табл. 2).

В связи с этим, развитие стеганографических техник доставки вредоносного программного обеспечения открывает новые векторы для атак с использованием социальной инженерии, упрощая при этом процесс манипуляции атакуемым работником. Таким образом, организация со зрелым уровнем информационной безопасности должна реализовывать комплексные меры по обеспечению информационной безопасности, как на программно-аппаратном, так и на организационном уровнях. В том числе организация должна осуществлять постоянное тестирование и обучение работников правилам информационной безопасности, а для работников отделов информационной безопасности и

информационных технологий должны проводиться периодические киберучения на предмет противостояния новым угрозам.

Литература

1. Ушаков Д.Н. Толковый словарь русского языка // Под ред. Д.Н. Ушакова. Д.Н. М.: Гос. ин-т «Сов. энцикл.»; ОГИЗ; Гос. изд-во иностр. и нац. слов., 1935-1940. (4 т.). – С. 88405.
2. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие // Интермедиа. – Санкт-Петербург, 2017. – С. 312.
3. В Китае принят закон о криптографии. URL: http://d-russia.ru/v-kitae-prinyat-zakon-o-kriptografii.html. (Дата обращения - февраль2024).
4. Encryption Law of the People's Republic of China (Adopted at the 14th meeting of the Standing Committee of the 13th National People's Congress on October 26, 2019) URL: http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml%20 (Дата обращения – февраль 2024).
5. Федосенко М.Ю. Социологическое исследование осведомленности выпускников образовательных учреждений в возможностях скрытого обмена данными в интернете // Скиф. Вопросы студенческой науки, 2022. – № 1 (65). – С. 287-295.
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: – URL: https://fstec.ru/en/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/bazovaya-model-ot-15-fevralya-2008-g (дата обращения – февраль 2024).
7. Методика оценки угроз безопасности информации: – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения – февраль 2024).
8. Федосенко М.Ю., Беззатеев С.В. Анализ проблематики применения методов стеганографии при осуществлении противоправных действий и ее роли в цифровой криминалистике // Проблемы информационной безопасности. Компьютерные системы, 2023. – № 3 (56). – С. 33-57.
9. Cyber Kill Chain: – URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения – февраль 2024).
10. MITRE ATT&CK Enterprise: – URL: https://attack.mitre.org/tactics/enterprise/ (дата обращения – февраль 2024).
11. Целевые атаки типа Duqu 2.0 – URL: https://www.kaspersky.ru/resource-center/threats/duqu-2?ysclid=lsek9g30qx963283925 (дата обращения – февраль 2024).
12. 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.
13. 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.
14. OWASP Top 10 Web Application Security Risks: – URL: https://owasp.org/www-project-top-ten/ (дата обращения – февраль 2024).
15. Никулина Т.В. Выявление вредоносного кода в графических файлах, внедренного с помощью методов стеганографии // Матрица научного познания, 2021. – № 1-2. – С. 62-67.