kaspersky

Стеганография

Методические рекомендации для учителя

kaspersky

Стеганография

Методический материал носит рекомендательный характер, и учитель, принимая во внимание особенности класса, может изменять вопросы и дополнять задания.

Цель урока:

Сформировать знания и умения у учащихся о методах сокрытия факта передачи информации и провести практическую работу на основе графических файлов для закрепления материала.

Ключевые слова:

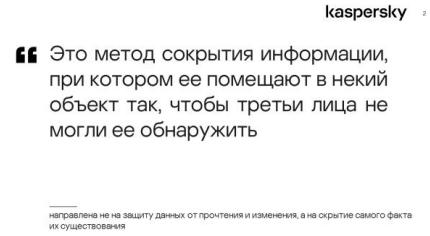
- **Стеганография**
- **Сокрытие информации**
- **Гистограммный анализ**
- **Zero.T**
- **CTF-соревнование**

Методическое обеспечение и средства обучения:

- **Презентация**
- **Материал для учителя**
- **ПК с доступом в сеть Интернет**
- **Изображения для практической работы**

Таблица 1. Комментарии к каждому слайду

Слайд	Комментарии
	После приветственных слов и обозначения темы мероприятия, следует провести опрос: знакомы ли учащиеся с понятием «стеганография»? Так как необходимо обозначить различие между шифрованием данных и стеганографией, то учащимся можно задать следующие наводящие вопросы: • Для чего необходимо защищать передаваемые сообщения? • Какие текстовые сообщения несут информативную нагрузку, а какие нет, то есть какие необходимо шифровать, а какие можно передавать в открытом доступе? • В чем заключается процесс шифрования данных и какие алгоритмы вам известны? • В чем различие симметричного и асимметричного методов шифрования? И после проведения серии вопросов и дискуссии актуализировать мотивационный компонент рассмотрения темы стеганография – сокрытие самого факта передачи необходимой информации.



Рассматривая определение стеганографии, следует поставить акцент на том, что в отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования.

Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания.

Спрятать секретное послание можно практически в любой цифровой объект – текстовый документ, лицензионный ключ, расширение файла. Однако один из самых удобных «контейнеров» – медиафайлы (картинки, аудио, видео и так далее). Они обычно достаточно большие сами по себе, а значит и вшитая информация может быть не такой маленькой.

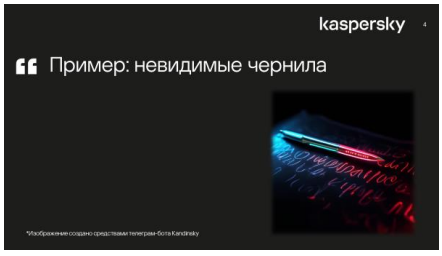
Секретную информацию можно записать в метаданные файла или же прямиком в основное содержимое.

Исторически впервые понятие стеганографии было введено в 1499 году, но сам метод существовал очень давно.

В течение всего XX века активно развивалась как стеганография, так и наука об определении факта внедрения информации в контейнер – стегоанализ.

Легенды донесли до нас метод, который использовался в Римской империи: для доставки сообщения выбирали раба, голову которого брили, а затем с помощью татуировки наносили текст. После того, как волосы отрастали, раба отправляли в путь. Получатель сообщения снова обривал голову раба и читал сообщение.

Проанализировав этот процесс, можно сказать, что для посторонних это была продажа рабов, без какого-то другого закладываемого смысла. На деле же скрывался сам факт передачи информации.



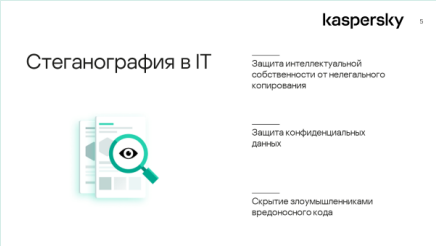
Одна из форм стеганографии – невидимые чернила, вещество, используемое для письма, которое становится невидимым при нанесении, либо вскоре после него, и позже может стать видимым с помощью некоторых средств.

К примеру, если в качестве чернил для бумаги используется молоко, то, нагрев поверхность бумаги, можно проявить написанное.

У многих учащихся, возможно, была ручка с невидимыми чернилами на одном конце и с неоновой лампой на другом, которая позволяла проявить написанное.

Представим процесс стеганографии с использованием невидимых чернил. Пусть необходимо передать какую-то секретную информацию. На листе бумаге обычными чернилами наносится текст, который не несет информативной нагрузки (приветствие, информация о погоде и т.д.). Невидимыми чернилами на свободном месте листа наносится секретная информация. Затем этот лист отправляется адресату, который уже знает о хранении дополнительной информации и способе ее

получения. Но, если кто-то перехватывает послание, то увидит только ту информацию, которая не содержит ничего секретного.

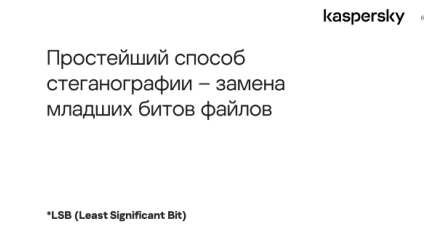


Возникает вопрос: для чего необходима стеганография на сегодняшний момент? Возможные варианты учащиеся смогут предложить сами.

Стеганография в IT используется для:

- Защита интеллектуальной собственности от нелегального копирования.
- Защита конфиденциальных данных.
- Скрытие злоумышленниками вредоносного кода.

Одним из явных примеров стеганографии за последнее время является NFT. Так, многие коллекционеры цифрового искусства получали уникальную картинку, принадлежность и ценность которой можно проверить через специальные технологии. Другим примером являются голливудские звезды, которые покупали одну конкретную картинку из ограниченной коллекции, а после получали специальный программный код, который из картинки извлекал скрытую информацию о закрытой вечеринке.



После рассмотрения различных примеров использования стеганографии вполне логично возникает вопрос о методах ее создания.

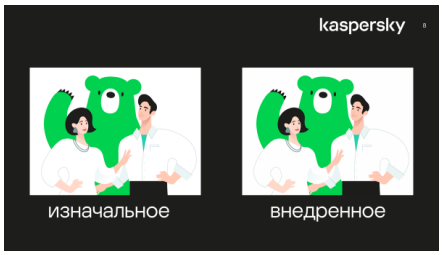
Простейший способ стеганографии – замена младших битов файлов. Чем меньше битов задействовано, тем меньше артефактов получает оригинальный контейнер после внедрения.

Распространен и метод сокрытия информации при помощи младших бит палитры – информация встраивается не в наименее значащие биты контейнера, а в наименее значащие биты палитры, очевидный недостаток такого метода – низкая емкость контейнера.

Рассмотрим пример стеганографии методом сокрытия текстовой информации в графическом файле в младших битах палитры.

На слайде представлен фрагмент кода рисунка.

Пусть нам необходимо спрятать букву «И». Ее код распределяем по младшим битам палитры (отмечены красным). И можно заметить, что некоторые новые фрагменты совпадают со старыми, это означает, что пиксель не поменяет свой цвет и внешне не будет никах изменений. В некоторых случаях в младших битах произошло изменение 0 на 1 или наоборот, что повлияет на смену оттенка цвета, но зрительно это не будет заметно, так как эти оттенки являются близкими друг к другу оттенками одного цвета.

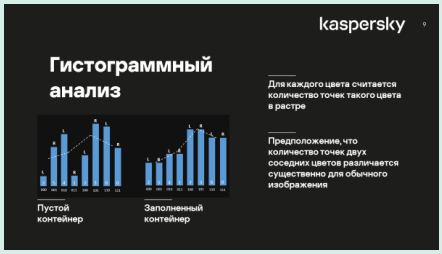


На слайде представлено две картинки.

Изначальное графическое изображение и внедренное графическое изображение, в которое вшили стихотворение Пушкина «У лукоморья дуб зеленый».

Заметим, что на глаз нет никакой разницы.

Отметим, что многим покажется, что одно изображение светлее другого или что-то подобное. Но это объяснимо тем, что разные углы обзора экрана монитора, электронной доски или другого гаджета, а сами картинки зрительно не отличаются.



После рассмотрения методов сокрытия информации в графический файл вполне закономерно возникает вопрос: как можно выявить наличие стеганографии?

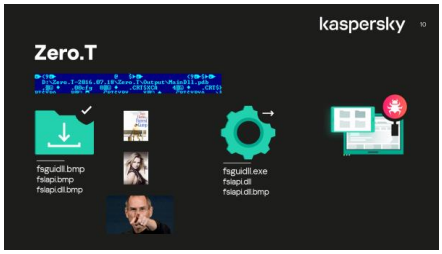
Существует множество различных методов. Но остановимся на том, который будет понятен учащимся и не составит труда для восприятия – статистический метод анализа – гистограммный метод.

Описываемый метод, предложенный в 2000 году Андресом Вестфелдом и Андреасом Пфитцманом, также известен как «хи-квадрат»-метод.

Весь растр анализируется, для каждого цвета считается количество точек такого цвета в растре (для простоты здесь говорим про изображение, имеющее одну цветовую плоскость).

Метод исходит из предположения, что количество точек двух соседних цветов («соседние» цвета – цвета, которые отличаются только наименее значимым битом) различается существенно для нормального, обычного изображения (пустого контейнера). И количество пикселей таких цветов является примерно одинаковым для заполненного контейнера.

Проще говоря, чем плавнее получается кривая на гистограмме, тем больше вероятность, что в изображении что-то дополнительно содержится, и следует более детально изучить файл.



Подробно рассмотрим пример использования стеганографии в киберугрозах – Zero.T

Этот загрузчик был обнаружен Лабораторией Касперского в конце 2016 года, но первое описание было опубликовано компанией Proofpoint.

Угрозу назвали Zero.T, так как такая строка присутствует в его исполняемом коде.

Не останавливаясь на попадании в систему и закреплении в ней, Zero.T скачивает полезную нагрузку в виде файлов: fsguidll.bmp, fslapi.bmp, fslapi.dll.bmp.

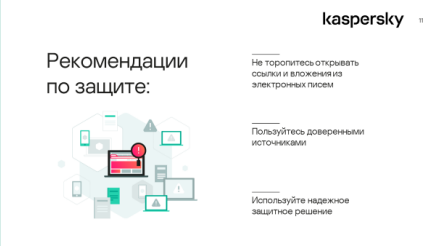
На поверку эти три BMP-файла оказались картинками с изображением афиши к фильму «Форрест Гамп» и портретами Бритни Спирс и Стива Джобса.

Вопросы учащимся для размышления и дискуссии:

- Что известно про формат *.bmp?
- Может ли графический файл сам по себе нести угрозу?
- Что может смущать в названии загруженных графических файлов, описанных на слайде?

Zero.T обрабатывает данные картинки особым образом, после чего получает вредоносные модули (извлекает необходимую информацию и создает файлы): fsguidll.exe, fslapi.dll, fslapi.dll.bmp.

Таким образом, скачивание данных изображений и извлечение из них полезной нагрузки было второй волной атаки.



Общие рекомендации, которые позволяют защитить свое информационное пространство от вредоносного воздействия различных средств, в том числе и стеганографии:

- Не торопитесь открывать ссылки и вложения из электронных писем.
- Пользуйтесь доверенными источниками.
- Используйте надежное защитное решение.

Для проведения практической работы необходимо на каждый ПК учащегося скачать архив «Изображения для практической работы».

Извлечение текстовой информации из графических файлов будет осуществляться с помощью онлайн-калькулятора.

Рекомендуется создать какую-либо форму для ответов, чтобы фиксировать результаты учащихся и придать практической работе стиль соревнования.

Предложенный онлайн-калькулятор позволяет как скрыть текстовую информацию в изображении, так ее и извлечь. Нас интересует второе.

Учащиеся извлекают информацию и получают следующие данные:

- Image1: Метод шифрования показан на самом изображении.
  Полученную информацию учащиеся должны истолковать так, что необходимо посмотреть на саму картинку и логически догадаться, кто изображен и какое отношение данная фигура имеет к методу шифрования.
  Ответ: шифр Цезаря.

- Image2: 5.
  Полученную информацию учащиеся должны истолковать так, что шаг в шифре Цезаря равен 5.

- Image3: Пчу цьнчейчцд фйхжас фхузхесснцчус ж нцчухнн?

Учащиеся должны прийти к выводу, что в данном изображении содержится зашифрованная информация, но уже известен метод и ключ.
После расшифровки учащиеся узнают вопрос, на который нужно дать ответ: Кто считается первым программистом в истории?

Если учащиеся не могут самостоятельно ответить на поставленный вопрос, то могут осуществить поиск информации в сети Интернет.

Ответ: Августа Ада Лавлейс.

Подводим итоги занятия.

Контрольные вопросы:

- С каким новым понятием мы познакомились на занятии?
- Для чего используют стеганографию?
- С какими способами и методами стеганографии мы сегодня познакомились?
- Можно ли выявить стеганографию в графическом файле?

Благодарим за внимание.

www.kaspersky.com/
www.securelist.com