М. В. Слива, Д. Ю. Орлов
Нижневартовский государственный университет, г. Нижневартовск
УДК 004.491.22

ВНЕСЕНИЕ ВИРУСОВ В СИСТЕМУ С ПОМОЩЬЮ СТЕГАНОГРАФИИ

Аннотация. В статье рассмотрен способ внесения вирусов в ПК и их активации с помощью методов сокрытия данных в цифровых контейнерах. Рассказана методология и рассмотрена актуальность такого способа занесения вируса в систему.

Ключевые слова: стеганография, вирусы, информационная безопасность, изображения, трояны, скрипты.

Введение. Проблема исследования. Стеганография — наука о сокрытии данных и их передаче, без раскрытия прецедента передачи [1]. Из графиков в статье [2], публикационной активности за 2010-2019 гг., стеганография находится на втором месте. Из этого делаем вывод, что тема до сих пор актуальна. Согласно отчетам Лаборатории Касперского, начиная с 2011 г., случаи применения стеганографии в вирусах возросли в большей степени. Сегодня благодаря бурному развитию компьютерной техники, интернет-сети и новых каналах передачи данных появились новейшие методы стеганографии, основы которых являются особенностями представления данных в файлах компьютера, компьютерных сетей и так далее [3]. На данный момент согласно исследованиям [4], алгоритмы встраивания информации используют самые различные контейнеры для скрытой передачи данных. Например, в [5] описаны несколько способов сокрытия информации для внедрения в сетевой трафик. А в [6] рассматриваются основы стеганографических алгоритмов применительно учетных записей и информационной безопасности в корпоративной среде.

Исходя из вышеперечисленных исследований, неудивительно, что стеганографию используют и при написании вирусов, ведь это хороший и актуальный способ сокрытия и попадания в систему. И тут встает вопрос и проблема, как именно скрипт попадает в систему, каким образом становится вирусом и обходит обнаружение системой защиты устройства?

Материалы и методы. Материалами данного исследования стали статьи Лаборатории Касперского, отчеты Dr.Web и собственный опыт применения стеганографии с цифровыми данными.

Рассмотрим последний образец 2020 г. В мае 2020 г. выявлены атаки в системы внутри Германии, Италии, Англии и Японии. Приблизительно 40-50% мишеней нападающих — это разнообразные компании, участвующие в различных секторах экономики. Потерпевшими от атак фирмами стали, в том числе, поставщики аппаратного и программного обеспечения для компаний широкого спектра промышленности. Преступники используют для этих целей внедрение в документы Microsoft Office, PowerShell скрипты, а кроме того, различные техники затруднения обнаружения и рассмотрения вирусного софта.

Для первоначального направления атаки используются фишинговые письма с текстом на целевом для каждой конкретной жертвы языке. Вредоносная программа, используемая в этой атаке, выполняет деструктивную активность только в том случае, если операционная система имеет локализацию, соответствующую языку, использованному в фишинговом письме. Например, в случае атаки на компанию из Японии текст фишингового письма и документ Microsoft Office, содержащий вредоносный макрос, написаны на японском, а для успешной расшифровки модуля вредоносной программы операционная система должна иметь японскую локализацию.

В случае с документом Microsoft Office, в котором есть вирусный макрос, ситуация такая: после открытия, если пользователь согласится на исполнение содержимого документа, вредоносный макрос начнет свою работу. Основная работа состоит в исполнении PowerShell скрипта (рис 1.) несмотря на пользовательскую политику, без загрузки пользовательской конфигурации и в скрытом режиме.

Таким образом скрипт начинает скрытую работу в системе, не обнаруживая себя для некоторых активных антивирусных систем.

```
Function GeneralCatalogO
GeneralCatalog = "pzq /p pzq /p CBjREFuryy -rC    OLCnfF   -j 1 -abAvAgR  -ABCEbsVY
End Function

Function !AstReport()
lAstReport = "ynpr(',V/'))-ercynpr(';'/ + ') ),[VB.pBzceRFfVBa.pbZCErfFVBAzBQr]::QRpbzcerff ) |:
End Function
```

Рис. 1. Часть макроса, запускающая PowerShell-скрипт

Этот скрип выбирает URL из списка и загружает из публичного хостинга изображений контейнер с еще одним скриптом. Контейнером является изображение и скрипт начинает процесс извлечения данных из него. Это позволяет обойти такой метод защиты, как сканер сетевого трафика. Часто в контейнер-изображение прячут данные с помощью метода LSB (Least Significant Bit). По окончании работы процесса получается еще один PowerShell-скрипт, и он начинает свою работу. В данном случае это троян, он крадет пароли от FTP-клиентов и электронной почты, а также сканируют интернет-трафик браузеров, чтобы украсть данные для авторизации на различных сайтах, также он может красть данные кошельков для криптовалюты. Все зависит от разработчика и семейства трояна.

Для разбора, возьмем еще один вирус-загрузчик: Zero.T. Попадание в систему, может быть, самыми различными способами, от спама и фишинга до прямого занесения скрипта в систему. Zero.T скачивает своим модули в виде Bitmap-файлов (.bmp). Тем самым обходит антивирусную систему. После чего обрабатывает их, получая вредоносную программу на выходе (рис 2.).

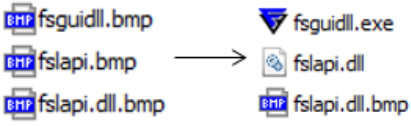

Рис. 2. Модули Zero.T до и после обработки

После обработки, загрузчик запускает в систему троян PlugX. PlugX — это вредоносный инструмент удаленного администрирования, позволяющий злоумышленникам управлять зараженными компьютерами без физического доступа.

Результаты. По итогу изучения двух выше представленных вирусов и основываясь на опыте написания курсовой, была разработана программа для записи данных в изображение методом LSB. Приложение написано на Java с использованием библиотеки Swing. Оно состоит из двух частей. Первая часть шифрует код в изображение. Вторая часть делает обратную процедуру и запускает дешифрованный

скрипт. Ниже представлен интерфейс программы и простой скрипт, записанный в контейнер-изображение (рис. 3).

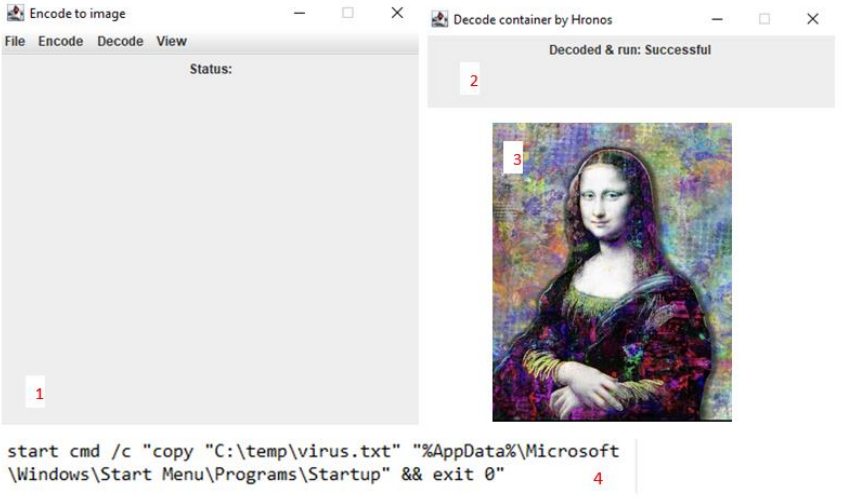

Рис. 3. 1) интерфейс шифровальщика; 2) программа исполнитель; 3) изображение-контейнер; 4) скрипт в контейнере

Заключение. Злоумышленники совершенствуют навыки применения и разработки вирусов, и стеганография стала мощным инструментом в их руках. Антивирусные системы разрабатывают способы обнаружения таких вирусов. Но автоматизация проверки файлов на присутствие скрытых данных является сложным процессом, на который влияет множество факторов, начиная от энтропии изображений и заканчивая множеством самих алгоритмов стеганографии и их прогресса с развитием информационных технологий. На данный момент из-за этих факторов популярность такого способа доставки вируса в систему возросла и актуальна. Но также совершенствуются и методы раскрытия подобного вредоносного софта.

Результатом данной работы стал программный комплекс из двух приложений: первое скрывает зловредный код в изображении, второе считывает этот код с изображения и запускает его в системе.

СПИСОК ЛИТЕРАТУРЫ

1. Белкина Т. А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности / Т. А. Белкина. — Текст : электронный // Молодой ученый. — 2018. — № 11 (197). — С. 36-44. — URL: https://clck.ru/34Xbjv (дата обращения: 09.05.2023).
2. Арутюнов В. В. Сравнительный анализ результативности и востребованности итогов научной деятельности российских ученых по актуальным направлениям исследований в области информационной безопасности / В. В. Арутюнов — Текст : электронный // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. — 2020. — № 4. — С. 31-45. — URL: https://clck.ru/34XbmN — (дата обращения: 16.05.2023).
3. Стеганография в кибератаках. Заключение. — Текст : электронный // — URL: https://clck.ru/34XbkH (дата обращения: 09.05.2023).
4. Боброва Е. М. Защита информации с использованием методов стеганографии / Е. М. Боброва, С.Н. Борисова. — Текст : электронный // Успехи современного естествознания. — 2011. — № 7. — С. 80-81. — URL: https://clck.ru/34Xbky (дата обращения: 10.05.2023).
5. Красов, А. В. Метод обнаружения сетевой стеганографии на основе машинного обучения / А. В. Красов — Текст : электронный // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. — 2022. — № 3. — С. 100-108. — URL: https://clck.ru/34Xbke (дата обращения: 16.05.2023).
6. Хорев, П. Б. Применение стеганографии в корпоративной среде / П. Б. Хорев, А. В. Сергеев — Текст : электронный // Информационно-технологический вестник. — 2020. — № 4(26). — С. 104-109. — URL: https://clck.ru/34Xbvy (дата обращения: 16.05.2023).