Министерство образования ХХХ

Государственное бюджетное профессиональное образовательное учреждение

ХХХ «Колледж «ХХХ»

09.02.07

ОТЧЕТ

По лабораторным работам

МДК 04.02 Внедрение и поддержка компьютерных систем

ККОО.ПМ.ХХХ.000

Студент ХХХ Максимова У. Р.

Преподаватель ХХХ

Дата защиты_____ Оценка_____

2022

Лабораторная работа № 5.1

Изучение путей распространения и форм проявления компьютерных вирусов

Цель работы и содержание: изучить пути распространения и формы проявления компьютерных вирусов.

Ход работы

В настоящее время большое количество разработчиков антивирусного ПО на своих web-сайтах размещают информацию о новых вирусных угрозах и мерах по их устранению.

В лабораторной работе необходимо оформить отчёт таким образом, чтобы он содержал

1). Теоретическое описание известных путей распространения и форм проявления компьютерных вирусов

2). Описание конкретных:

- путей распространения компьютерных вирусов;
- форм проявления компьютерных вирусов;
- действий по устранению работы компьютерных вирусов.

Bad Rabbit.

Деструктивная активность:

Дроппер вымогателя распространяется за счет попутных загрузок (drive-by). Цель посещает вполне легитимный сайт, а зловредный дроппер меж тем загружается из инфраструктуры злоумышленника. Эксплойты не используются, жертва запускает дроппер вручную — тот притворяется инсталлятором Adobe Flash.

Дроппер вымогателя загружается с hxxp://1dnscontrol.com/flash_install.php.

По нашим данным, жертвы перенаправляются на вредоносный ресурс с легитимных и безвредных новостных сайтов.

Загруженный файл с именем install_flash_player.exe запускается жертвой вручную. Для корректной работы он нуждается в повышенных административных привилегиях, которые и пытается получить с помощью стандартного запроса UAC. При запуске он сохранит вредоносную библиотеку DLL как C:\Windows\infpub.dat и запустит ее с помощью rundll32.

Bad Rabbit шифрует файлы и жесткий диск по типичной для шифровальщиков схеме, с помощью алгоритмов AES-128-CBC и RSA-2048. Что интересно, троянец сверяет хэши имен запущенных процессов с заданной таблицей. И алгоритм хэширования похож на тот, что использовался знаменитым exPetr.

Судя по всему, исполняемый файл dispci.exe создан на основе кода безвредной утилиты DiskCryptor. Он действует как модуль шифрования диска, который к тому же устанавливает модифицированный загрузчик и препятствует нормальному процессу загрузки зараженной машины.

Рекомендации по защите: Пользователи могут чувствовать себя защищенными, если у них активированы все защитные механизмы продуктов антивирусов, а также обновлены их базы данных

В качестве дополнительных мер предосторожности имеет смысл заблокировать исполнение файлов C:\Windows\infpub.dat и C:\Windows\cscc.dat.

Контрольные вопросы

1. Где можно взять описание работы компьютерных вирусов (конкретные примеры)?

В интернете при запросе нужного вам вируса.

2. Какие есть пути распространения компьютерных вирусов?

Все съемные носители, в случае заражения файлов, сами файлы, локальные сети, загрузка зараженного файла из интернета, различные сети, вроде Bluetooth.

3. Какие есть формы проявления компьютерных вирусов?

- прекращение работы или неправильная работа ранее успешно функционирования программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

4. Какие формы проявления компьютерных вирусов наиболее незаметны для пользователя?

Наиболее незаметны для пользователя скрытые проявления.

В отсутствие явных или косвенных проявлений о присутствии вируса можно судить, например, по необычной сетевой активности, когда ни одно сетевое приложение не запущено, а значок сетевого соединения сигнализирует об обмене данными. Другими признаками могут служить незнакомые процессы в памяти или файлы на диске.

Скрытые проявления включают:

- Наличие в памяти подозрительных процессов
- Наличие на компьютере подозрительных файлов
- Наличие подозрительных ключей в системном реестре Windows

- Подозрительная сетевая активность