

**«Лабораторная работа №1 «Изучение путей распространения и форм проявления компьютерных вирусов»»**

**Выполнил(а):**

студент группы 2ИСП11-18

Кашутина М.А.

**Проверил**: преподаватель Возвахов Д.А.

Москва

2022

Оглавление

[Вирус №1. 3](#_Toc117859751)

[Как избавиться от вируса Trojan-Ransom.Win32.Wanna.m? 4](#_Toc117859752)

[Вирус №2 5](#_Toc117859753)

[Как избавиться от вируса Trojan-Spy.Win32.Zbot? 6](#_Toc117859754)

[Как предотвратить атаку Trojan-Spy.Win32.Zbot в будущем? 7](#_Toc117859755)

[Вирус №3 8](#_Toc117859756)

[Как избавиться от Worm:Win32/Cridex на нашем ПК? 9](#_Toc117859757)

[Контрольные вопросы 10](#_Toc117859758)

**Лабораторная работа №1**

**«Изучение путей распространения и форм проявления компьютерных вирусов»**

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

## Вирус №1.

Trojan-Ransom.Win32.Wanna.m

|  |  |
| --- | --- |
| **Класс** | Trojan-Ransom |
| **Платформа** | Win32 |
| **Описание** | Вредоносное ПО WannaCry, шифрующее файлы пользователя и распространяющееся по сети путем эксплуатации уязвимости в SMB.  Наиболее популярный путь распространения – электронная почта. Обычно он скрывается в письмах, которые якобы отправлены от известных организаций.  После заражения вирус выполняет следующие действия:   * шифрование данных; * изменяет системные файлы и папки; * собирает информацию о пользователе; * отслеживает работу в браузере, при необходимости модифицирует данные.   После того, как важные данные будут зашифрованы, модифицированы или уничтожены с вами могут связаться мошенники, с предложением восстановить все данные за определенную плату. |

## Как избавиться от вируса Trojan-Ransom.Win32.Wanna.m?

1. Нужно закрыть все работающие приложения
2. Запустить диспетчер задач, при помощи комбинации клавиш (Ctrl+Alt+Delete). Перейти на вкладку «Процессы». Находим процесс mssecsvc.exe, правой кнопкой мыши -> открыть место хранения файла.
3. Проверить папку с файлом антивирусом. Антивирус должен удалить этот вирус. Если это не произошло, то выполняем следующие действия:

3.1 Останавливаем процесс mssecsvc.exe

3.2 Удаляем файл mssecsvc

3.3 Очищаем корзину

3.4 Перезагружаем ПК

3.5 Скачиваем антивирус

3.6 Проверяем ПК на вирусы

Если при выполнении этих действий ничего не произошло, то нужно перезагрузить ПК и при его загрузке нажимать на клавишу F8, после чего выбрать загрузку в безопасном режиме. После загрузки в безопасном режиме удалить файл, и выполнить пункты 3-6 загрузившись в обычном режиме.

## Вирус №2

Trojan-Spy.Win32.Zbot

|  |  |
| --- | --- |
| **Класс** | [Trojan-Spy](https://threats.kaspersky.com/ru/class/Trojan-Spy/) |
| **Платформа** | Win32 |
| **Описание** | Вредоносные программы этого семейства используются для кражи аутентификационных данных пользователя к различным сервисам, например, к сервисам онлайн-банкинга. Кроме того, такие вредоносные программы предоставляют злоумышленнику возможность удаленного управления зараженной машиной.  Вредоносные программы этого семейства обладают богатым функционалом, таким как: перехват данных, подмена DNS, снятие скриншотов экрана, получение паролей из хранилища Windows, загрузка и выполнение файлов на компьютере пользователя, атака других компьютеров в сети Интернет.  Загрузка бесплатных программ, просмотр видео для взрослых или игра в онлайн игры, использование пиратского программного обеспечения или торрент-файлов, Обмен одноранговой сетью, открытие нежелательной почты вложения и т.д. являются основными причинами его проникновения. Будьте внимательны при установке сторонней программы. Внимательно прочитайте правила и условия и всегда выбирайте пользовательские/расширенные настройки вместо ‘Default ‘. Кроме того, Избегайте посещения подозрительных веб-доменов, поскольку это не просто для новичка, чтобы узнать, какой сайт содержит вредоносные питания. Игнорировать сомнительные сообщения, поступающие из неизвестного источника, они могут выглядеть аутентичными, но включать фиктивные содержание.   * Еще несколько симптомов: * отображает коммерческое содержимое на каждой посещаемой вами веб-странице и плохо прерывает веб-сеансы * руины важные системные файлы, которые обеспечивают бесперебойную работу ПК и предотвращает устройство от нормальной работы * съедает огромное количество ресурсов памяти и сильно замедляет общую производительность системы * приносит много других пресловутых инфекций, таких как Adware, руткиты, черви, шпионские программы, вымогателей и т.д. в системе и вызывает больше повреждений |

## Как избавиться от вируса Trojan-Spy.Win32.Zbot?

Метод 1. Можно вручную удалить Trojan-Spy.Win32.Zbot **с Windows PC.**

1. Сначала нужно перезапустить ПК в безопасном режиме. Таким образом, ваш компьютер будет работать только необходимые запуска служб и исключает все ненужные тяжелый процесс.
2. Откройте диспетчер задач при помощи сочетания клавиш Ctrl+Alt+Delete. Найдите процесс, связанный с Trojan-Spy.Win32.Zbot и закончить свою задачу, нажав на опцию «Завершить задачу».
3. Откройте «Run» вариант и введите команду regedit для открытия редактора реестра. Найдите поврежденные и вредоносные записи и удалите каждый из них. (тщательно)
4. Откройте панель управления и нажмите на «Добавить/Удалить» программу. Поиск подозрительных программ, которые имеет отношения с Trojan-Spy.Win32.Zbot и удаленным их мгновенно.
5. После Поиск и сканировать все файлы и папки, связанные с Trojan-Spy.Win32.Zbot и мгновенно удалить их по одному

Метод 2. Можно удалить Trojan-Spy.Win32.Zbot автоматически при помощи инструмента PWS:Win32/ZbotPWS:Win32/Zbot.

1. Загрузите и установите автоматический инструмент в вашем ПК Windows. Начните процесс сканирования, нажав на опцию «Сканировать компьютер».
2. **Custom Scan:**это специальная функция, которая используется, если вы хотите сканировать определенной части компьютера, такие как сканирование руткитов, файлы браузера, системной памяти и особый раздел жесткого диска и так далее. Это как быстрое сканирование, которое экономит время и является столь же эффективным, как полное сканирование.
3. **Защита системы:**Эта функция является все в одной безопасности функции для управления процессом, управления Active X, раздел реестра и так далее. Он блокирует все виды вредоносных записей и обеспечивает полную гарантию от нежелательного изменения внутренних параметров.
4. **Help Desk:**Эта функция может прийти активно, когда вы все еще не удовлетворены производительность вашего ПК даже после завершения сканирования. Здесь пользователь может соединиться с удаленной технической службы для заказной помощи в решении конкретных проблем. Системы и пользовательские исправления системы являются ее мощной защиты механизма.
5. **Сеть караул:**это специальная функция для плавного сетевого подключения и защиты от нежелательного изменения и несанкционированного доступа. Он будет защищать параметры DNS и размещение файлов.
6. **Проверка времени планировщика:**Эта функция, как настроить планировщик, который позволяет пользователю сканировать их системы в заданное время, на основе ежедневной, еженедельной или ежемесячной основе.

## Как предотвратить атаку Trojan-Spy.Win32.Zbot в будущем?

* Остерегайтесь неизвестные подозрительные ссылки и избегать нажатия на них.
* Не загружайте неизвестных прибыльный freeware, потому что они, как правило, содержат скрытые коды с ними.
* Не получить манипулировать с невероятными предложениями, торговые преимущества, Лаки схем или победитель мошенничества и др.
* Не загружайте подозрительные плагины и дополнения, которые утверждает, предоставляют дополнительные возможности бесплатно, но на самом деле загружает пакеты вредоносного программного обеспечения.
* Отключите все дополнительные программы, которые используются очень меньше, таких как Active X, подозрительные файлы cookie и расширение и др.
* Удалить временные файлы, записи реестра неизвестных, печенье и др. на регулярные промежутки времени.

## Вирус №3

Worm:Win32/Cridex

|  |  |
| --- | --- |
| **Класс** | [Worm](https://threats.kaspersky.com/ru/class/Worm/) |
| **Платформа** | [Win32](https://threats.kaspersky.com/ru/platform/Win32/) |
| **Описание** | Первоначально Worm.Win32.Cridex был червем, который распространялся через съемные диски. За годы эволюции червь приобрел функционал полноценного банкера.  Последние версии вредоносной программы имеют следующие возможности: • вставка веб-инжектов; • создание снимков экрана и кликшотов (снимков веб-страниц при нажатии пользователем на клавишу мыши); • блокирование доступа к определенным веб-адресам; • перенаправление пользователя с одного веб-адреса на другой.  Worm.Win32.Cridex тщательно скрывает свой командный сервер с помощью P2P-сети и прокси-сервера.  При взаимодействии с командным сервером используются симметричный алгоритм шифрования, а также дополнительное XOR-шифрование для полученного от командного сервера конфигурационного файла.  Он использует несколько иллюзорных трюков и методов, чтобы проникнуть в целевую систему, некоторые из них наиболее распространены:   * Вложения спама в электронной почте * Бесплатная загрузка * Через использование пиратского программного обеспечения или торрент-файлов * Совместное использование одноранговых сетей * Передача данных через зараженные удаленные диски |

## Как избавиться от Worm:Win32/Cridex на нашем ПК?

Можно удалить вирус Cridex вручную.

1. Завершить процессы и удалить соответствующие файлы KB(8 digit number).exe (только те файлы, которые находятся в списке вредоносных)
2. Удалить папки «no information»
3. Удалить ключи и\или значения ключей реестра:

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
Value: KB(8 digit number).exe

1. Сбросить настройки браузеров (для каждого браузера своя инструкция)

## Контрольные вопросы

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

Конкретные примеры можно взять по ссылкам ниже:

<https://threats.kaspersky.com/ru/threat/Trojan.Win32.Neurevt/>

<https://threats.kaspersky.com/ru/threat/Virus.Win32.Nimnul/>

1. **Какие есть пути распространения компьютерных вирусов?**

* **Уязвимость операционной системы.**
* **Уязвимость в браузере**
* **Качество антивируса хромает**
* **Глупость пользователя**
* **Сменные носители.**

1. **Какие есть формы проявления компьютерных вирусов?**

* Мерцание экрана.
* Медленная работа компьютера.
* Появление на экране непредусмотренного сообщения.
* Блокировка ввода с клавиатуры.
* Изменение размеров файла, даты создания программ.
* Значительное увеличение файлов на диске.
* Частые зависания и сбои в работе компьютера.
* Уничтожение файлов или частичное разрушение.
* Блокировка записи на жесткий диск.

1. **Какие формы проявления компьютерных вирусов наиболее незаметны для пользователя?**

Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметно. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

* некоторые программы перестают работать или начинают работать неправильно;
* на экран выводятся посторонние сообщения, символы и т.д.;
* работа на компьютере существенно замедляется;
* некоторые файлы оказываются испорченными и т.д.