

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

**Выполнили:**

студенты группы 2ИСП11-18

Радченков В.В.

Зверев Н.Д.

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

Москва

2022

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

Троян: W32/Trickbot

Классификация

Категория: Вредоносное ПО

Тип: Троян

Платформа: W32

Псевдоним: Трикбот

Информация

Trickbot – это банковский троян, который крадёт учётные данные для входа на банковские сайты.

Технические детали

Троян Trickbot пытается украсть учетные данные для входа в определенные банки в определенных странах, при этом список целевых банков регулярно меняется и пополняется.

Причины возникновения вируса на ПК

Операторы трояна Trickbot обычно распространяют вредоносное ПО в виде файла, прикрепленного к спам-сообщениям электронной почты. Как и в большинстве таких сообщений, содержание электронной почты выглядит безопасно, чтобы пользователь мог открыть вложение. При этом запускается встроенный в него скрипт, который загружает троян Trickbot с удаленного сервера, устанавливает и запускает его на компьютере пользователя.

Кража паролей от банковских сайтов

Троян Trickbot может использовать любой из двух методов, чтобы обманом заставить пользователя невольно выдать свои учетные данные для входа. Первый метод (известный как статическая инъекция) заключается в замене безопасной страницы входа на банковский сайт поддельной, которая выглядит почти точно так же. Второй метод (известный как динамическая инъекция) перенаправляет веб-браузер на сервер, находящийся под контролем оператора трояна, всякий раз, когда пользователь вводит URL-адреса целевых банковских сайтов. В любом случае, если пользователь вводит свои данные для входа на поддельной странице, информация перехватывается и отправляется операторам. Украденные данные затем могут быть использованы для совершения финансового мошенничества.

|  |  |
| --- | --- |
| Название вируса | Trickbot |
| Тип угрозы | Троян, вирус для кражи паролей, банковское вредоносное ПО, шпионское ПО |
| Названия обнаружения | Avast (Win32:Malware-gen), BitDefender (Trojan.Agent.CWSV), ESET-NOD32 (Win32/TrickBot.AJ), Kaspersky (Trojan.Win32.Mansabo.awr) |
| Симптомы | Отсутствуют, так как троян создан для того, чтобы без ведома пользователя красть пароли от банковских сайтов |
| Методы распространения | Вложения электронной почты, содержащие троян |
| Ущерб | Кража паролей, банковских аккаунтов и кража личных данных |
| Рекомендации по удалению | Чтобы удалить вирус нужно воспользоваться антивирусом. Рекомендуется пользоваться антивирусом Kaspersky Antivirus |

Рекламный вирус: savefrom.net

Классификация

Категория: Вредоносное ПО

Тип: Рекламный вирус

Платформа: W32

Псевдоним: Реклама от savefrom.net

Информация

savefrom.net – это рекламный вирус, который на ПК будет открывать сайты с рекламой и показывать ненужную пользователю информацию.

Технические детали

savefrom.net содержит различные рекламные объявления, при нажатии на которые открываются сомнительные веб-сайты. Посещение этих веб-сайтов и нажатие отображаемой на них рекламы может привести к загрузке и установке различных потенциально нежелательных приложений (PUA).

Причины возникновения вируса на ПК

В некоторых случаях пользователи могут загружать потенциально нежелательные приложения с веб-сайтов, которые разработчики используют для рекламы, однако люди чаще устанавливают PUA, нажимая на навязчивую, вводящую в заблуждение рекламу, или когда разработчики программного обеспечения используют «связку», обманчивый маркетинговый метод, который разработчики используют для того чтобы обманным путем заставить людей загружать и устанавливать PUA вместе с другими обычным программным обеспечением, которое люди обычно загружают намеренно.

Как избежать скачивание рекламных вирусов и нежелательных приложений?

Все программные обеспечения должны быть скачаны с официальных сайтов и источников. Нужно избегать скачивание ПО с сайтов с плохой репутацией. Так же, нельзя нажимать на рекламные объявления в интернете.

|  |  |
| --- | --- |
| Название вируса | savefrom.net |
| Тип угрозы | Рекламный вирус, всплывающие окна |
| Ссылки обнаружения | de.saveform.net, en.saveform.net, es.saveform.net, rek.saveform.net, ru.saveform.net, tr.saveform.net |
| Симптомы | Рекламные объявления, всплывающие, не связанные, с сайтами которые посещал пользователь |
| Методы распространения | Обман через рекламные всплывающие окна |
| Ущерб | Ухудшение работоспособности ПК, заражение дополнит. вирусами |
| Рекомендации по удалению | Чтобы удалить вирус нужно воспользоваться антивирусом. Рекомендуется пользоваться антивирусом Kaspersky Antivirus |

Фейковый антивирус: Total Antivirus 2020

Классификация

Категория: Вредоносное ПО

Тип: Фейковый антивирус

Платформа: W32

Псевдоним: Total Antivirus 2020

Информация

Total Antivirus 2020 – это ПО рекламировалось как анти-вирус, который помогает пользователю устранять вирусы, но на самом деле анти-вирус не может выполнить поставленные задачи, соответственно он нагружает ПК пользователя и некоторые пользователи приобрели этот анти-вирус, «выкинув деньги на ветер».

Технические детали

После скачивания данного ПО, на ПК пользователя могут появиться вирусы, антивирус об этом сообщит и пользователю придётся купить этот фейковый антивирус, для того чтобы избавиться от несуществующих вирусов.

Причины возникновения вируса на ПК

Пользователю может понадобиться скачать антивирус для того, чтобы обезопасить свой ПК от вредоносных программ. При выборе антивируса он может наткнуться на Total Antivirus 2020, подумав, что это настоящий антивирус, когда на самом деле это ПО предназначено для обмана пользователя.

Как отличить настоящий антивирус от фейкового?

Для того, чтобы скачать настоящий антивирус, который действительно выполняет необходимые функции, нужно перед скачиванием прочитать про него отзывы, узнать репутацию данного антивируса или посоветоваться с экспертами компьютерной безопасности. Примеры настоящих антивирусов: Bitdefender, Kaspersky, Norton, Avast и т.д.

|  |  |
| --- | --- |
| Название вируса | Total Antivirus 2020 |
| Тип угрозы | Фейковый антивирус |
| Названия обнаружения | Emsisoft (Gen:Variant.Razy.720981 (B)), BitDefender (Gen:Variant.Razy.720981), ESET-NOD32 (A Variant Of MSIL/Hoax.FakeAV.K), Arcabit (Trojan.Razy.DB0055), Full List Of Detections (VirusTotal). |
| Симптомы | Антивирус просит плату за то, чтобы делать базовый функционал |
| Методы распространения | Обман через скачивание «лучшего» антивируса с интернета |
| Ущерб | Ухудшение работоспособности ПК, заражение дополнит. вирусами, трата денег на покупку фейкового антивируса |
| Рекомендации по удалению | Чтобы удалить вирус нужно воспользоваться антивирусом. Рекомендуется пользоваться антивирусом Kaspersky Antivirus |

**Контрольные вопросы**

1. Взять описание работы компьютерных вирусов можно с этих сайтов:

* <http://www.securelist.com/ru/descriptions>
* http://www.kaspersky.ru/rss/technews
* http://www.securitylab.ru/\_Services/Export/RSS/
* http://www.viruslist.com/ru/rss/latestvirusdescriptions
* http://www.viruslist.com/ru/rss/virusalerts
* http://www.viruslist.com/ru/rss/latestnews
* <http://news.drweb.com/list/?c=10>
* http://www.kaspersky.com/viruswatch3

1. Основными путями распространения компьютерных вирусов являются интернет и носители информации
2. Основными формами проявления компьютерных вирусов являются медленная работа ПК, невозможность загрузки ОС, исчезновение файлов и каталогов или искажение их содержимого и прекращение работы ранее успешно функционировавших программ.
3. Наиболее заметными проявлениями компьютерных вирусов для пользователя являются медленная работа ПК, невозможность загрузки ОС, исчезновение файлов и каталогов или искажение их содержимого и прекращение работы ранее успешно функционировавших программ.