Trojan.AndroidOS.Triada.eq

Модуль расшифровывал и запускал на устройстве уже знакомую нам полезную нагрузку Trojan.AndroidOS.Triada.ef.

Расшифровка и запуск полезной нагрузки

Помимо этого, вредоносный модуль крал различные ключи, необходимые для работы легитимного WhatsApp. Мы предполагаем, что для решения этой задачи злоумышленникам перед написанием новой версии пришлось разобраться во всех тонкостях мессенджера.

Интересующие злоумышленников ключи, как правило, используются в утилитах с открытым исходным кодом, которые позволяют пользоваться аккаунтом WhatsApp, не прибегая к загрузке приложения. Утечка этих ключей может привести к тому, что пользователь вредоносной модификации WhatsApp потеряет контроль над своим аккаунтом.

**Как распространяется вредоносный Trojan.AndroidOS.Triada.eq**

Обнаружив новую вредоносную модификацию WhatsApp, мы решили узнать, как она распространяется. Проанализировав статистику, мы пришли к выводу, что одним из основных источников оказалась реклама в популярном приложении Snaptube. Оказалось, что в официальном приложении Snaptube действительно можно встретить рекламу YoWhatsApp, при нажатии на которую пользователь получает предложение установить вредоносную сборку.

Классификация

Категория: Вредоносное ПО

Тип: Рекламный вирус

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.

1. Где можно взять описание работы компьютерных

вирусов (конкретные примеры)?

Ниже приведён примерный перечень таких сайтов, на которых приведено описание вирусных угроз, которое необходимо использовать при выполнении данной лабораторной работы: 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

2. Какие есть пути распространения компьютерных

вирусов?

Дискеты

Флеш-накопители

Электронная почта

Системы обмена мгновенными сообщениями

Веб-страницы

Интернет и локальные сети (черви)

3. Какие есть формы проявления компьютерных вирусов?

1. Вирусы

2. Черви

3. Рекламное ПО

4. Шпионское ПО

5. Программы-вымогатели

6. Боты

7. Руткиты

8. Троянские программы

4. Какие формы проявления компьютерных вирусов

наиболее незаметны для пользователя?

Черви

Шпионское ПО

Троянские программы