

Злоумышленники используют фальшивые приложения Google Play для обмана пользователей

7 октября 2016 года

Многие разработчики вредоносных программ для Android пытаются маскировать их под легитимное и полезное ПО. Таким образом они убеждают пользователей на их загрузку. Для этого злоумышленники могут использовать интересное название приложения и добавить к нему фальшивое описание, которое не соответствует функционалу этого приложения. Специалисты ESET обнаружили восемь таких фальшивых приложений на Google Play, обещавших пользователям увеличить количество подписчиков в их аккаунтах социальных сетей. Наши AV-продукты обнаруживают эти приложения как Android/Fasurke.



Будучи доступными в магазине Google Play более четырех месяцев, приложения собрали от 250К до 1М просмотров. После нашего обращения в Google, Android security team удалила все эти приложения из Play. Несмотря на то, что эти приложения уже не представляют опасности для пользователей Android, нам стоит обнародовать подробности их анализа, так как, в будущем, в Play могут появиться аналогичные приложения.



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

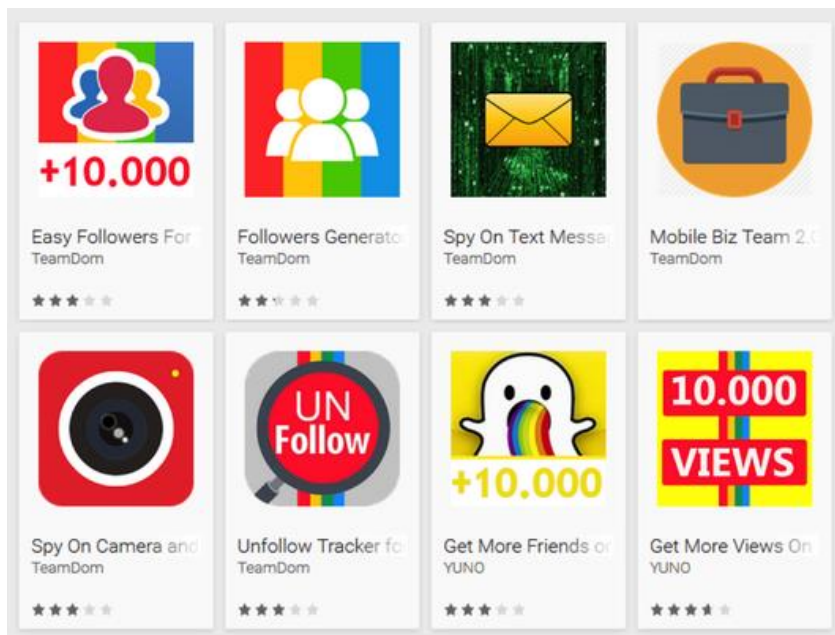


Рис. 1. Значки фальшивых приложений, которые размещались в Google Play

Эти восемь приложений обещали пользователям больше подписчиков, друзей или большее число просмотров их публикаций в социальных сетях. Однако, настоящая их цель совершенно иная и заключается в заманивании пользователей на приобретение платных подписок, распространении их персональных данных, получение согласия от пользователя на показ рекламных объявлений.

Easy Followers For Instagram

+FOLLOWERS

1. Select Your Device

- ☐ Samsung
- ☐ HTC
- ☐ Nokia
- ☐ Others

3. Select The Amount Of Followers To Generate

- ☐ 10.000
- ☐ 50.000
- ☐ 100.000
- ☐ 500.000

Next

Start Generating

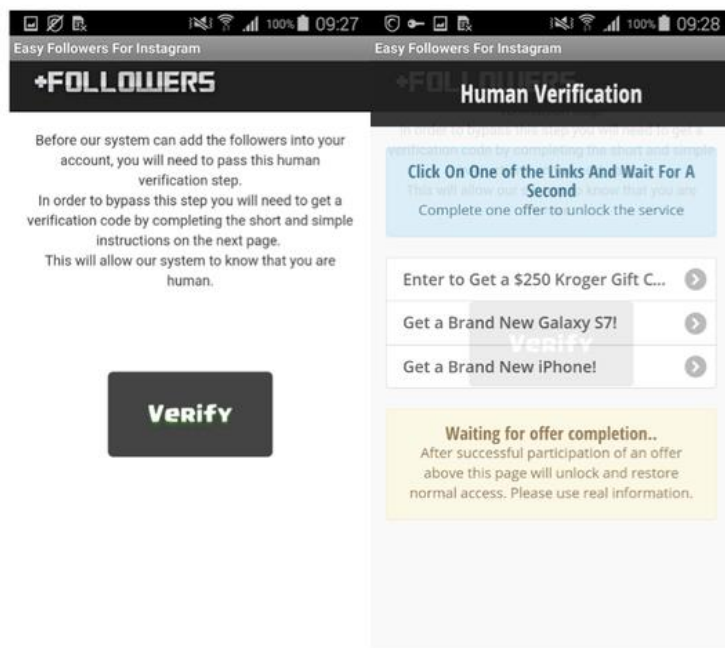


Рис. 2. Пример фальшивого приложения

Указанная выше на картинке «проверка» была всего лишь прикрытием для того, чтобы начать предлагать пользователю бесконечное количество подарков, купонов и бесплатных услуг. Кроме этого, приложение также специализируется на сборе персональных данных пользователя, запрашивая у него такую личную информацию как имя, адрес электронной почты, адрес, телефон, дату рождения и пол. Пользователям предлагали подписаться на специальные платные SMS-рассылки стоимостью около 4,8 евро в неделю.

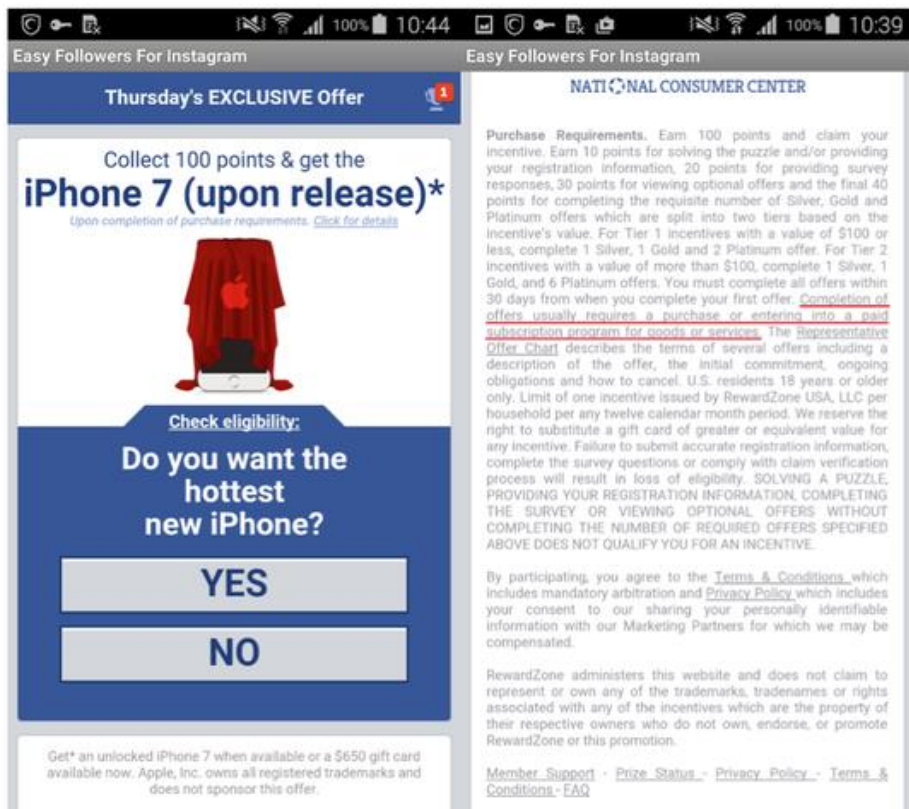


Рис. 3. Одно из приложений предлагает пользователям платную подписку.



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Easy Followers For Instagram

IPHONE 7 (UPON RELEASE) Total Points: 10 of 100

Take survey (20 pts)

CONFIRM YOUR INFORMATION
to finish your registration

FIRST NAME
[Redacted]

LAST NAME
[Redacted]

ZIP CODE
[Redacted]

PRIMARY PHONE
[Redacted]

EMAIL
[Redacted]

DATE OF BIRTH
[Redacted]
(You must be 18 years or older)

By checking the box below I consent to receive phone sales calls and text messages - Msg and data rates may apply - from Verde Energy and our Marketing Partners on the landline or mobile number I provided even if I am on a federal or State do not call registry. I understand these calls may be generated using an autodialer and may contain pre-recorded messages and that consenting is not required to participate in the offers promoted.

☒ I CONFIRM that all of my information is accurate and consent to be called and texted as provided above.

CONTINUE

NATIONAL CONSUMER CENTER

Рис. 4. Приложение заманивает пользователя на подписку телефонных вызовов и сообщений с рекламой.

На самом деле, этот «проверочный шаг» представляет собой бесконечный процесс отображения рекламы и других объявлений для получения от пользователя как можно больше денег.



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

REVIEWS



Helpfulness ▾ All Devices ▾ All Versions ▾

User reviews

Sheena Petrovic April 29, 2016
★ ★ ★ ★ ★
SCAM! FAKE! You have to do one of those ENDLESS surveys like 'enter to win a free apple watch'

Patience A March 29, 2016
★ ★ ★ ★ ★
Good but Why do u have to get a gift card and does this even work i rate this as a 3

Miyetta White April 19, 2016
★ ★ ★ ★ ★
Stupid did not get my followers Dumb stupid hate it 😡😡😡😡😡

torry chandler April 21, 2016
★ ★ ★ ★ ★
Doesn't work You have to buy a gift card and etc. Once it's done you have to do it all over again and it still doesn't work...

Kylie Arnold May 23, 2016
★ ★ ★ ★ ★
F### THIS I should not have to buy an iPhone 7 to get 500,000 followers. Srsly?? Checkinng if I'm human huh?? Wtf nope. Bad app.

kayla's videos April 20, 2016
★ ★ ★ ★ ★
Really This sucks it doesn't even work you have to get a whole bunch of gift cards and offers 😡😡😡😡😡

PlatinumVlogs May 5, 2016
★ ★ ★ ★ ★
IG is 55.unlty App does not work but who ever follows me I will follow back

Kate Raeder May 30, 2016
★ ★ ★ ★ ★
It basically asked me to spend money on a gift card then to put my personal info in a survey. This is a waste of time and space on your phone. HIGHLY DONT RECOMMEND!

ADDITIONAL INFORMATION

Updated	Size	Installs
March 18, 2016	18k	100,000 - 500,000
Current Version	Requires Android	Content Rating
1.0	2.3.3 and up	PEGI 3 Learn more
Permissions	Report	Offered By
View details	Flag as inappropriate	TeamDom
Developer		
Email issam@myself.com		

G+1 2.7k

Рис. 5. Оценки и отзывы об одном из фальшивых приложений.

Все эти приложения имеют большой процент низких рейтингов и крайне негативных комментариев. Несмотря на это, статистика их установки показывает сотни тысяч установок.

Заключение

Упомянутые выше приложения, которые были обнаружены нашими специалистами в Google Play, не выполняют заявленных авторами функций, т. е. не увеличивают количество последователей аккаунта пользователя в социальных сетях. Вместо этого, они специализируются на отображении пользователю бесконечного числа рекламных предложений, которые стараются заставить пользователя подписаться на рассылку платных SMS, а также получить от него персональные данные.

Следующие рекомендации помогут вам избежать установки вредоносных приложений Android:



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

- Загружайте приложения только из магазина Google Play или другого доверенного магазина. Такие хранилища приложений не являются абсолютно безопасными, но шанс установить оттуда вредоносное ПО намного меньше.
- Перед установкой любого приложения, проверяйте его рейтинг и читайте отзывы пользователей. Обращайте внимание на негативные отзывы, так как они оставляются проверенными пользователями, при этом положительные отзывы могут быть оставлены злоумышленниками.
- Сталкиваясь с каким-либо неправдоподобным предложением, держите в памяти золотое правило, что «это слишком хорошо, чтобы быть правдой». Если авторы предлагают полмиллиона подписчиков для вашего аккаунта бесплатно или с помощью всего одного клика, скорее всего, это обман.
- Подумайте дважды при вводе своей личной информации или при заказе какой-либо услуги. Будьте точно уверены в том, что вы получите желаемый функционал взамен.
- Используйте антивирусный продукт для своего устройства.