Заразить смартфон вирусом не так легко, как в случае с компьютером — приложения в Google Play проходят проверку, а создатели смартфонов регулярно выпускают новые версии прошивок с антивирусными заплатками. Но вирусописатели регулярно «пробивают» такую защиту, а пользователи спешат установить на смартфон игры и приложения в обход официальных магазинов. Мы расскажем, какие зловреды способны поразить даже самые новые версии Android, и чем они опасны.

Triada

Начнём со «свежака» — Триаду сегодня можно считать самым новым и «пуленепробиваемым» вирусом для смартфонов. Его и обнаружили-то только в марте 2017 года.

Уникален он своей близостью к классическим вирусам, а не троянам-вымогателям, как это обычно бывает на Android. Вам всё же нужно умудриться подхватить его из «непроверенных источников», а вот дальше начинается гораздо весёлый «боевичок»:

*Triada — вирус, который не просто хулиганит в системе,
а вклинивается в её жизненно важные участки*

Triada включается после того, как вы установите и дадите разрешения вашей любимой качалке музыки из ВКонтакте, например. После программа втихаря выясняет модель вашего смартфона, версию прошивки и Android, объём свободного места на накопителях и список установленных приложений. И отправляет эту информацию в интернет, на свои серверы. Этих серверов огромное количество, они разбросаны в различных странах, то есть, даже приехать и устроить «маски-шоу» по местоположению сервера со зловредом не получится.

В ответ Triada получает инструкции (прямо-таки, индивидуальный подход к пациенту!), как лучше спрятать себя конкретно в этой разновидности Android и этом смартфоне, внедряется в каждое (!) из установленных приложений и берёт контроль над системными компонентами, чтобы скрыть себя в списке установленных приложений и запущенных процессов. После этого отдельно стоящая в системе часть вируса «заметает» за собой следы — он больше не работает как отдельное приложение, а согласовывает свои действия с помощью кусочков заражённой системы.

Готово, система завоёвана! С этого момента смартфон превращается в «марионетку», которой злоумышленники отдают команды на расстоянии и принимают информацию на любой из доступных серверов. Сейчас Triada действует примитивно — выясняет данные вашей банковской карты, снимает с неё деньги, достаёт из входящих SMS нужные для оплаты коды, «рисует» ложные цифры о балансе владельцу.

Но с возможностью «распотрошить» любое установленное приложение или установить новое на расстоянии это только «цветочки» — особенность «Триады» заключается в том, что это модульный вирус, к нему можно будет прикрутить самые разные виды дистанционных трюков.

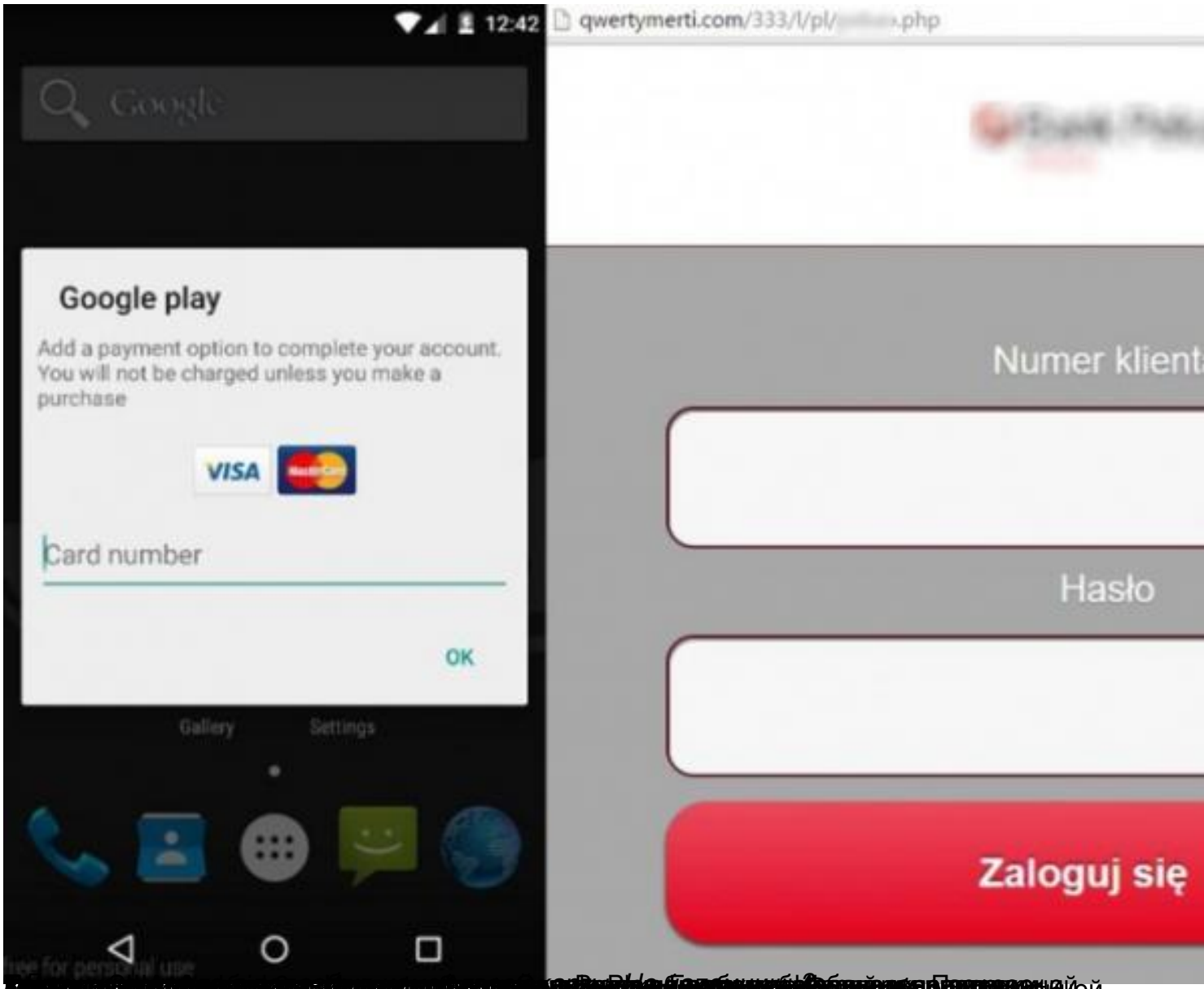
Как видите, вирусы для Android — это не только примитивные «ваш телефон заблокирован, с вас сто баксов», от которых можно избавиться удалением приложения. И, если в новых версиях Android хотя бы усложнён доступ к получению root и можно увидеть что-то подозрительное на этапе запроса прав приложением, то старые версии (Android 4.4, 4.3 и старее) абсолютно беззащитны перед новой заразой — спасёт только полная перепрошивка.

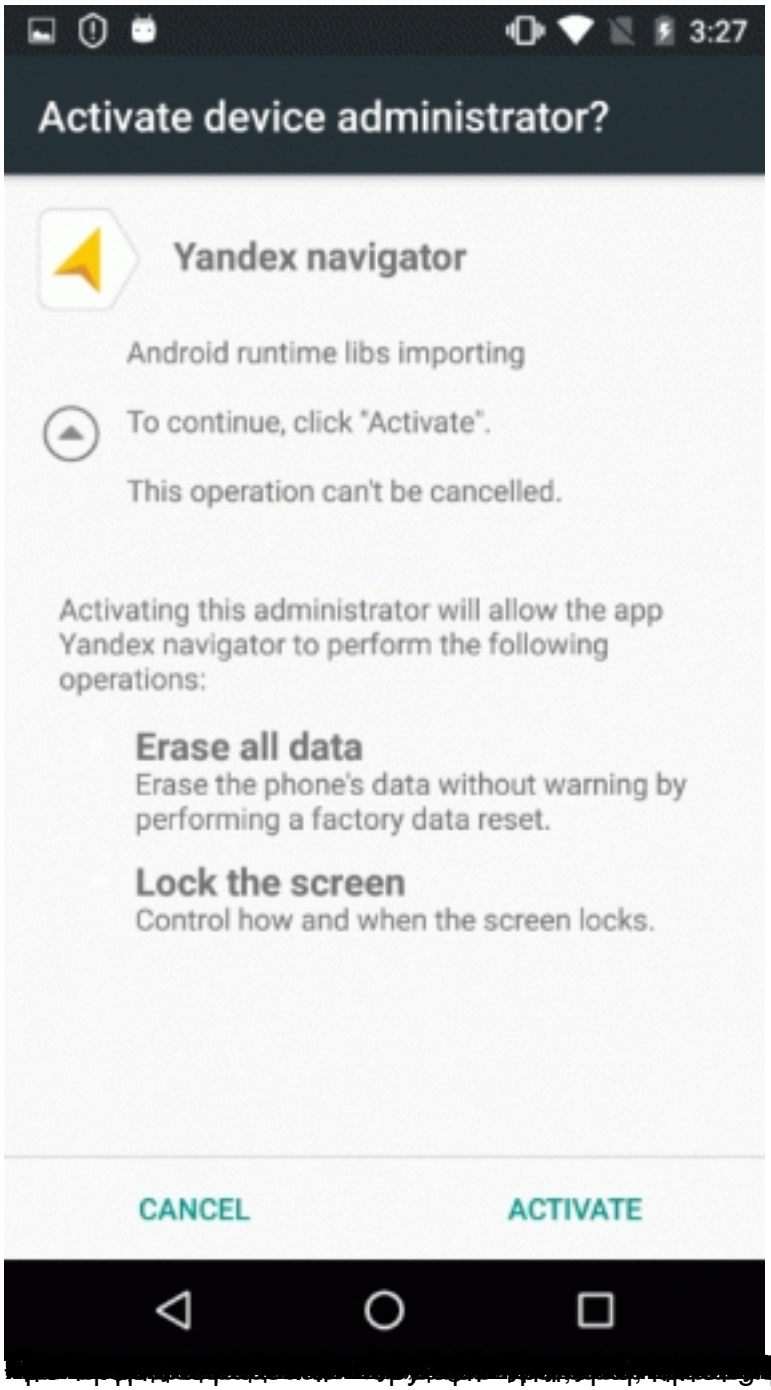
Marcher

Так называемый «банковский зловред» был разработан ещё в 2013 году, но его «звёздный час» настал только летом 2016 года. Знаменит хорошей маскировкой и «интернационализмом», если можно так сказать.

Marcher представляет собой простой троян, который не проворачивает ничего сверхъестественного, а просто подменяет собой служебные страницы огромного количества банков с помощью всплывающих окон. Механизм следующий:

Троян проникает в систему вместе с заражённым приложением. Пик популярности Marcher пришёлся на «свежеукраденные» у Nintendo версии Super Mario Run. Если вы не помните, это такая супер-раскрученная «бегалка» от создателей Pokemon GO!
Ищет на смартфоне банковские приложения и приложения интернет-магазинов выбирает «заготовки» в соответствии с тем, каким банком вы пользуетесь.
Отправляет на смартфон «приманку» — сообщение в шторке уведомлений со значком банка/магазина и сообщением в стиле «на ваш счёт поступило N рублей»/«купон на скидку 75% для любого товара только сегодня!».
Владелец смартфона кликает на уведомление. После чего троян открывает точнейшую копию, страницу, 1-в-1 похожую на ту, что вы привыкли видеть в официальном приложении. И говорит что-то в стиле «соединение с сетью прервано, повторите ввод данных банковской карты».
Владелец смартфона вводит данные банковской карты. Тут-то денюжки тю-тю!


12:42
Google
Google play
Add a payment option to complete your account. You will not be charged unless you make a purchase
VISA
Card number
OK
Gallery
Settings
qwertymerti.com/333/l/pl/
.php
Numer klient
Hasło
Zaloguj się


3:27
Activate device administrator?
Yandex navigator
Android runtime libs importing
To continue, click "Activate".
This operation can't be cancelled.
Activating this administrator will allow the app Yandex navigator to perform the following operations:
Erase all data
Erase the phone's data without warning by performing a factory data reset.
Lock the screen
Control how and when the screen locks.
CANCEL
ACTIVATE

Summer Flashligh

Crazy WiFi Team Tools

E Everyone

This app is compatible with all of your

India	46.19%
Indonesia	10.27%
Thailand	9.47%
Philippines	6.31%
Malaysia	5.01%
Vietnam	2.12%
Japan	1.87%
Russia	1.85%
United States	1.51%
Iran	0.90%
Others	14.50%