Троянское приложение для Android обходит проверки Google Bouncer

Аналитики ESET обнаружили интересный метод скрытной атаки на пользователей Android, который содержит в себе интересную особенность. В магазине приложений Google Play нам удалось обнаружить несколько приложений, которые маскировались под легитимные, но на самом деле содержали в себе другое приложение с вредоносными функциями. Это встроенное приложение называлось systemdata или resourcea.

Это второе приложение скрытно сбрасывается в память устройства из первого, но спрашивает у пользователя разрешение на установку. Оно представляется в качестве инструмента для управления настройками устройства «Manage Settings». После своей установки, приложение работает как служба в фоновом режиме.

Антивирусные продукты ESET обнаруживают приложения, которые содержат в себе это дополнительное приложение как **Android/TrojanDropper.Mapin**. Согласно нашим данным, на долю Индии приходится наибольшее количество заражений устройств Android этим вредоносным ПО.

Вредоносная программа представляет из себя бэкдор, который получает контроль над устройством и включает его в состав ботнета. Бэкдор использует специальный внутренний таймер для отложенного исполнения своей полезной нагрузки. Таким образом, авторы могут обмануть различные автоматические системы анализа файлов, которые могут причислить файл к подозрительным из-за его поведения. В некоторых случаях, бэкдор может ждать три дня прежде чем активировать полезную нагрузку. Скорее всего, такая мера позволяет авторам обойти механизмы проверки инструмента анализа файлов Google Bouncer, используемый Google для проверки загружаемых в Play приложений.

После активации полезной нагрузки, троян запрашивает права администратора в системе и начинает взаимодействовать со своим C&C-сервером. Android/Mapin содержит в себе различные функции, например, отображение пользователю различных уведомлений, загрузка, установка и запуск других приложений, а также получение личной информации пользователя на устройстве. В то же время, основной его функцией является отображение fullscreen-рекламы на зараженном устройстве.

Векторы распространения

Вредоносные приложения были размещены в магазине приложений Google Play в конце 2013 г. и в 2014 г. Названия приложений были различными, включая, «Hill climb racing the game», «Plants vs zombies 2», «Subway suffers», «Traffic Racer», «Temple Run 2 Zombies», «Super Hero Adventure» разработчиков TopGame24h, TopGameHit и SHSH. Точные даты загрузки приложений были 24-30 ноября 2013 г. и 22 ноября 2014 г. Согласно статистике ресурса MIXRANK, приложение Plants vs zombies 2 было загружено более 10 тыс. раз перед его удалением из магазина. В то же самое время, приложения «System optimizer», «Zombie Tsunami», «tom cat talk», «Super Hero adventure», «Classic brick game», а также вышеупомянутые приложения Google Play с вредоносными возможностями, были загружены в альтернативные магазины приложений Android теми же авторами. Такой же бэкдор был обнаружен в комплекте с другими приложениями, которые были загружены в магазин разработчиком PRStudio (не путать с prStudio) в альтернативные магазины приложений со ссылками на Google Play. Данный разработчик загрузил как минимум и пять других троянских приложений в альтернативные магазины приложений: «Candy crush» или «Jewel crush», «Racing rivals», «Super maria journey», «Zombie highway killer», «Plants vs Zombies». Эти приложения все еще доступны для скачивания из этих магазинов. Перечисленные приложения были загружены пользователями сотни раз.

Рис. Значки вредоносных приложений.

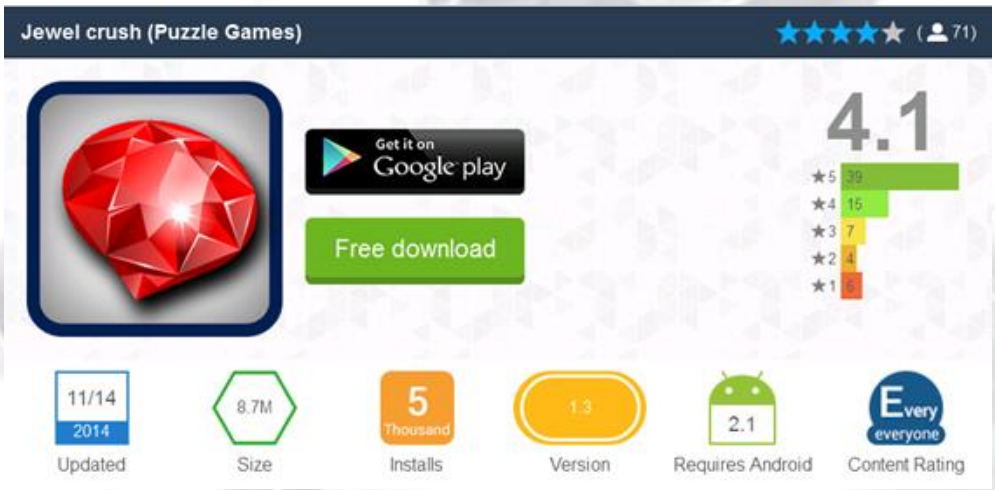

Рис. Вредоносное приложение, которое получило достаточно положительных оценок.

Рис. Еще одно приложение, получившее положительные оценки.

Анализ

Существуют различные варианты исполнения вредоносной программы после того, как пользователь загрузил нелегитимное приложение. Один из вариантов предполагает, что жертве будет предложено запустить файл с вредоносной программой спустя 24 после первого исполнения загруженного приложения. Такой метод является менее подозрительным для пользователя, который считает, что запрос на запуск поступил от ОС. Другой метод подразумевает под собой выдачу мгновенного запроса пользователю. Оба варианта рассчитаны на срабатывание после изменения подключения к сети, для этого вредоносная программа регистрирует т. н. broadcast receiver в манифесте.

```
<receiver android:name="com.systemservice.sdk.NetworkStateReceiver">
    <intent-filter>
        <action android:name="android.net.conn.CONNECTIVITY_CHANGE" />
    </intent-filter>
</receiver>
```

Рис. Регистрация т. н. broadcast receiver.

После изменения подключения, пользователю будет предложено установить «системное приложение». Само сброшенное на устройство вредоносное приложение может называться «Google Play Update» или «Manage Settings».

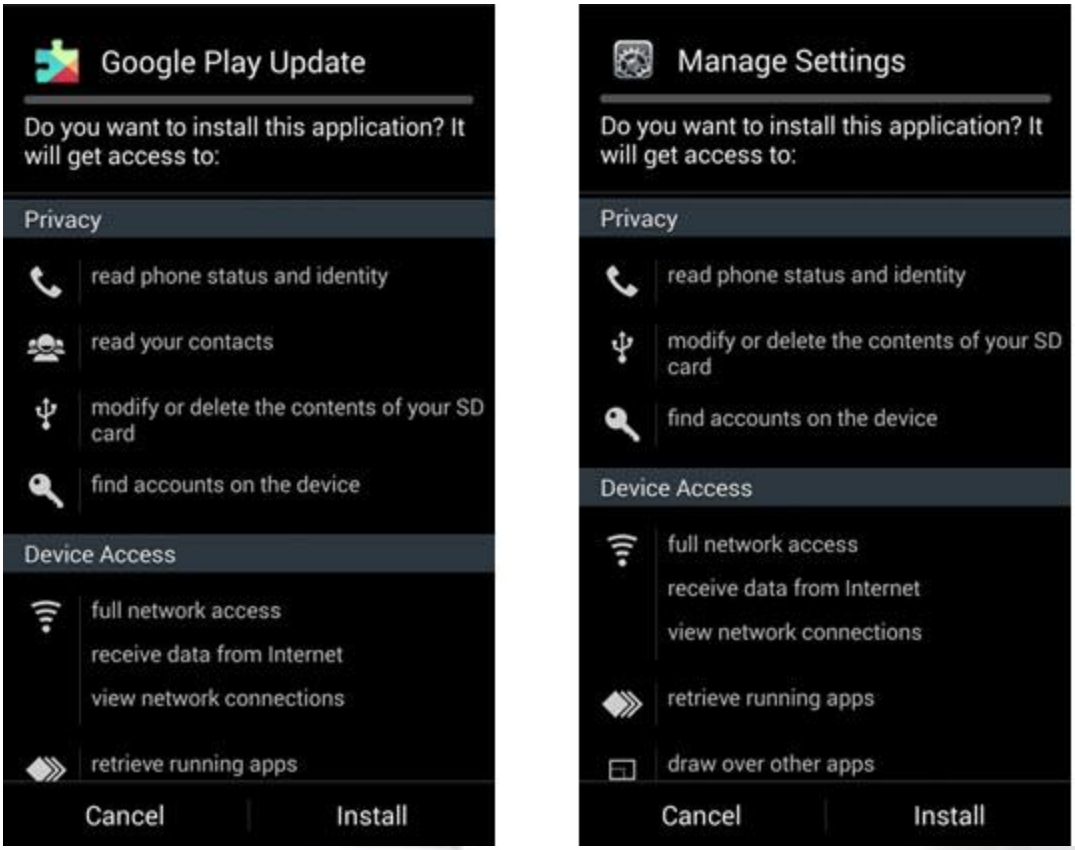

Рис. Вредоносное приложение маскируется под системное.

В том случае, если пользователь выбирает отмену установки, то вредоносная программа будет показывать запрос каждый раз при смене сетевого подключения. Можно предположить, что простой пользователь будет уверен в серьезности отображаемого уведомления и в какой-то момент, скорее всего, нажмет кнопку установки только чтобы избавиться от него. После запуска троян исполняется в качестве сервиса со своим зарегистрированным broadcast receiver, ожидая изменения подключения.

Когда такое изменение произойдет, троян попытается зарегистрировать себя с помощью сервиса Google Cloud Messages (GCM) для последующего получения сообщений. После этого, Android/Mapin попытается зарегистрировать зараженное устройство на сервере злоумышленников, отправляя туда такую информацию как имя пользователя, аккаунт Google, IMEI, регистрационный идентификатор (ID) и название своего пакета приложения.

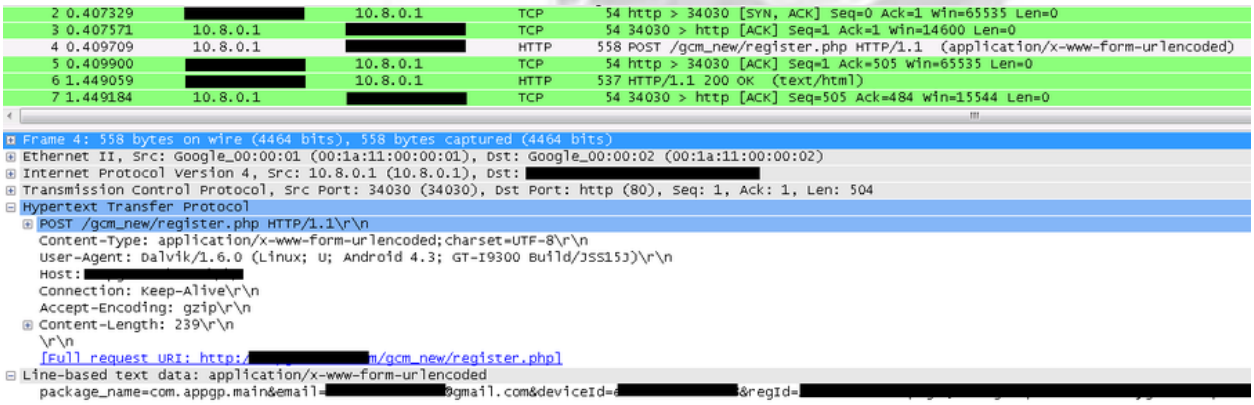

Рис. Процесс регистрации устройства на сервере злоумышленников.

Для того, чтобы исключить возможность своего удаления из системы, троян требует от пользователя активировать режим администратора устройства.

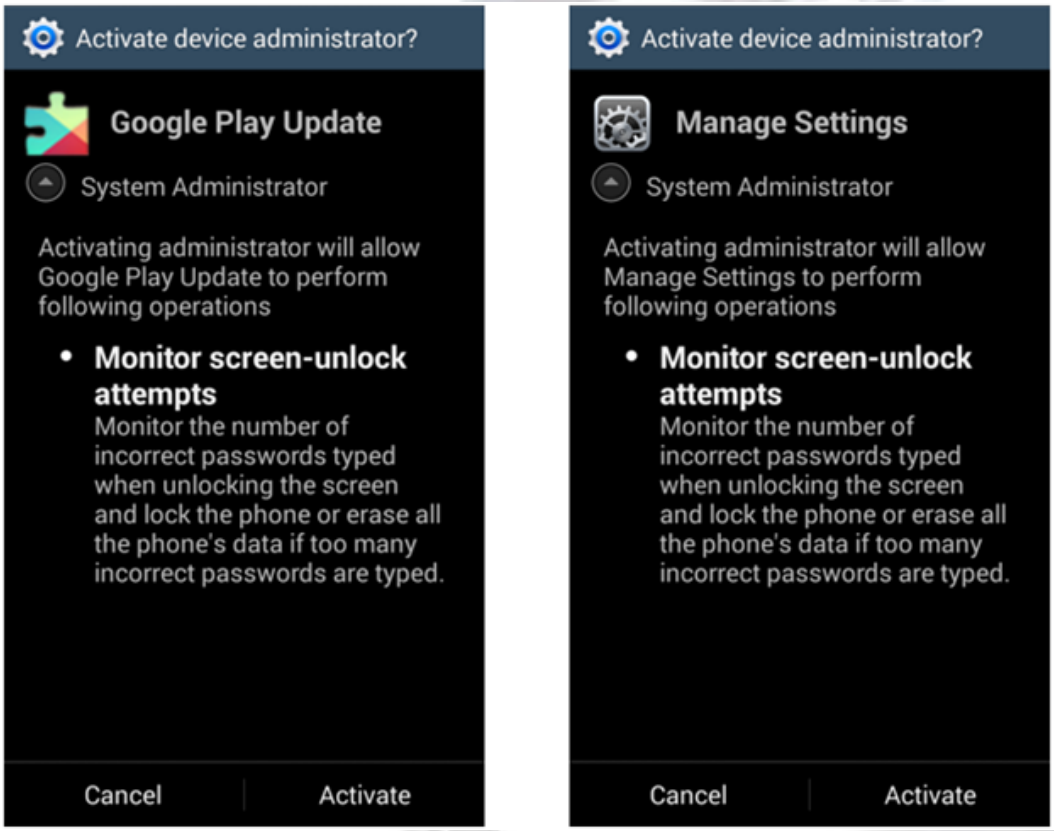

Рис. Предложение пользователю об активации режима администратора устройства.

Троян сообщит на удаленный сервер об успешности активации режима администратора устройства. Как только такая операция произойдет, вредоносная программа будет показывать пользователю рекламу в полноэкранном режиме (interstitial). Такая реклама (interstitial ad) будет отображаться пользователю заново каждый раз при смене подключения. Разработка такого типа рекламы возможна с использованием легитимного AdMob SDK.

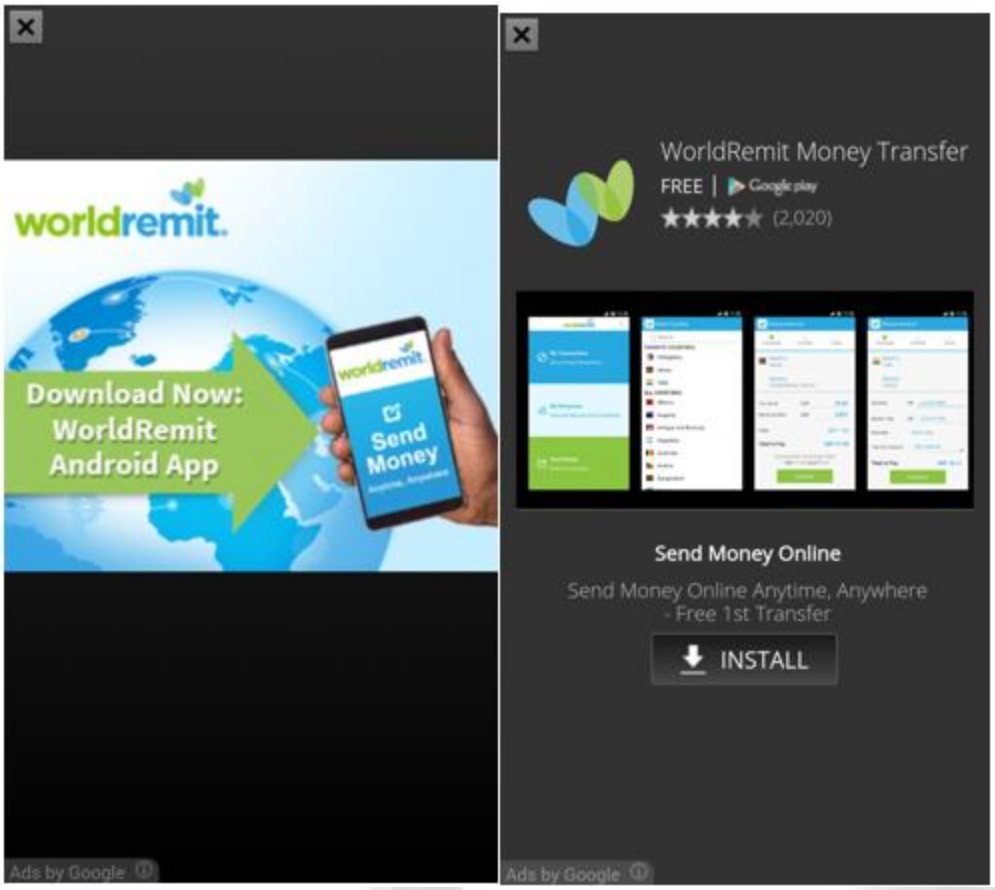

Рис. Full-screen реклама (interstitial ad).

Сетевое взаимодействие

Троян взаимодействует со своим управляющим сервером используя сервис Google Cloud Messaging (GCM). Этот сервис все чаще используется современными вредоносными программами для своих целей, через него злоумышленники могут инструктировать бот на выполнение нужных им действий.

```
if(v4.contains("i_a")) {
    CmdHandler.handleInstallApkFromTxtAsset(context, v4);
    v0 = 1;
}
else if(v4.contains("c_sa")) {
    v0 = 2;
    CmdHandler.handleChangeServerAddress(context, v4);
}
else if(v4.contains("l_a")) {
    v0 = 3;
    CmdHandler.handleLaucheAppNoLaucher(context, v4, true);
}
else if(v4.contains("l_a_l")) {
    v0 = 4;
    CmdHandler.handleLaucheAppWithLauncher(context, v4, true);
}
else if(v4.contains("g_n_gp")) {
    v0 = 5;
    CmdHandler.handleGenarateNotificationToLaucheGooglePlay(context, v4);
}
else if(v4.contains("c_ad")) {
    v0 = 6;
    CmdHandler.handleChangeAdmobId(context, v4);
}
else if(v4.contains("d_ts")) {
    v0 = 7;
    CmdHandler.handleDownloadTxtSilently(context, v4);
}
else if(v4.contains("a_aa")) {
    v0 = 8;
    CmdHandler.handleActiveAdminApp(context, v4);
}
else if(v4.contains("c_acr")) {
    v0 = 9;
    CmdHandler.handleConfigAdsClickRequirement(context, v4);
}
else if(v4.contains("c_md")) {
    v0 = 10;
    CmdHandler.handleChangeAdsShowConfig(context, v4);
}
else if(v4.contains("s_gpi")) {
    v0 = 11;
    CmdHandler.handleSetupGooglePlayLaunchIcon(context, v4);
}
else if(v4.contains("s_mads")) {
    v0 = 12;
    CmdHandler.handleSetupMyAds(context, v4);
}
```

Рис. Обрабатываемые ботом команды.

Не все функции вредоносной программы полностью реализованы в ее коде, кроме этого, не все уже реализованные функции используются. Возможно, что сама угроза все еще находится на уровне разработки и будет улучшена в будущем. Как мы уже упоминали, ее основная цель заключается в доставке агрессивной full-screen рекламы для ее отображения пользователю, маскируясь под системное приложение. Бот также может быть использован злоумышленниками для установки другого вредоносного ПО на скомпрометированное устройство.

Кроме показа рекламы, список выполняемых им вспомогательных функций достаточно обширен: изменение идентификатора publisher ID отображаемой рекламы, загрузка и запуск других приложений, отображение уведомлений пользователю, отключение режима администратора устройства, изменение адреса управляющего C&C-сервера, создание на домашнем экране Android ярлыков, которые ведут на URL-адреса загрузки приложений. После исполнения каждой задачи, полученной с помощью GCM, бот будет информировать об этом удаленный сервер с использованием протокола HTTPS.

Заключение

Троянская программа была успешно загружена в магазин Google Play, поскольку содержала в себе механизм отложенной активации вредоносных функций и, таким образом, не вызвала к себе подозрений со стороны инструмента Bouncer. Интересным вопросом является и то, почему Bouncer не специализируется на статическом анализе исполняемых файлов внутри загруженных приложений. По этим причинам троянская программа свободно распространялась пользователям через официальный магазин приложений Google для Android. Вредоносная игра «Super Hero adventure» была загружена в Play Store разработчиком SHSH. Вполне возможно, что этот разработчик загрузил больше приложений в магазин Play. В конечном счете, все они были удалены из магазина, но оставались незамеченными там в течение полутора лет. Возможно, что подобные случаи стали причиной того, что в марте 2015 г. Google объявила о том, что все приложения и обновления должны проходить проверку со стороны человека.

Лучшей практикой для поддержания своего устройства в безопасности является использование только официального магазина приложений для их загрузки. Кроме этого, необходимо уделять внимание отзывам и комментариям пользователей к размещаемым там приложениям. При установке приложения следует внимательно следить за запрашиваемыми приложением правами. Если вы заметили что-либо подозрительное в поведении приложения, его можно отправить в качестве образца в антивирусную лабораторию с соответствующими комментариями о причинах отправки.

Ниже представлена информация о проанализированных нами образцах вредоносной программы.

Название приложения	Название пакета	MD5	Обнаружение ESET
Highway Zombie	com.heighwayzombie	2f6323af124f9fd57edb1482827f9481	Android/TrojanDropper.Mapin
Plant vs Zombie	com.plantzombie	8721901a2caaeb98a19e0fb909ce2569	Android/TrojanDropper.Mapin
USubway Suffer	com.subwaysuffers	ba3c1894310d38aa814ad3c58f1c8469	Android/TrojanDropper.Mapin
Climb racing	com.hillclimbrace	87cc79d6f6795fea0df109e181d1a3e8	Android/TrojanDropper.Mapin
Temple run 2 Zoombie	com.templerunzombies	d5afd7ba5b3bd24cd4fa5201882e1a9d	Android/TrojanDropper.Mapin
Traffic Racer	com.traficracer	9cbfd66f35a36d9f75a89f342da9c784	Android/TrojanDropper.Mapin
Google Play update	com.system.main	f8df9e2d21018badc7555a9233a8b53e	Android/Mapin
Arrange Block - Brick game	com.game.arrangeblock	d7facf652d3947a53f85431ba8a4cd4a	Android/TrojanDropper.Mapin
Manage Settings	com.appgp.main	5586e93ac84317348904adfe01c9715c	Android/Mapin
Candy crush	com.tgame.candycrush	745e9a47febb444c42fb0561c3cea794	Android/TrojanDropper.Mapin
Manage Settings	com.appgp.main	c19896fdd3b96b9324c6b79cc39eca5b	Android/Mapin

Название приложения	Название пакета	MD5	Обнаружение ESET
Super maria adventure	com.game.supermario	0d7c889e8a9be51a58041d55095f104f	Android/TrojanDropper.Mapin
Manage Settings	com.appgp.main	c19896fdd3b96b9324c6b79cc39eca5b	Android/Mapin
Super maria journey	com.tgame.maria	ee8e4e3801c0101998b7dfee33f35f95	Android/TrojanDropper.Mapin
Google Play Update	com.appgp.main	195432955e70ec72018ead058f7abc2d	Android/Mapin
Zombies highway killer	com.absgame.zombiehighway killer	1516174c4a7f781c5f3ea6ac8447867b	Android/TrojanDropper.Mapin
Manage Settings	com.appgp.main	f05ac3ac794ee8456db4d0331830d2d8	Android/Mapin
Plants Vs Zombies	com.tgame.plantvszombie	10edaf2b4c25375644faf78a25790061	Android/TrojanDropper.Mapin
Google Play Update	com.appgp.main	f8879f759b00ed9d406dd14ce450584b	Android/Mapin
Plants Vs Zombies	com.popcap.pvz_row	9b72df484915ce589ade74e65ecdfaed	Android/TrojanDropper.Mapin