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

Выполнил: Первых Никита Николаевич

# **Android.Spy.4498**

Троян, работающий на устройствах под управлением ОС Android. Его основная функция — кража содержимого уведомлений от других приложений. Кроме того, он загружает и предлагает пользователям установить другие программы, а также может демонстрировать различные диалоговые окна.

Известные версии Android.Spy.4498 встроены в некоторые неофициальные модификации (моды) мессенджера WhatsApp, такие как GBWhatsApp, OBWhatsApp, WhatsApp Plus и другие, которые злоумышленники распространяют через вредоносные сайты.

**Принцип действия**

В процессе работы Android.Spy.4498 запрашивает доступ к управлению уведомлениями и чтению их содержимого. Рассматриваемая версия трояна нацелена на уведомления от следующих приложений:

com.sec.android.app.samsungapps — Samsung Galaxy Store (Galaxy Apps);

com.android.vending — Google Play Store.

Дополнительно троян способен вести удаленное логирование содержимого уведомлений от приложений из заданного списка с использованием различных сервисов статистики — например, Flurry (используемый сервис зависит от модификации вредоносного приложения). Однако в известных версиях Android.Spy.4498 такой список отсутствует.

Помимо этого, во время использования приложения троян скрытно скачивает apk-файл по полученной от злоумышленников ссылке, а затем предлагает установить его под видом новой версии приложения, для чего демонстрирует соответствующее диалоговое окно. При этом во время своего запуска Android.Spy.4498 демонстрирует другой диалог обновления, в котором отображается прогресс загрузки apk-файла.

Кроме того, троян может демонстрировать произвольные диалоговые окна, содержимое которых он также получает от злоумышленников. Когда пользователь нажимает на кнопку «Ок» такого диалога, в браузере происходит загрузка целевого сайта.

Демонстрация запроса доступа к уведомлениям и диалоговых окон с настраиваемым содержимым, а также загрузка apk-файла выполняются из модифицированной активности com.whatsapp.HomeActivity оригинального приложения WhatsApp.

**Рекомендации по лечению**

**Android**

Если мобильное устройство функционирует в штатном режиме, загрузите и установите на него бесплатный антивирусный продукт Dr.Web для Android Light. Выполните полную проверку системы и используйте рекомендации по нейтрализации обнаруженных угроз.

Если мобильное устройство заблокировано троянцем-вымогателем семейства Android.Locker (на экране отображается обвинение в нарушении закона, требование выплаты определенной денежной суммы или иное сообщение, мешающее нормальной работе с устройством), выполните следующие действия:

загрузите свой смартфон или планшет в безопасном режиме (в зависимости от версии операционной системы и особенностей конкретного мобильного устройства эта процедура может быть выполнена различными способами; обратитесь за уточнением к инструкции, поставляемой вместе с приобретенным аппаратом, или напрямую к его производителю);

после активации безопасного режима установите на зараженное устройство бесплатный антивирусный продукт Dr.Web для Android Light и произведите полную проверку системы, выполнив рекомендации по нейтрализации обнаруженных угроз;

выключите устройство и включите его в обычном режиме.

**Android.DownLoader.1049.origin**

**Описание**

Вредоносный модуль, который злоумышленники внедряют в Android-программы. Например, он был обнаружен в системном приложении для беспроводного обновления прошивки смарт-часов Elari Kidphone 4G. Троян используется для сбора и отправки на удаленный сервер большого объема информации об Android-устройствах и их пользователях. Кроме того, по команде сервера он способен загружать различные файлы.

**Принцип действия**

Модуль представляет собой файл libcore.jar, который в зашифрованном виде хранится в программном пакете основного приложения. При первом включении устройства встроенный в эту программу вредоносный код (Android.DownLoader.3894) расшифровывает и запускает его. При последующих включениях устройства и при изменении сетевого подключения модуль запускается автоматически.

После запуска Android.DownLoader.1049.origin с определенной периодичностью подключается к C&C-серверу, расположенному по адресу hxxps://g[.]sinfoon[.]com:40081/pull. По умолчанию интервал подключений составляет 8 часов, но может быть изменен соответствующей командой сервера.

**Рекомендации по лечению**

**Android**

Если мобильное устройство функционирует в штатном режиме, загрузите и установите на него бесплатный антивирусный продукт Dr.Web для Android Light. Выполните полную проверку системы и используйте рекомендации по нейтрализации обнаруженных угроз.

Если мобильное устройство заблокировано троянцем-вымогателем семейства Android.Locker (на экране отображается обвинение в нарушении закона, требование выплаты определенной денежной суммы или иное сообщение, мешающее нормальной работе с устройством), выполните следующие действия:

загрузите свой смартфон или планшет в безопасном режиме (в зависимости от версии операционной системы и особенностей конкретного мобильного устройства эта процедура может быть выполнена различными способами; обратитесь за уточнением к инструкции, поставляемой вместе с приобретенным аппаратом, или напрямую к его производителю);

после активации безопасного режима установите на зараженное устройство бесплатный антивирусный продукт Dr.Web для Android Light и произведите полную проверку системы, выполнив рекомендации по нейтрализации обнаруженных угроз;

выключите устройство и включите его в обычном режиме.

# **Android.FakeApp.110**

Троянская программа, работающая на устройствах под управлением ОС Android. Впервые была выявлена в каталоге Google Play, где распространялась под именем «Опрос».

При запуске **Android.FakeApp.110** открывает в WebView адрес http://neopros18.we\*\*\*\*\*/Elena, с которого происходит перенаправление на один из мошеннических веб-сайтов, где пользователю за вознаграждение предлагается ответить на несколько вопросов.

После ответа на все вопросы жертве сообщается, что для получения якобы заработанных денег она должна совершить некий платеж в размере от 100 до 200 рублей. Однако это — уловка злоумышленников, поскольку никакого вознаграждения после перевода указанной суммы владелец мобильного устройства на самом деле не получит.

**Рекомендации по лечению**

**Android**

Если мобильное устройство функционирует в штатном режиме, загрузите и установите на него бесплатный антивирусный продукт Dr.Web для Android Light. Выполните полную проверку системы и используйте рекомендации по нейтрализации обнаруженных угроз.

Если мобильное устройство заблокировано троянцем-вымогателем семейства Android.Locker (на экране отображается обвинение в нарушении закона, требование выплаты определенной денежной суммы или иное сообщение, мешающее нормальной работе с устройством), выполните следующие действия:

загрузите свой смартфон или планшет в безопасном режиме (в зависимости от версии операционной системы и особенностей конкретного мобильного устройства эта процедура может быть выполнена различными способами; обратитесь за уточнением к инструкции, поставляемой вместе с приобретенным аппаратом, или напрямую к его производителю);

после активации безопасного режима установите на зараженное устройство бесплатный антивирусный продукт Dr.Web для Android Light и произведите полную проверку системы, выполнив рекомендации по нейтрализации обнаруженных угроз;

выключите устройство и включите его в обычном режиме.

**Контрольные вопросы**

1. Где можно взять описание работы компьютерных

вирусов (конкретные примеры)? 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 ?

Письма со спамом

Вредоносные Office макрос

Зараженные съемные носители

Вместе с другим программным обеспечением

Взломанные или скомпрометированные веб-страницы

Другие вредоносные программы

3. Какие есть формы проявления компьютерных вирусов?

Черви

Вирусы-маскировщики

Вирусы – шпионы

Зомби

Рекламные вирусы

Вирусы – блокировщики

Троянские вирусы

4. Какие формы проявления компьютерных вирусов

наиболее незаметны для пользователя?

Вирусы-маскировщики

Вирусы – шпионы

Черви