УДК 003.26+347.78

Студ. А.С. Бондарев
Науч. рук. доц. Д. М. Романенко
(кафедра информатики и веб-дизайна, БГТУ)

ТЕНДЕНЦИИ РАЗВИТИЯ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВИРУСОВ НА ПЛАТФОРМЕ ANDROID

Платформа Google Android входит в число самых популярных в мире на сегодняшний день. Это довольно гибкое решение устанавливается практически в каждый смартфон, планшет и электронную книгу. Если учесть, что Android OS подвержена уязвимостям, которые в силу разных причин неактуальны для прочих платформ, то можно заключить, что заражения Android OS вирусами несут большой негативный эффект и затрагивают очень существенный сегмент мобильных устройств.

Stagefright (уязвимость MMC). В конце июля 2015 года в ядре мобильной операционной системы Android были обнаружены критические уязвимости, позволяющие злоумышленнику беспрепятственно выполнить любой вредоносный код и получить удалённый доступ к мобильному устройству и хранящимся на нём данным.

Данной угрозе подвержены мобильные устройства на базе операционной системе Android версий: 2.2 – 5.1.1. Самым опасным вектором атаки на абонентов является внедрение специального вредоносного кода в мультимедийный контент и рассылка его через службу мультимедийных сообщений – MMS. При поступлении подобного mms-сообщения вредоносный код выполняется автоматически, тем самым мобильное устройство оказывается заражённым вредоносным ПО. Адресату в данном случае не требуется выполнять никаких действий.

Получив контроль над устройством, вредоносный код может удалить присланное MMS-сообщение. Таким образом, владелец телефона может и не узнать о том, что ему было прислано подобное mms-сообщение. Демонстрация использование уязвимости на рис. 1.

Троян Шифровальщик. Вредоносные программы семейства Trojan.Encoder на сегодняшний день представляют, пожалуй, наиболее актуальную угрозу для пользователей персональных компьютеров. Впервые подобного рода троянцы были обнаружены в 2006–2007 году, когда пользователи неожиданно сталкивались с тем, что на их компьютерах оказались зашифрованными важные файлы, за расшифровку которых злоумышленники требовали заплатить выкуп (рис. 2). В те времена подобные инциденты были достаточно редки, а сам шифровальщик не отличался технологическим совершенством, поэтому компания «Доктор Веб» довольно быстро выпустила утилиту

для расшифровки пострадавших от его действия файлов. Однако вирусописатели начали стремительно модифицировать свои изделия, усложняя алгоритмы шифрования и структуру самих энкодеров. Уже к январю 2009 года насчитывалось 39 различных модификаций троянцев-шифровальщиков, а на сегодняшний день число их версий перевалило за несколько сотен.

Рисунок 1 – Пример использования вирусом уязвимости типа Stagefright

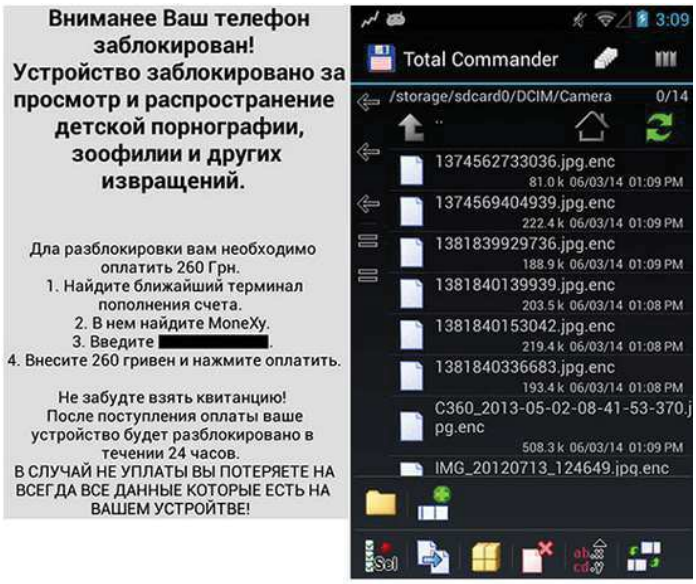

Рисунок 2 – Пример работы вируса Троян Шифровальщик

Троянцы-энкодеры распространяются различными способами: известны случаи рассылок таких троянцев по электронной почте, массовой отправки ссылок на вредоносные интернет-сайты в социальных сетях и с помощью программ обмена сообщениями (нередко вредоносная программа скачивается на компьютер жертвы под видом кодека, якобы необходимого для просмотра видео) — иными словами,

злоумышленники используют в своих целях все возможные методы, включая технологии социальной инженерии.

Технологически энкодеры различаются алгоритмами шифрования пользовательских файлов, языком, на котором они были написаны, но принцип их действия в целом одинаков. Запустившись на инфицированном компьютере, троянец выполняет поиск хранящихся на дисках файлов — документов, изображений, музыки, фильмов, иногда — баз данных и приложений, после чего шифрует их. Затем вредоносная программа демонстрирует жертве требование оплатить расшифровку файлов — оно может быть помещено на диске в виде текстового документа, выполнено в виде графического изображения и установлено в качестве обоев Рабочего стола Windows, либо сохранено в виде веб-страницы и добавлено в параметры автозагрузки. Для связи злоумышленники обычно используют адрес электронной почты, зарегистрированный на одном из бесплатных публичных сервисов.

Android ZBot. Троянская программа-банкер, работающая на смартфонах и планшетах под управлением ОС Android и предназначенная для кражи денег с банковских счетов пользователей (рис. 3). Попадает на мобильные устройства при посещении мошеннических или взломанных веб-сайтов, загружаясь с них под видом безобидных программ, либо скачивается другим вредоносным ПО.

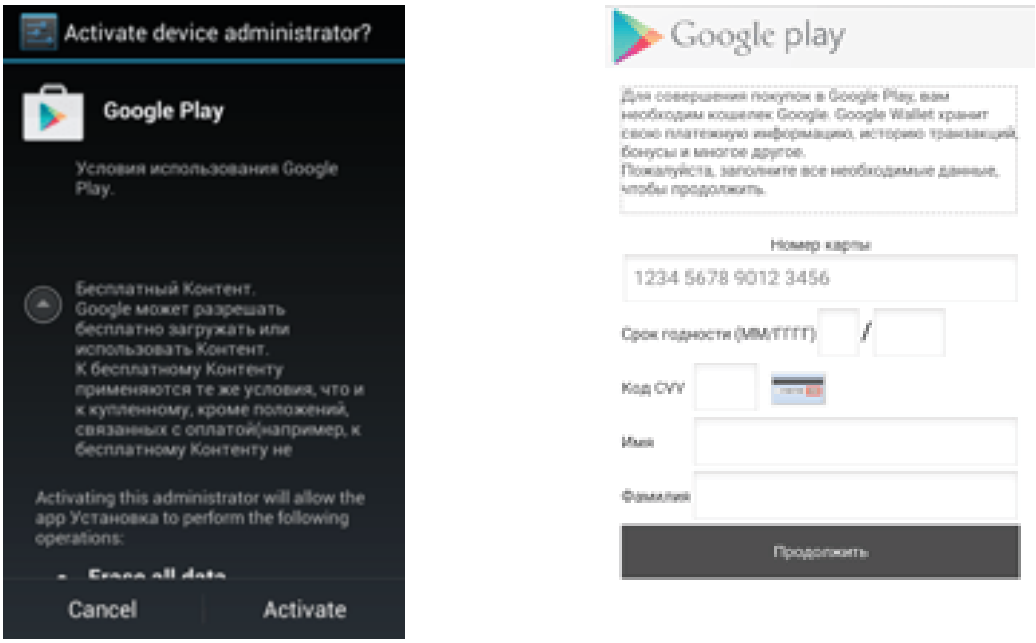

Рисунок 3 – Пример работы вируса *Android ZBot*

При первом запуске Android.ZBot.1.origin пытается получить доступ к функциям администратора мобильного устройства, после чего выводит сообщение об ошибке и предлагает выполнить перезагруз-

ку. Затем троянец удаляет свой значок с экрана приложений. Если пользователь отказывается предоставить вредоносной программе необходимые полномочия, Android.ZBot.1.origin пытается похитить у него данные о кредитной карте, показывая поддельную форму настроек платежного сервиса приложения Google Play. Аналогичное окно троянец может показывать через некоторое время после установки на целевом устройстве.

Android.SmsSend. Это семейство вредоносных программ, работающих на мобильных устройствах под управлением ОС Android. Троянцы этого семейства предназначены для отправки СМС-сообщений с повышенной тарификацией и подписки пользователей на различные платные контент-услуги и сервисы, в результате чего с абонентского счета может списываться определенная денежная сумма.

Большинство троянцев Android.SmsSend представляют собой самостоятельные программные пакеты с относительно простой архитектурой и функционалом, и чаще всего распространяются при помощи мошеннических сайтов под видом популярных игр и приложений, а также их обновлений.

Рисунок 4 – Пример работы вируса *Android.SmsSend*

По результатам проведенного исследования можно сделать вывод, что платформа ANDROID уязвима для сторонних атак и деструктивных программ. Задача устранения уязвимостей этой OS в большей части лежит на производителях смартфонов, в отличие от ОС Windows на PC занимается Microsoft. Большое внимание вредоносным программ ANDROID OS привлекла тем, что она очень популярна на смартфонах, этот факт облегчает получить доступ к счёту клиента мобильного оператора.