УДК 004.056

В.Н. Федорченко, И.В. Гензерский, Н.Ю. Шевякова

Харьковский национальный экономический университет, Харьков

АНАЛИЗ УГРОЗ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ И СПОСОБОВ ИХ ЗАЩИТЫ

Рассматриваются вопросы, связанные с существующими угрозами информационной безопасности для мобильных устройств. Предлагаются рекомендации для защиты мобильных устройств от угроз информационной безопасности для пользователей, предприятий, государственных учреждений, малого и среднего бизнеса, а также для разработчиков приложений под мобильные платформы.

Ключевые слова: *информационная безопасность, вредоносное ПО, мобильные устройства, угрозы мобильных устройств, утечка данных, целостность данных, модель безопасности, фишинг, троянские программы .*

Введение

Смартфоны и планшетные компьютеры стали распространенным способом доступа к информации, приложениям и ведению бизнеса, в то же время создавая новые возможности угроз. Возникают новые направления мобильной киберпреступности, новые возможности для злоупотребления и неправомерного использования мобильных устройств и данных.

Сегодня возникла необходимость сделать решения для обеспечения безопасности интегрированной и неотъемлемой частью работы с мобильными устройствами.

Цель статьи – выявить и проанализировать существующие угрозы для мобильных устройств и на основе проведенного анализа предложить возможные способы их устранения.

Угрозы

К главным угрозам для мобильных устройств можно отнести:

1). Атаки через веб-приложения и сети.

Как правило, запускаются вредоносными или скомпрометированными сайтами, а также используют уязвимости браузеров устройств. Такие сети пытаются установить вредоносное ПО или украсть конфиденциальные данные, проходящие через браузер.

2). Вредоносное ПО.

Аналоги классических вирусов, троянских программ и червей для мобильных.

3). Атаки с использованием социальной инженерии.

Иными словами, фишинг или прицельные атаки – представляют собой психологические уловки с целью обмана пользователей. Они вынуждают пользователя раскрыть секретную информацию или установить вредоносное ПО.

4). Захват ИТ-ресурсов.

Попытки использования сети, устройства и учетных данных пользователя во вредоносных целях – например, рассылка спама с инфицированных устройств, а также использование захваченных устройств для проведения атак "отказ в обслуживании".

5). Утечка данных.

Раньше угроза утечки данных применялась только для стандартных мобильных телефонов, но с развитием мобильных устройств атаке подверглись смартфоны и планшетные компьютеры. Такие атаки могут быть как намеренными, так и случайными. Они по-прежнему остаются крупнейшей угрозой для мобильных устройств. В ходе подобной операции злоумышленник уводит секретную информацию с устройства или из сети.

6). Угрозы целостности данных.

Цель такого мошенничества – нарушить работу организации или извлечь финансовую выгоду. Заключается в попытках злоумышленников изменить или повредить персональные данные владельца мобильного устройства.

Анализ угроз показал, что основной угрозой для мобильных устройств является вредоносное ПО. Исследование, проведенное лабораторией G Data SecurityLabs, показывает, что в начале 2011 года доля вирусов для смартфонов и планшетов увеличилась на 140% в соотнесении с общим количеством вредоносного ПО [1]. Также эксперты отмечают особую активность со стороны кросс-платформенных троянских программ, которые в данный момент доминируют на фоне других угроз. Большинство из них были созданы для распространения спама и прочей нелегальной деятельности, которую ведут электронные мошенники. Увеличение доли подобных преступлений лишь показывает, что нелегальный рынок вредоносных программ находится в своем зените.

В первую половину 2011 года специалисты G Data SecurityLabs зарегистрировали очередной рекорд: появление 1 245 403 новых семейств вредоносных программ. Это на 15,7% больше по сравне-

нию со второй половиной 2010 года. Эксперты предсказывают дальнейшее продолжение роста. К концу года G Data Software ожидает появление как минимум 2,5 миллиона новых семейств вирусов, и это будет составлять количество вирусов, равное числу зарегистрированных с 2006 по 2009 год.

Троянские программы по-прежнему будут доминировать, как отдельная категория. Рост их числа свидетельствует о том, что дела у кибермошенников идут более чем успешно, потому что эта группа вредоносного ПО помогает осуществлять большинство криминальных услуг, в ряду которых атаки по перегрузке целых систем. Также будет заметен рост рекламного вредоносного ПО. Количество атак, осуществленных через незакрытые уязвимости и при попутной загрузке, увеличилось лишь на доли процентов.

Существует серьезная опасность получения мобильного вируса через онлайн-магазины приложений App Store: вредоносное ПО распространяется преимущественно с закачиваемыми приложениями. Особую опасность это приобретает в свете того, что подавляющее большинство владельцев смартфонов сегодня не пользуются мобильным антивирусом для сканирования на наличие зараженных программ.

Кроме того, все чаще начинает встречаться угроза атаки через существующие беспроводные сети: мобильные устройства всё более восприимчивы к таким атакам, – существуют мобильные приложения, используя которые злоумышленник легко получает доступ к электронной почте и социальным сетям «жертвы». Основными последствиями этой угрозы является перехват данных через GPRS, 3G или WI-FI сети. На телефон может поступить сообщение с настройками сети, сохранив и активировав которое, пользователь сменит точки доступа, куда и пойдет нужный (через промежуточный сервер) мошенникам трафик.

Теперь рассмотрим более подробно другие угрозы для мобильных устройств. Текущая схема монетизации большинства мобильных троянских программ в настоящее время связана с отправкой SMS-сообщений на короткие номера. В результате либо со счета пользователя списываются деньги, либо владельца телефона без его согласия подписывают на платный сервис. Во втором случае, более распространенном в Азиатском регионе, пользователю с сервиса приходит SMS-сообщение с информацией о подписке. Чтобы владелец телефона не заподозрил неладное, троянцы удаляют сообщение о платной подписке, как только оно приходит. Таким образом, троянские программы могут функционировать на одном устройстве очень долго – и приносить своему хозяину постоянный доход.

По данным Juniper GTC, 17% всех устройств были поражены SMS троянскими программами [2].

Несмотря на все уловки хакеров, по-прежнему более серьезную опасность представляет кража или потеря самих устройств – по статистике, с этим сталкивается каждый 20-й абонент. В результате возникает необходимость в командах геолокации, блокировки или уничтожения данных, хранящихся на таких устройствах. Кроме того, около 20% подростков допускают отправку с мобильного устройства конфиденциальных или персональных данных.

По статистике Лаборатории Касперского рост количества мобильных угроз под различные мобильные платформы набирает обороты.

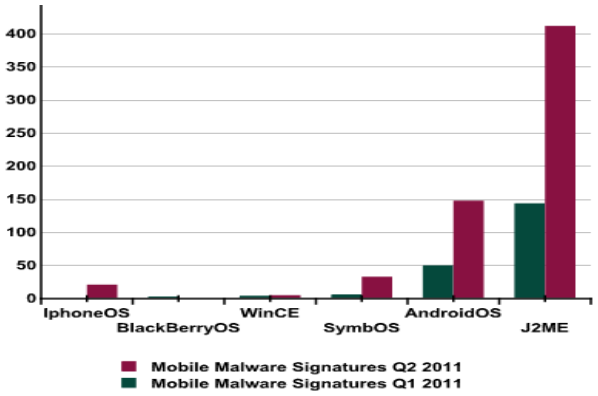

Рис. 1. Число добавленных сигнатур для нового мобильного вредоносного ПО под различные платформы за первый и второй квартал 2011 года

Количество записей, детектирующих вредоносное ПО под J2ME (вредоносное ПО для телефонов и смартфонов начального уровня), за квартал увеличилось в два раза, а число детектов вредоносных программ для Android OS выросло почти в три раза, что получило даже собственное название – «Droid-бедствие» [5].

Одним из аспектов безопасности мобильных устройств связан с развитием мобильных платежей. Эксперты отмечают, что смартфоны и коммуникаторы, коренным образом изменили отношение к возможностям сотового телефона. Теперь смартфонами пользуются не только бизнесмены, но и обычные пользователи, которым удобнее покупать цифровой контент или контролировать состояние банковского счета прямо с телефона.

Одним из самых распространенных видов атаки стал также фишинг с использованием URL-адресов, похожих на адреса веб-сайтов налоговых служб, подарочных ваучеров, премиальных программ и учетных записей в социальных сетях. Согласно исследованию компания McAfee Labs было установлено, что среди 100 первых результатов поиска по самым популярным ежедневным запросам 51 процент вел на вредоносные сайты, и на каждой из таких страниц с искаженными результатами поиска содержалось в среднем более пяти вредоносных ссылок [3, 4].

В октябре 2010 г. по заказу компании Juniper агентствами KRC Research и Synovate было проведено международное исследование, в ходе которого было опрошено 6000 владельцев смартфонов и планшетных компьютеров в 16 странах мира. Исследование показало, что более 76% потребителей используют мобильные устройства для доступа к секретным бизнес-ресурсам или важной персональной информации, в том числе: 51% вводят или изменяют пароли, 43% проверяют банковские счета, 30% – коммунальные платежи, 20% передают финансовую информацию, например, номера кредитных карт, 1 % используют мобильные устройства для доступа информации, составляющей корпоративную тайну работодателя, 17% – к медицинским данным, 16% – для передачи данных социального страхования.

Способы защиты мобильных устройств

Чтобы защитить устройство от растущего числа мобильных вредоносных программ, пользователям рекомендуется следующее [5]:

1) устанавливать приложения для защиты от вредоносного ПО, шпионских программ, инфицированных SD-карт, а также хакерских атак на устройства;

2) использовать персональный брандмауэр для защиты интерфейсов устройства;

3) следить за недоступностью для других лиц пароля для доступа к устройству.

Можно установить и антиспам-программы для защиты от нежелательных голосовых и SMS/MMS-сообщений. Родителям рекомендуется пользоваться программами и устройствами мониторинга ПО для контроля и управления обращения детей с мобильными устройствами, а также для защиты от запугивания, преследования, провокационного или неправильного использования и других угроз.

Для предприятий, государственных учреждений, малого и среднего бизнеса рекомендуется следующее: устанавливать встроенные приложения защиты от вредоносного ПО, шпионских программ, инфицированных SD-карт, а также хакерских атак на устройство. Использовать стратегии компании, позволяющие свести к минимуму воздействие угроз безопасности на мобильные устройства. Из них стоит выделить следующие подходы:

VPN (Virtual Private Network – виртуальная частная сеть): VPN является достаточно хорошей и понятной технологией безопасности. Многие предприятия приняли его и пришли к мнению, что VPN позволяет обезопасить использование мобильных устройств. SSL (Secure Sockets Layer), в частности, также становится все более популярным – как форма VPN, который может быть использован со стандартным веб-браузером и не требуют установления специализированного клиентского программного обеспечения на компьютерах конечных пользователей.

NAC (Network Access Control – сетевой контроль доступа): путем ограничения доступности сетевых ресурсов для конечного устройства через NAC, можно существенно повысить безопасность сети. Доступ предоставляется или запрещается на основе заранее определенных политик безопасности, которые определяют, где пользователи и устройства могут быть допущены к сети и то, что они смогут сделать. Хотя хороший NAC иногда трудно осуществить, особенно, когда используется множество устройств и пользователей, основная идея состоит в том, что, контроль доступа осуществляется на постоянной основе.

Централизовать локальную и удаленную блокировку, форматирование, резервное копирование и восстановление данных для потерянных и украденных устройств, кроме того, строго соблюдать политику безопасности и использовать надежные PIN-коды и коды доступа. Можно также максимально использовать устройства регистрации и видеозаписи для выявления утечек данных и неправомерного использования устройств, а также централизовать управление мобильными устройствами для соблюдения и контроля требований политики безопасности.

Рассмотрим способы обеспечения безопасности разработчиками мобильных устройств на четырех наиболее распространенных платформах: iOS, Android, Windows Phone 7 и J2ME. Модель безопасности iOS предлагает серьезную защиту от традиционного вредоносного ПО, главным образом, за счет строгих процедур сертификации приложений и разработчиков, используемых компанией Apple, что позволяет достоверно установить автора любой программы и отсеять злоумышленников.

Google в отношении Android выбрала менее жесткую модель сертификации, позволяя любому разработчику ПО создавать и выпускать свои приложения анонимно, без дополнительной проверки. Облегченная сертификация привела к тому, что сегодня можно наблюдать постоянный прирост числа вредоносных программ для Android-устройств [8].

В Windows Phone 7 реализованы функции безопасности как часть архитектуры ОС. Безопасность на уровне приложения позволяет только непрямой доступ к файловым ресурсам и функциям операционной системы через API. Изолированное хранилище предлагает каждому приложению отдельную область хранения данных.

Windows Phone Application Platform использует различные технологии, предназначенные для защиты пользователей от приложений, которые обладают определенным нежелательным поведением:

1). Структурированное представления заявки и процесса сертификации приложений, которое включает в себя набор сертификационных испытаний для выявления определенного поведения (Windows Phone Marketplace).

2). Необходимость разработки Windows приложений с использованием только .NET управляемого кода помогает улучшить производительность труда разработчиков и надежность их применения.

3). Windows Phone приложения запускаются в изолированных процессах.

4). Windows Phone приложения выполняются под контролем менеджера исполнения.

5). Изолированный процесс, в котором конкретное приложение работает имеет настраиваемый набор функций безопасности.

Модель безопасности J2ME использует следующие механизмы [6-7]:

1) java byte-code pre-verification – данную проверку проходят все классы приложения, прежде, чем происходит формирование пакета приложения (jar-файла);

2) интерпретируемая инсталляция – под данным термином понимается то, что у приложения нет активной стадии установки в ОС устройства (тоже касается и удаления);

3) дескриптор безопасности. Реализует ограничение действий приложения, если оно пытается выполнить действия, которые выходят за рамки установленных ограничений виртуальной машины;

4) подписка приложения – предоставляет дополнительные права доверенным приложениям.

Выводы

Выявлены и проанализированы существующие угрозы информационной безопасности для мобильных устройств. Предложены рекомендации для защиты мобильных устройств от угроз информационной безопасности для пользователей, предприятий, государственных учреждений, малого и среднего бизнеса, а также для разработчиков приложений под мобильные платформы. Ситуация с мобильными угрозами усугубляется тем, что личные смартфоны все чаще используются для хранения и передачи ценной корпоративной информации. При этом сами сотрудники компаний относятся к защите данных на таких устройствах довольно беспечно. Кроме того, уже в ближайшем будущем телефоны могут превратиться в мобильные кошельки, в результате чего вопрос об их защите приобретет еще большую актуальность.

Список литературы

1. Исследование лаборатории G Data SecurityLabs [Электронный ресурс]. – Режим доступа к ресурсу: http://ru.gdatasoftware.com/security-labs.

2. Доклад «Мобильные угрозы 2010/2011» [Электронный ресурс]. – Режим доступа к ресурсу: http://www.juniper.net/ru/ru/dm/interop/go/.

3. McAfee Threats Report: Second Quarter 2011 [Электронный ресурс]. – Режим доступа к ресурсу: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf.

4. McAfee Threats Report: First Quarter 2011 [Электронный ресурс]. – Режим доступа к ресурсу: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2011.pdf.

5. Сайт SecureList [Электронный ресурс]. – Режим доступа к ресурсу: http://www.securelist.com/ru /analysis.

6. Bryan Morgan. J2ME Security: Now and in the Future. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.informit.com/articles/

7. Michael Yuan. Securing your J2ME/MIDP apps. [Электронный ресурс]. – Режим доступа к ресурсу: http://www-128.ibm.com/developerworks/library/

8. Доклад «A Window into Mobile Device Security: Examining the security approaches employed in Apple's iOS and Google's Android» [Электронный ресурс]. – Режим доступа к ресурсу: http://okfo.net/svyaz/symantec-ios-i-android-uyazvimy-dlya-zloumyshlennikov.html.

Поступила в редколлегию 4.10.2011

Рецензент: канд. екон. наук, проф. І.О. Золотарьова, Харківський національний економічний університет, Харків.

АНАЛІЗ ЗАГРОЗ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ ТА ЗАСОБІВ ЇХ ЗАХИСТУ

В.М. Федорченко, І.В. Гензерський, Н.Ю. Шевякова

Розглядаються питання, що стосуються існуючих загроз інформаційної безпеки для мобільних пристроїв. Пропонуються рекомендації щодо захисту мобільних пристроїв проти загроз інформаційної безпеки до користувачів, підприємств, державних установ, малих та середніх підприємств та розробникам додатків до мобільних платформ.

Ключові слова: *інформаційна безпека, шкідливе ПЗ, мобільні пристрої, загрози мобільних пристроїв, витік даних, цілісність даних, модель безпеки, фішинг, троянські програми.*

ANALYSIS OF THREATS FOR MOBILE DEVICES AND METHODS OF PROTECTION

V.N. Fedorchenko, I.V. Genzersky, N.Yu. Shevyakova

The questions arising from the threats of information security for mobile devices. Proposes recommendations to protect mobile devices from threats of information security for users, enterprises, government agencies, small and medium businesses, and for developers of applications for mobile platforms.

Keywords: *information security, malicious software, mobile devices, the threat of mobile devices, data leakage, data integrity, safety model, phishing, Trojans.*