

УДК 34:004

МОБИЛЬНЫЕ КОММУНИКАЦИОННЫЕ УСТРОЙСТВА И ИХ ИСПОЛЬЗОВАНИЕ В ПРОТИВОПРАВНЫХ ЦЕЛЯХ

А. Н. Лямцев

ФГБОУ ВПО «Тамбовский государственный технический университет», г. Тамбов

Рецензент д-р техн. наук, профессор В. Н. Чернышов

Ключевые слова и фразы: мобильные устройства; мошенничество с помощью мобильных устройств; мобильные бот-сети; способы заражения мобильных устройств; меры предосторожности.

Аннотация: Рассмотрены некоторые вопросы безопасности использования мобильных устройств, возможные риски и проблемы. Исследованы некоторые способы совершения противоправных деяний с использованием мобильных устройств. Даны рекомендации по избежанию данных ситуаций.

Роль мобильного устройства в жизни человека сложно переоценить. Мобильные телефоны, смартфоны и планшеты становятся все более доступными, функциональными и удобными в использовании. Сегодня телефон в нашей жизни – это не редкость и не роскошь, а необходимость. Большую долю среди мобильных устройств имеют смартфоны – более функциональные и сложные, чем простой телефон, предоставляющие своим владельцам широкий спектр полезных и развлекательных приложений, доступ в Интернет, управление банковскими счетами и т.д. По данным аналитиков уже к концу 2014 года смартфонами будет пользоваться около четверти населения Земли, а к 2017 году данный показатель может достигнуть отметки в 1/3 часть населения нашей планеты.

Цель данной статьи – указать на отрицательные стороны и возможные опасности при использовании мобильных устройств, а также на необходимость эффективной правовой защиты пользователей от возможных преступных посягательств, помочь избежать ненужных рисков и быть более внимательным при обращении с мобильным устройством. С ростом числа пользователей смартфонов растет и количество противоправных действий,

Лямцев Александр Николаевич – аспирант кафедры «Уголовное право и прикладная информатика в юриспруденции», e-mail: alex-l.a.n@yandex.ru, ТамбГТУ, г. Тамбов.

связанных с ними, особенно в отношении устройств на базе ОС Android. И в большинстве своем жертвы таких действий просто не подготовлены и даже не задумываются о том, что сами могут быть отчасти виновны в наступивших последствиях.

Одним из основных плюсов смартфона является возможность практически всегда и везде иметь доступ к различного рода информации, что без сомнения, полезно и удобно, однако, все может сработать и в обратную сторону. Обладая некоторыми навыками и опытом, можно получить информацию и о самом устройстве, и его владельце. Злоумышленник может получить полный дистанционный контроль над устройством и использовать это в дальнейшем в своих преступных целях. Целью, в основном, являются деньги, а способов достижения великое множество – начиная с мошенничества и заканчивая использованием добытой информации для взлома целых банковских систем.

В качестве примера мошеннических действий приведем следующую, уже неоднократно использовавшуюся злоумышленниками, схему: потерпевшему приходит СМС-сообщение с текстом: «Ваша банковская карта заблокирована. Информация по телефону: (указывается абонентский номер мошенника)». Потерпевший звонит на номер, указанный в СМС-сообщении. Мошенник представляется работником службы безопасности банка и объясняет потерпевшему, что была попытка взлома банковской карты потерпевшего и поэтому банковскую карту заблокировали. Для ее разблокировки нужно подойти к банкомату и снова позвонить по указанному номеру. При этом мошенник говорит потерпевшему, что если не сделать разблокировку в течение 1-2 часов, то нужно будет менять банковскую карту, а данный процесс занимает около месяца и все это время денежными средствами на карте нельзя будет воспользоваться. Потерпевший, действуя по указаниям мошенника, вставляет банковскую карту в банкомат, набирает пин-код и сообщает остаток денежных средств на карте мошеннику. Далее, действуя по указаниям мошенника, набирая цифры, якобы кода для разблокировки карты, переводит денежные средства со своей карты на лицевые счета абонентских номеров сотовых операторов, на банковскую карту. Получая чеки банкомата, потерпевший видит, что перевел деньги со своей карты на чужой счет, но мошенник убеждает его, что денежные средства временно переведены на другой счет – зарезервированы и скоро вернутся обратно. При этом обращает внимание потерпевшего на надпись внизу чека: «Средства зарезервированы». После этого мошенник просит не пользоваться картой в течение 2 часов или более. Далее мошенник в течение нескольких часов переводит деньги либо на другие счета, либо обналичивает. По похожей схеме также могут быть похищены денежные средства с использованием услуги «Мобильный банк», но в этом случае злоумышленники, получив всю необходимую им информацию, могут осуществлять хищение со счета потерпевшего неоднократно.

Таким образом, доверчивость, на которую и делают ставку мошенники, может серьезно ухудшить финансовое положение пользователя мобильного устройства и отнять большое количество времени на то, чтобы попытаться похищенные средства вернуть. Пользователям необходимо знать, что в такой ситуации решать все проблемы с банковскими картами

необходимо только в офисах банков в ходе личного общения с их работниками. Иные способы не могут дать гарантии безопасности и сохранности денежных средств.

Существуют и гораздо более сложные способы совершения противоправных деяний с мобильными устройствами, и они одновременно могут охватывать очень большое их количество. Так в конце 2013 года специалисты компании «Доктор Веб» обнаружили самую крупную в мире бот-сеть из инфицированных мобильных устройств на базе ОС Android. На момент обнаружения было известно о более чем 200 000 (более половины при этом принадлежит российским пользователям) смартфонах, которые были заражены вредоносными программами. Ущерб, нанесенный пользователям в результате противоправных действий, может исчисляться сотнями тысяч долларов. Для заражения мобильных устройств и включения их в состав бот-сети злоумышленники использовали несколько вредоносных приложений, маскирующихся под различные полезные программы – браузеры, клиенты социальных сетей и т.д. Появившись в телефоне, программа отправляет злоумышленникам информацию об инфицированном устройстве, включая уникальный идентификатор IMEI, сведения о балансе, код страны, номер телефона жертвы, код оператора, модель мобильного телефона и версию ОС. Далее программа ожидает поступления от злоумышленников соответствующей команды, по которой может отправить СМС-сообщение с определенным текстом на заданный номер, выполнить СМС-рассылку по списку контактов, открыть заданный адрес в браузере или продемонстрировать на экране мобильного устройства сообщение

с определенным заголовком и текстом. Такие бот-сети в дальнейшем могут быть использованы, например, для атаки на банковские системы и их пользователей. В конце 2013 года службой безопасности Сбербанка России была зафиксирована кибератака на владельцев смартфонов на базе ОС Android. Злоумышленники заражали их вредоносным программным обеспечением через массовую рассылку MMS-сообщений от имени «RomanticVK» или «VK_Gift» с обещанием «романтического подарка»: переход по ссылке приводил к загрузке вируса. Вирус совершал операцию пополнения счета мобильного телефона клиента, а затем через СМС-сервисы мобильных операторов средства выводились на счета других абонентов операторов связи и электронных платежных систем.

Первая волна атаки, благодаря оперативной реакции подразделения безопасности Сбербанка России и взаимодействию с операторами сотовой связи, была успешно отражена. После небольшой паузы, злоумышленники продолжили противоправную деятельность, усовершенствовав вредоносную программу. В дальнейшем злоумышленников, осуществивших данные противоправные действия, задержали, но их место могут занять другие с еще более совершенным программным обеспечением, поэтому за безопасностью должны следить, в том числе, и обычные пользователи. Заражения устройств вредоносными программами каждый раз происходило по вине самих пользователей, которые по невнимательности или незнанию сами скачивали и устанавливали эти приложения. Будь то сомнительного содержания источник или сообщение со ссылкой, скачивал файл или переходил по ссылке сам пользователь.

В данном случае пользователям мобильных устройств, особенно столь функциональных как смартфон, стоит более внимательно относиться к поступающим с незнакомых номеров сообщениям, обещающим какие-то подарки, награды и т.д. Не стоит переходить по различным ссылкам в таких сообщениях, что бы они ни обещали. Даже ссылка от кого-то из контакт-листа может оказаться вредоносной, если его устройство подверглось заражению. Поэтому сообщение, к примеру, от друга, знакомого или родственника, которые раньше ничего подобного не присылали, должно явно насторожить. Также не стоит качать приложения с различных сомнительных источников. Для ОС Android есть официальная платформа – Play Market, предустановленная на большинстве смартфонов под управлением данной ОС. Эта платформа позволяет не только найти и скачать множество полезных приложений, но и увидеть отзывы о них реальных людей, рейтинги данных приложений и сделать выводы о его полезности и безопасности. Для устройств под управлением других ОС (iOS, Windows Phone, и др.) также есть свои подобные площадки, помогающие уменьшить риск заражения устройства вредоносной программой. Администрация данных ресурсов всегда следит за публикуемым там содержимым и удаляет или не допускает вовсе появления сомнительных приложений.

В заключение отметим следующее: технические средства злоумышленников совершенствуются с каждым днем, и количество их жертв растет, однако, в большинстве своем этот рост связан с тем, что сами жертвы предоставляют преступникам такую огромную свободу действий, совершенно не задумываясь о последствиях. В наш цифровой век владение информацией является ключевым моментом, который может оказать серьезное влияние на множество вещей. Не стоит доверять полученной откуда-либо информации, если нет возможности проверить ее, особенно если она поступила от совершенно незнакомых лиц, с неизвестных номеров и т.д. Не стоит так пренебрежительно относиться к ее безопасности. Нужно быть внимательней и осторожней в своих действиях в информационном пространстве, иначе последствия могут наступить самые серьезные.

Также необходима и более серьезная правовая защита от указанных выше преступных посягательств. Рост количества таких преступлений указывает на то, что в данный момент защита не эффективна и не является таким сдерживающим фактором, каким должна быть. Ужесточение наказаний, в особенности увеличение штрафов, может быть и действенной ответной мерой на уже совершенное преступление, а также предупредить готовящиеся. Поскольку деятельность преступников в указанных выше случаях направлена, в основном, на завладение чужими денежными средствами, именно этого в первую очередь и стоит их лишить. Более крупные сроки лишения свободы также могут сыграть положительную роль, поскольку преступник не только будет изолирован от общества и не сможет совершать противоправные деяния, но также и технический прогресс неизбежно пройдет мимо него (что должно быть обеспечено условиями отбытия наказания), и ранее работавшие методы станут не эффективными.

Таким образом, сочетание собственной внимательности и ответственности с развитой и эффективной правовой защитой может стать серьезным препятствием на пути злоумышленников и обеспечить возможность более безопасного использования современных технологий.

Список литературы

1. Волков, Д. Мобильная бот-сеть и как на ней зарабатывают [Электронный ресурс] / Дмитрий Волков, Николай Шелехов // Хакер. – 18.12.2013. – Режим доступа : <http://хакер.ru/61780/> (дата обращения: 02.09.2014).

2. Обнаружена крупнейшая в мире бот-сеть из 200000 зараженных устройств на базе Android [Электронный ресурс] // Доктор Веб. – 20.09.2013. – Режим доступа : <http://news.drweb.com/?i=3929> (дата обращения: 05.09.2014).

3. Пользоваться смартфонами будет четверть населения Земли уже в 2014 году. [Электронный ресурс] // Lenta.ru. – 11.06.2014. – Режим доступа : <http://lenta.ru/news/2014/06/11/smartfoni> (дата обращения: 11.09.2014).

4. Group-IB: впервые задержаны создатели мобильной банковской бот-сети [Электронный ресурс] // Group-IB. – 11 июня 2014. – Режим доступа : <http://group-ib.ru/list/176-news/?view=article&id=1675> (дата обращения: 22.09.2014).

References

1. Volkov D., Shelekhov N., available at: <http://хакер.ru/61780/> (accessed 5 September 2014).

2. <http://news.drweb.com/?i=3929> (accessed 5 September 2014).

3. <http://lenta.ru/news/2014/06/11/smartfoni> (accessed 11 September 2014).

4. <http://group-ib.ru/list/176-news/?view=article&id=1675> (accessed 14 September 2014).

Mobile Communication Devices and their Usage for Illegal Purposes

A. N. Lyamtsev

Tambov State Technical University, Tambov

Key words and phrases: cheating by means of mobile devices; mobile botnets; mobile devices; precautionary measures.

Abstract: Some questions of safe usage of mobile devices, possible risks and problems are investigated in this work. The ways of committing illegal actions by means of mobile devices are investigated. Some recommendations on prevention of such situations have been made.

© А. Н. Лямцев, 2014

Статья поступила в редакцию 07.10.2014 г.