МОБИЛЬНЫЕ УГРОЗЫ - 2013

Унучек Роман Сергеевич,
Чебышев Виктор Владимирович

Индустрия мобильного вредоносного программного обеспечения (ПО) стремительно развивается, как в технологическом плане, так и в структурном. Можно смело утверждать, что современный киберпреступник уже не пират-одиночка, а, скорее, звено в серьезном криминальном бизнес-процессе. Вирусописатели, тестеры, дизайнеры интерфейса вредоносных приложений и веб-страниц, с которых они распространяются, владельцы партнерок, распространяющих вредоносные программы, владельцы мобильных ботнетов и т.д. – каждый из них выполняет свою роль в процессе производства и реализации вредоносного ПО.

В 2013 году зафиксированы факты сотрудничества (скорее всего – на коммерческой основе) разных групп вирусописателей. К примеру, ботнет Trojan-SMS.AndroidOS.Opfake.a, помимо собственной вредоносной деятельности, распространял Backdoor.AndroidOS.Obad.a путем рассылки спама со ссылками на зловред по списку контактов жертвы.

Сегодня такая, можно сказать, индустрия достаточно оформилась и становится все более ориентированной на эффективное извлечение прибыли, что хорошо иллюстрируют возможности вредоносных программ.

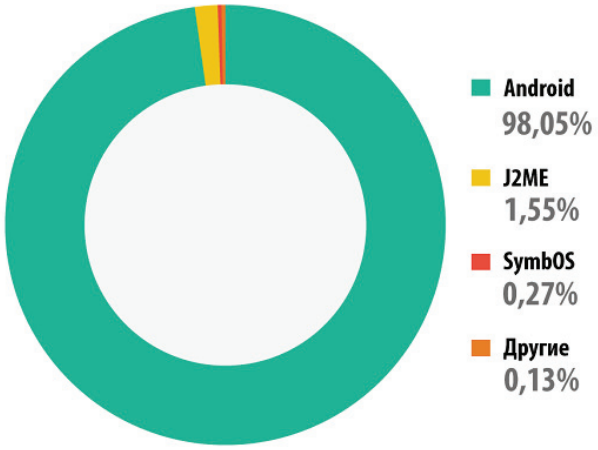
Приведем соответствующие цифры года:

- в течение года было обнаружено 143 211 новых модификаций вредоносных программ для мобильных устройств (данные на 1 января 2014 г.).
- в 2013 году для распространения мобильных зловредов злоумышленники использовали около 4 млн (3 905 502) установочных пакетов. Всего за 2012-2013 годы специалисты Лаборатории Касперского выявили около 10 млн уникальных вредоносных установочных пакетов.

Напомним, что разные установочные пакеты могут устанавливать программы с одним и тем же функционалом, разница может заключаться лишь в интерфейсе вредоносного приложения и, например, в содержимом отправляемых им SMS.

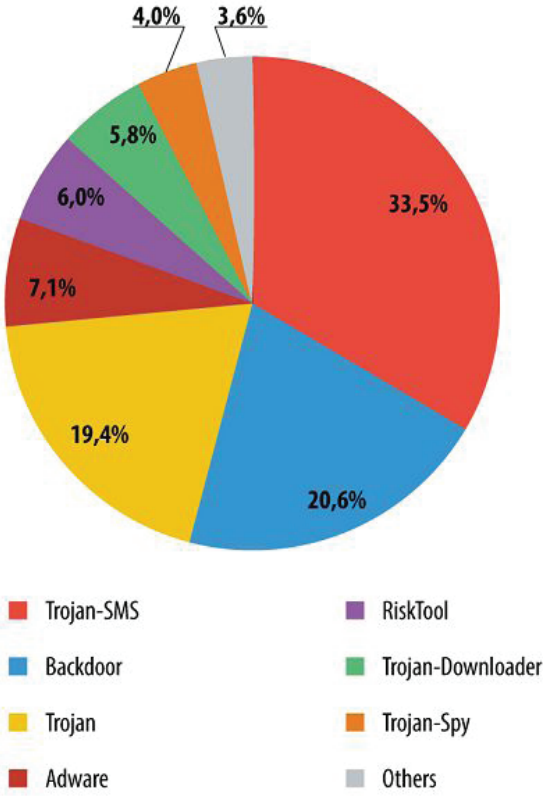
- Анализ свидетельствует, что Android по-прежнему остается основной целью для вредоносных атак. Так, 98,05% всех зловредов, обнаруженных в 2013 году, нацелены именно на эту платформу, что свидетельствует как о популярности этой мобильной ОС, так и об уязвимости ее архитектуры.

Ниже см.: распределение мобильных вредоносных программ, обнаруженных в 2013 году, по платформам:



Отметим, что большинство мобильных вредоносных программ нацелены на кражу денег пользователей, особенно этим промышляют Trojan-SMS, многие бэкдоры и часть вредоносных программ категории Trojan.

Ниже см.: распределение мобильных вредоносных программ по категориям:



За 2013 г. число модификаций мобильных здовредов для фишинга, кражи информации о кредитных картах и хищения денег с банковских счетов пользователей увеличилось в 19,7 раз. За этот период мобильные продукты Лаборатории Касперского предотвратили 2,5 тыс. заражений банковскими троянцами.

Рассмотрим применяемые вирусописателями технологии.

В 2013 году мобильные вирусописатели не просто радикально увеличили количество своей вредоносной продукции, но и активно применяли методы и технологии, которые позволяют киберпреступникам использовать вредоносные программы более эффективно. При этом можно выделить несколько направлений развития мобильных зловредов:

1) Распространение – при его применении злоумышленники использовали весьма непростые способы заражения мобильных устройств.

1.2) Инфицирование легальных веб-ресурсов позволяет распространять мобильные вредоносные программы через популярные веб-сайты. Все больше людей используют свои смартфоны и планшеты для посещения веб-сайтов, не задумываясь о том, что даже самый солидный ресурс может быть взломан злоумышленниками. По нашим подсчетам из всех веб-сайтов, на которые заходили с мобильных устройств пользователи продуктов «Лаборатории Касперского», 0,4% были заражены в результате взлома.

1.3) Распространение через альтернативные магазины приложений. В Азии расположено множество компаний, выпускающих Android-устройства и Android-приложения, и многие из них предлагают пользователям собственные магазины приложений, которые содержат программы, отсутствующие в Google Play. Контроль за загруженными приложениями в этих магазинах нередко чисто формальный, что позволяет злоумышленникам размещать там своих троянцев под видом вполне невинных игр и утилит.

1.4) Распространение через ботнеты. Как правило, боты распространяют себя, рассылая SMS с вредоносной ссылкой по контактам жертвы. Был отмечен и случай распространения мобильного зловреда через сторонний ботнет.

При этом подчеркнем, что важным направлением развития вредоносного мобильного программного обеспечения (ПО) является максимальное продление срока, в течение которого оно может действовать на мобильном устройстве жертвы. Чем дольше троянец «живет» на смартфоне, тем больше у него возможностей «умыкнуть» денег для киберзлоумышленника. В этом направлении вирусописатели активно ведут исследования, о чем свидетельствует, в частности, растущее количество технологических новинок.

В этих целях все чаще злоумышленники используют обфускацию – процедуру запутывания кода, затрудняющую его анализ. При этом чем сложнее обфускация, тем больше времени пройдет до того момента, когда вредоносная программа будет уверенно обезвреживаться антивирусами. Сейчас вирусописатели освоили и коммерческие обфускаторы, что подразумевает вложение денег - зачастую немалых. Например, один из коммерческих обфускаторов стоимостью от 350 евро использовался для троянцев Opfake .bo и Obad.a.

2) Android-уязвимости злоумышленники используют для трех разных целей: для обхода проверки целостности кода приложения при его установке (уязвимость Master Key, см.: http://www.securelist.com/en/blog/9107/Master_Keys_and_Vulnerabilities); для повышения прав вредоносных приложений, что значительно расширяет их возможности; и для затруднения удаления зловредов. К примеру, Svpeng использует уязвимость для защиты от удаления вручную или антивирусом.

Также киберпреступники, эксплуатируя уязвимость Master Key, освоили внедрение в инсталляционные пакеты Android-программ неподписанных исполняемых файлов. Проверку цифровой подписи удается обойти, назвав вредоносный файл точно так же, как легитимный, и поместив его на том же уровне архива. Система проверяет подпись легитимного файла, а устанавливается вредоносный.

К сожалению, у Android-устройств есть неприятная особенность: избавиться от уязвимостей в них можно лишь с получением обновления от производителя устройства, а многие из них не спешат обновлять ОС своих продуктов. Если же ваш смартфон или планшет выпущен более года назад, его поддержка производителем, скорее всего, прекращена, и на закрытие уязвимостей рассчитывать вообще не стоит. В данном случае помочь может только антивирусное решение, например, Kaspersky Internet Security для Android.

3) Внедрение вредоносного кода в легитимные программы помогает скрывать от жертвы сам факт заражения. Разумеется, это не позволяет использовать цифровую подпись разработчика программы, но, благодаря отсутствию удостоверяющих центров для цифровых подписей Android-программ, ничто не мешает злоумышленникам поставить собственную подпись, что они и делают. Таким образом, вполне нормально рабо-

тающие Angry Birds, установленные из неофициального магазина приложений или загруженные с форума, запросто могут обладать и вредоносным функционалом.

Кроме того, в 2013 году специалисты ЛК обнаружили несколько технологических новинок, разработанных и использующихся злоумышленниками в своем вредоносном ПО. Отметим несколько наиболее интересных.

Управляемость зловредов из единого центра обеспечивает максимальную гибкость в применении зловреда. Ботнеты позволяют получить значительно большую прибыль, чем автономные троянцы. Не удивительно, что многие SMS-троянцы обладают еще и функционалом ботов. По нашим оценкам, около 60% мобильных вредоносных программ представляют собой элементы больших и малых мобильных ботнетов.

Так, управление через Google Cloud Messaging позволяет владельцам ботнета обходиться вообще без C&C-сервера, что устраняет угрозу его обнаружения и закрытия правоохранительными органами. Сервис Google Cloud Messaging предназначен для передачи на мобильные устройства небольших сообщений объемом до 4 Кб посредством серверов Google. Для его использования разработчику нужно лишь зарегистрироваться и получить уникальный ID для своих приложений. Команды, получаемые через GCM, невозможно заблокировать непосредственно на зараженном устройстве.

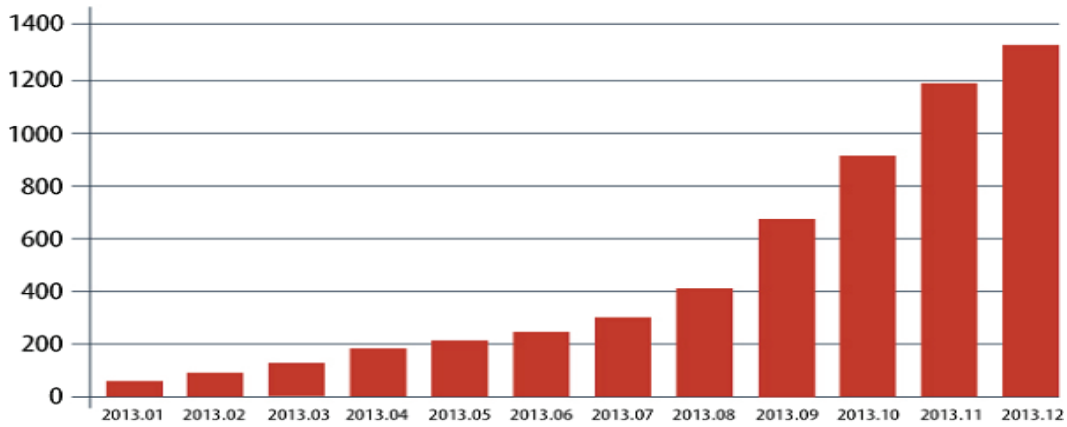
Мы обнаружили несколько вредоносных программ, использующих GCM для управления и контроля: широко распространенный Trojan-SMS.AndroidOS.FakeInst.a, Trojan-SMS.AndroidOS.Agent.ao, Trojan-SMS.AndroidOS.OpFake.a и многие другие. Google активно противодействует такому использованию сервиса и блокирует ID злоумышленников, оперативно реагируя на сообщения антивирусных компаний.

Мобильный зловред может провести атаку на Windows XP и заразить персональный компьютер при подключении к нему смартфона или планшета. В начале 2013 года мы обнаружили в Google Play два идентичных приложения, служащих якобы для очистки операционной системы Android-устройства от ненужных процессов. На деле задачей этих приложений является загрузка файла autorun.inf, файла иконки и файла win32-троянца, которые мобильный зловред размещает в корневой директории SD-карты. При подключении смартфона в режиме эмуляции USB-накопителя к компьютеру, работающему под управлением Windows XP, система автоматически запускает троянца (если функция автозапуска с внешних носителей не отключена) и заражается. Троянец обеспечивает злоумышленникам удаленное управление компьютером жертвы, и, кроме того, он способен записывать звук с микрофона. Подчеркнем, что этот метод атаки работает только на Windows XP и Android версии до 2,2 включительно.

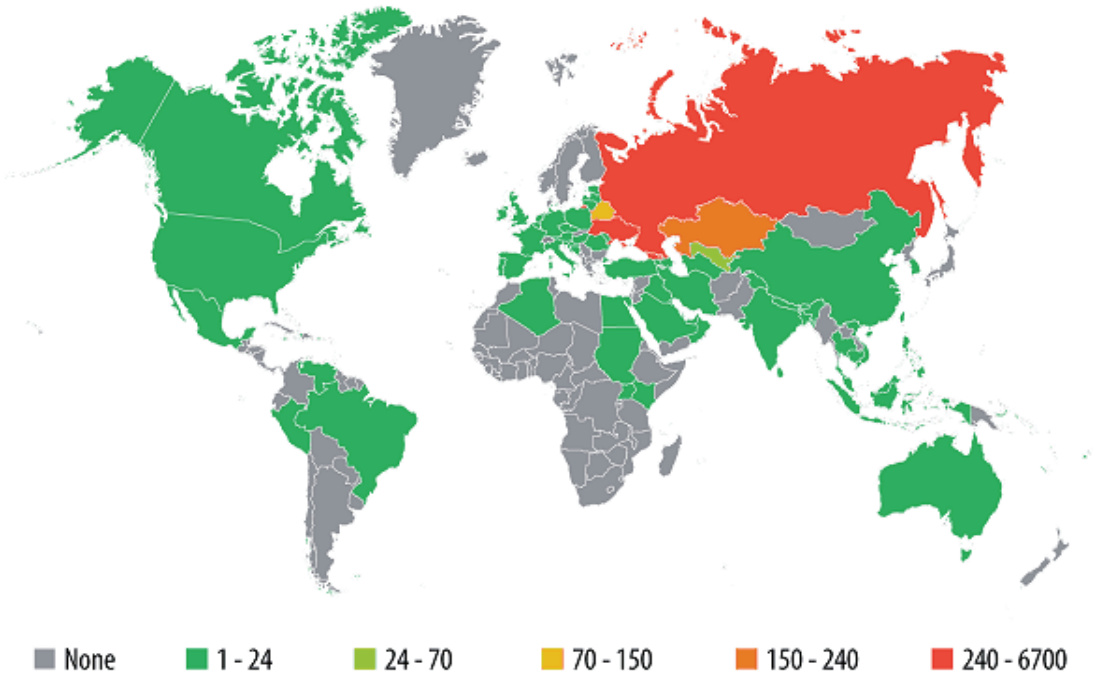
Наиболее совершенные мобильные вредоносные программы на сегодняшний день – троянцы, нацеленные на банковские счета.

Тенденция года: мобильные банкеры

2013 год ознаменовался резким увеличением числа банковских Android-троянцев. Кибериндустрия мобильных вредоносных программ становится все более ориентированной на эффективное извлечение прибыли - мобильный фишинг, кражу информации о кредитных картах, перевод денег с банковских карт на счёт мобильного телефона и оттуда на электронные кошельки злоумышленников. Киберпреступники по-настоящему распробовали этот способ незаконного заработка: если к началу года было известно 67 банковских троянца, то на конец года в нашем распоряжении имелось уже 1321 уникальных образцов. Мобильные продукты «Лаборатории Касперского» предотвратили 2,5 тыс. заражений банковскими троянцами.



Количество банковских мобильных троянцев нашедших место в коллекции ЛК



Карта попыток заражений мобильными банкерами

Мобильные банкеры могут работать в паре с Win-32 троянцами, такие зловреды используются для обхода двухфакторной аутентификации – хищения mTAN (кодов подтверждения банковских операций, которые банки присылают своим клиентам в SMS-сообщениях). Однако в 2013 году получили дальнейшее развитие самостоятельные мобильные банкеры. Пока такие троянцы атакуют клиентов ограниченного числа банков, но можно ожидать, что киберпреступники придумают новые технологии, которые позволят им расширить число и географию потенциальных жертв.

На сегодняшний день большинство банковских троянцев атакует пользователей России и стран СНГ. Однако такая ситуация долго не продлится: учитывая интерес злоумышленников к банковским счетам пользователей, в 2014 году можно ожидать роста активности мобильных банкеров в других странах.

Как уже было сказано выше, среди всех мобильных угроз банковские троянцы, пожалуй, наиболее сложные. Один из ярких примеров - троянец Svpeng.

Этот троянец был обнаружен специалистами ЛК в июле 2013 г. Trojan-SMS.AndroidOS.Svpeng.a, в отличие от своих собратьев Trojan-SMS, ориентирован на хищение денег не с мобильного, а с банковского счета жертвы. Он лишен самостоятельности и действует строго в соответствии с указаниями, получаемыми от C&C-сервера. Распространяется зловред с помощью SMS-спама и со взломанных легитимных сайтов, перенаправляющих мобильных посетителей на вредоносный ресурс. Там пользователю предлагают скачать и установить троянец под видом обновления Adobe Flash Player.

Кстати, потенциальные возможности Svpeng следующие.

Собирает информацию о смартфоне (IMEI, страна, оператор связи, язык операционной системы) и отправляет хозяину посредством HTTP POST-запроса. По всей видимости, это нужно для определения круга банков, которыми может пользоваться жертва. Пока что Svpeng был замечен в атаках на пользователей лишь некоторых российских банков, но ничто не мешает злоумышленникам распространить свою деятельность и на другие страны, обкатав технологию в России.

Крадет SMS-сообщения и информацию о голосовых вызовах. Это также помогает узнать злоумышленнику, клиентом каких банков является владелец смартфона - список номеров банков троянец получает со своего C&C-сервера.

Крадет деньги с банковского счета жертвы. В России некоторые крупные банки предоставляют своим клиентам услугу пополнения счета мобильного телефона переводом денег с банковской карты. Для этого клиенту банка достаточно отправить со своего смартфона SMS определенного содержания на специальный номер банка. Svpeng отправляет SMS-сообщения на адрес SMS-сервисов двух таких банков. Таким способом хозяин Svpeng может узнать, привязаны ли к номеру зараженного смартфона карты этих банков и, если привязаны, получить информацию о балансе счета. После это-

го злоумышленник может дать Svpeng команду на перевод денег с банковского на мобильный счет жертвы. В дальнейшем «слить» деньги с мобильного счета можно разными способами – например, переводом на электронный кошелек через личный кабинет в системе оператора связи, или банальной отправкой сообщений на премиум-номера.

Крадет логин и пароль к системе онлайн-банкинга, подменяя окно банковского приложения. Пока что нам известно лишь про подмену окна в приложениях российских банков, но технические возможности Svpeng позволяют осуществить подмену любых других банковских приложений.

Крадет данные банковской карты (номер, дату окончания действия, CVC2/CVV2) под видом привязки карты к Google Play. При попытке запуска приложения Play Market троянец перехватывает это событие и поверх настоящего окна Google Play показывает свое окно «Добавить карту» на языке системы с предложением ввести данные банковской карточки. Все введенные данные немедленно отправляются злоумышленникам.

Вымогает деньги у пользователей: пугает блокировкой смартфона, показывая сообщение с требованием уплаты $500 за разблокировку. На самом деле троянец ничего не блокирует, телефоном можно пользоваться без проблем.

Скрывает следы своей деятельности, маскируя отправленные и полученные SMS-сообщения, а также блокируя вызовы и сообщения с номеров банка. Список этих номеров троянец также получает со своего C&C-сервера.

Защищает себя от удаления, запрашивая при установке права Device Administrator. В результате в списке приложений кнопка удаления троянца становится неактивной, что может составить проблему для неподготовленного пользователя. Лишить троянец этих прав без применения специализированных средств (таких, как Kaspersky Internet Security для Android) не получится. Для защиты от удаления Svpeng использует уязвимость в Android, которая на момент обнаружения зловреда еще была неизвестна. Тем же способом он пытается помешать восстановить на смартфоне заводские настройки.

Распространен этот троянец в России и странах СНГ. Вместе с тем злоумышленники легко могут нацелить его и на пользователей других стран.

В 2013 году зарубежные пользователи также получили несколько вредоносных новинок, нацеленных на банковские счета. К ним относятся:

Android-троянец Perkele. Он атакует пользователей не только российских, но и некоторых европейских банков. Он представляет интерес прежде всего тем, что орудует в связке с различными банковскими win32-троянцами. Основной его задачей является обход двухфакторной аутентификации клиента в интернет-банке.

В силу специфического предназначения, Perkele распространяется необычным методом. Заразивший ПК жертвы банковский зловред (ZeuS, Citadel) при заходе пользователя на сайт интернет-банкинга внедряет в загружаемый код страницы аутентификации запрос номера смартфона и типа его операционной системы. После ввода вся информация попадает к злоумышленникам, а на экран компьютера выводится QR-код со ссылкой якобы на сертификат интернет-банка. Просканировав QR-код и установив загруженный по ссылке компонент, пользователь заражает свой смартфон троянцем, который обладает весьма интересным для злоумышленников функционалом.

Perkele перехватывает mTAN (коды подтверждения банковских операций), присылаемые банком посредством SMS. Пользуясь похищенными из браузера логином и паролем пользователя, Windows-троянец инициирует поддельную транзакцию, а Perkele перехватывает и сообщает ему (через C&C-сервер) присланный банком mTAN. Деньги жертвы уходят со счета и обналичиваются без каких-либо внешних признаков.

Корейский зловред Wroba, помимо традиционного вектора заражения через файлообменные сервисы, распространяется через альтернативные магазины приложений. После заражения устройства Wroba ведет себя предельно агрессивно. Он ищет установленные приложения мобильного банкинга, удаляет их, и загружает имитирующие их подделки. Внешне они неотличимы от легитимных приложений, но никаких функций обычного банковского приложения у них нет, они лишь похищают вводимые логины и пароли.

TOP 10 мобильных угроз 2013 года

	Название	% от всех атак
1	DangerousObject.Multi.Generic	40,42%
2	Trojan-SMS.AndroidOS.OpFake.bo	21,77%
3	AdWare.AndroidOS.Ganlet.a	12,40%
4	Trojan-SMS.AndroidOS.FakeInst.a	10,37%
5	RiskTool.AndroidOS.SMSreg.cw	8,80%
6	Trojan-SMS.AndroidOS.Agent.u	8,03%
7	Trojan-SMS.AndroidOS.OpFake.a	5,49%
8	Trojan.AndroidOS.Plangton.a	5,37%
9	Trojan.AndroidOS.MTK.a	4,25%
10	AdWare.AndroidOS.Hamob.a	3,39%

Рассмотрим их подробнее.

1. DangerousObject.Multi.Generic. Такой вердикт говорит о том, что детектирование осуществляется нашими облачными технологиями, которые дают возможность нашему продукту быстро реагировать на новые и неизвестные угрозы.

2. Trojan-SMS.AndroidOS.OpFake.bo. Один из представителей сложных SMS-троянцев. Имеет красиво прорисованный интерфейс. Запуск троянца лишает владельца телефона денег - от $9 до всей суммы на счете мобильного оператора. Также есть риск дискредитации телефонного номера, поскольку троянец умеет собирать номера из телефонной книги и отправлять на них произвольные сообщения. Нацелен в основном на русскоязычных пользователей и пользователей стран СНГ.

3. AdWare.AndroidOS.Ganlet.a. Рекламный модуль, который имеет функцию установки других приложений.

4. Trojan-SMS.AndroidOS.FakeInst.a. Троянец эволюционировал на протяжении двух последних лет, из простого отправителя SMS превратившись в полноценный бот, управляемый по различным каналам (в том числе посредством Google Cloud Messaging). Может красть деньги со счета абонента и рассылать сообщения по контакт-листу жертвы.

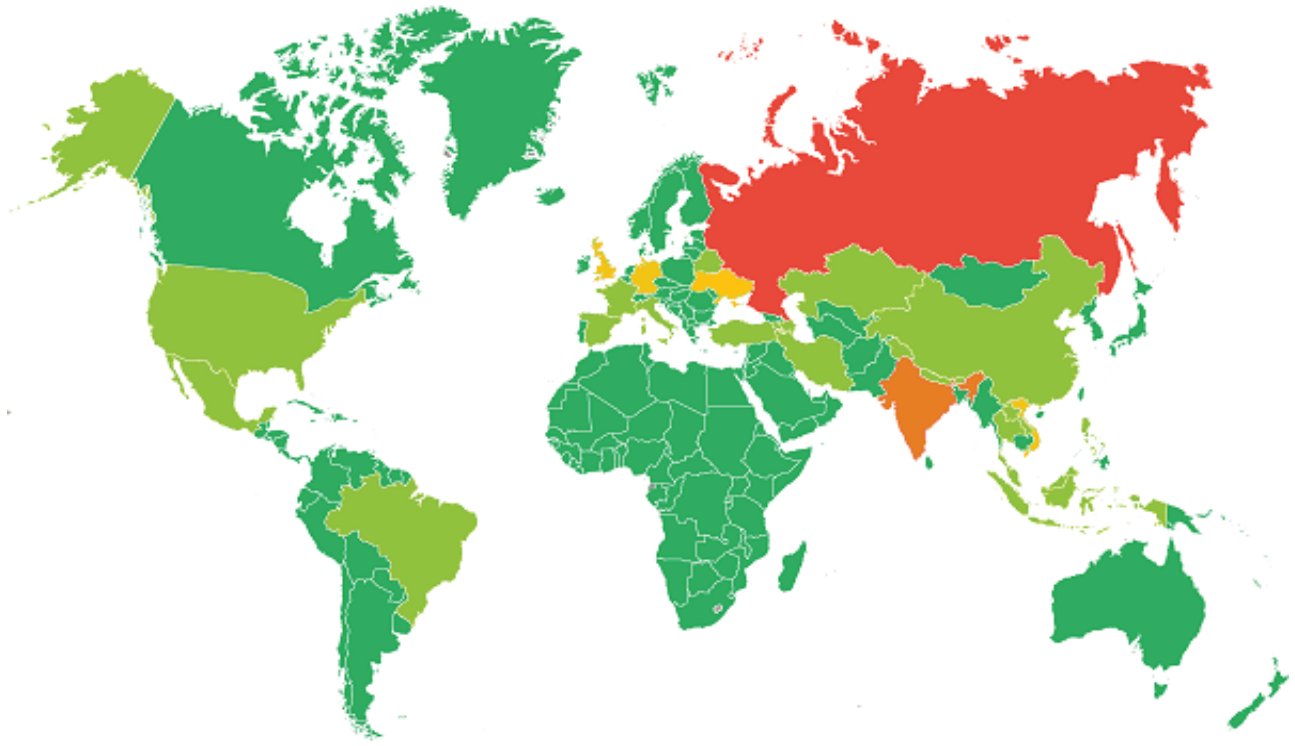
5. RiskTool.AndroidOS.SMSreg.cw. Чрезвычайно распространённый в Китае платёжный модуль, который включен в состав различных игр как модуль осуществления покупок внутри приложения посредством SMS. Удаляет подтверждающие SMS от биллинговой системы без ведома пользователя. Жертва не догадывается о том, что с ее мобильного счета украли деньги, пока не проверит баланс.

6. Trojan-SMS.AndroidOS.Agent.u. Первый троянец, который начал использовать уязвимость в ОС Android для получения прав DEVICE ADMIN и тем самым чрезвычайно усложнял своё удаление. Наряду с этим может сбрасывать входящие звонки и звонить самостоятельно. Возможный ущерб от заражения – отправка ряда SMS на общую сумму от $9.

7. Trojan.AndroidOS.Plangton.a. Рекламный модуль, который без предупреждения передает личную информацию пользователя на сервер рекламодателей, меняя startpage и создавая новые ярлыки в браузере. Ущерб: дискредитация мобильного номера, учетной записи Google и некоторых других данных. К тому же этот троянец без ведома пользователя меняет стартовую страницу браузера и добавляет рекламные закладки.

8. Trojan-SMS.AndroidOS.OpFake.a. Многофункциональный бот, помогает в распространении сложного Android-зловреда Backdoor.AndroidOS.Obad.a. Вместе они образуют связку приложений, крайне опасную для пользователей по причине:

1. широких возможностей: хищение личных данных, отправка SMS на любые номера с



География угроз и карта попыток заражений мобильными зловредами (процент от всех атакованных уникальных пользователей)

заданным текстом. Установка такого приложения может привести к полному опустошению мобильного счета. Риск дискредитации номера, вследствие того что по списку похищенных контактов будут разосланы SMS от имени жертвы. Также контакт-лист будет загружен на сервер злоумышленников.

2. чрезвычайно сложных механизмов самозащиты и противодействия удалению. Благодаря эксплуатации уязвимости в ОС Android этого трояна нельзя удалить без использования специальных программ, таких как KIS для Android.

Следует отметить, что география **Trojan-SMS.AndroidOS.OpFake.a** шире, чем у лидеров списка. Мы очень часто фиксируем попытки заражений им устройств не только в странах СНГ, но и в Европе.

9. Trojan.AndroidOS.MTK.a. Сложный троянец с богатым функционалом и очень сложными методами шифрования. Основная задача — запуск загруженных вредоносных приложений.

10. AdWare.AndroidOS.Hamob.a. Рекламное приложение, которое распространялось под видом легитимных программ (используя название и иконки, например, WinRAR), при этом единственная его функция - показ рекламы.

Как видно, в TOP 10 вошли четыре SMS-троянца, но значительная часть этих троянцев обладает механизмами управления, что превращает зараженные ими устройства в боты.

Топ 10 стран по числу атакованных уникальных пользователей:

	Страна	% от всех атакованных пользователей
1	Россия	40,34%
2	Индия	7,90%
3	Вьетнам	3,96%
4	Украина	3,84%
5	Великобритания	3,42%
6	Германия	3,20%
7	Казахстан	2,88%
8	США	2,13%
9	Малайзия	2,12%
10	Иран	2,01%

В распределении мобильных угроз существует региональная специфика: в разных регионах и странах злоумышленники используют разные категории мобильных зловредов. Рассмотрим ситуацию в нескольких странах из различных регионов мира.

Россия. В России мобильные злоумышленники орудуют особенно активно: 40,3% всех атакованных в 2013 году пользователей находились именно в России.

Топ 5 семейств мобильных зловредов, распространенных в России:

Семейство	% атакованных уникальных пользователей
Trojan-SMS.AndroidOS.OpFake	40,19%
Trojan-SMS.AndroidOS.FakeInst	28,57%
Trojan-SMS.AndroidOS.Agent	27,11%
DangerousObject.Multi.Generic	25,30%
Trojan-SMS.AndroidOS.Stealer	15,98%

Как и год назад, Россия лидирует по количеству попыток заражения SMS-троянцами, и пока нет никаких предпосылок к изменению ситуации. Как мы уже отмечали выше, на российских пользователей нацелено и большинство банковских мобильных троянцев.

Россия и страны СНГ зачастую служат своего рода полигоном для тестирования новых технологий: отработав технологию в Рунете, злоумышленники начинают использовать ее и в атаках на пользователей других стран.

Германия. Германия – одна из западноевропейских стран, где орудуют Trojan-SMS. Российские вирусописатели, разрабатывающие такие троянские программы, в 2013 году были нацелены и на Европу, так как схема монетизации с использованием отправки SMS на премиум-номера применима в этом регионе. Мы фиксировали в Германии активные попытки заражения Trojan-SMS, в частности зловредами семейства Agent.

Кроме того, в этой стране активно используются банковские мобильные троянцы: среди стран Западной Европы Германия занимает первое место по числу уникальных атакованных пользователей (6-е место в мировом рейтинге).

Топ 5 семейств мобильных зловредов, распространенных в Германии:

Семейство	% атакованных уникальных пользователей
RiskTool.AndroidOS.SMSreg	25,88%
DangerousObject.Multi.Generic	20,83%
Trojan-SMS.AndroidOS.Agent	9,25%
Trojan.AndroidOS.MTK	8,58%
AdWare.AndroidOS.Ganlet	5,92%

Топ 5 семейств мобильных зловредов, распространенных в США:

Семейство	% атакованных уникальных пользователей
DangerousObject.Multi.Generic	19,75%
RiskTool.AndroidOS.SMSreg	19,24%
Monitor.AndroidOS.Walien	11,24%
Backdoor.AndroidOS.GinMaster	8,05%
AdWare.AndroidOS.Ganlet	7,29%

Топ 5 семейств мобильных зловредов, распространенных в Китае:

Семейство	% атакованных уникальных пользователей
RiskTool.AndroidOS.SMSreg	46,43%
AdWare.AndroidOS.Dowgin	19,18%
DangerousObject.Multi.Generic	13,89%
Trojan-SMS.AndroidOS.Agent	10,55%
Trojan.AndroidOS.MTK	10,13%

США. В США специфика иная. В этой стране не работают схемы монетизации через SMS, посему нет явного преобладания мобильных зловредов категории Trojan-SMS. В числе лидеров присутствуют боты, собирающие данные о зараженных смартфонах.

Китай. В Китае очень много рекламных модулей, интегрируемых в легальные и даже во вредоносные приложения. Функционал рекламных модулей весьма широк - вплоть до загрузки зловреда на телефон жертвы. Для Китая характеры также SMS-троянцы и бэкдоры.

Заключение

Вредоносное ПО, атакующее банковские счета мобильных пользователей, в настоящее время развивается, и количество его стремительно растет. Очевидно, что эта тенденция продолжится: мобильных банкеров будет все больше, они будут использовать новые технологии противодействия обнаружению, детектированию и удалению.

Среди образцов мобильных зловредов, обнаруженных в 2013 году, преобладают боты. Злоумышленники в полной мере оценили преимущества мобильных ботнетов для получения прибыли. Возможно появление новых механизмов управления мобильными ботнетами.

В Лаборатории Касперского ожидают, что 2014 год станет очень богатым на эксплуатацию разного рода уязвимостей, которые позволят укореняться вредоносному ПО на устройстве и усложнят его удаление.

Кстати, в 2013 году был зафиксирован первый случай атаки на персональные компьютеры (ПК) с мобильного устройства. В будущем не исключается атак с использованием Wi-Fi с мобильных устройств на расположенные вблизи от них рабочие станции и инфраструктуру в целом.

Скорее всего, Trojan-SMS по-прежнему будут в числе лидеров среди всех видов вредоносных программ и смогут завоевывать новые территории.