Kaspersky Security Bulletin

МОБИЛЬНАЯ ВИРУСОЛОГИЯ 2015

Роман Унучек, Виктор Чебышев

ОГЛАВЛЕНИЕ

ЦИФРЫ ГОДА

В 2015 году было обнаружено:

- 2 961 727 вредоносных установочных пакетов;
- 884 774 новых мобильных вредоносных программ – в 3 раза больше, чем в предыдущем году;
- 7 030 мобильных банковских троянцев.

ТЕНДЕНЦИИ ГОДА

- Рост числа вредоносных приложений, которые пользователь самостоятельно удалить не может.
- Активное использование зловредами фишиновых окон для перекрытия легитимных приложений.
- Рост числа программ-вымогателей (RansomWare).
- Использование прав суперпользователя программами для показа агрессивной рекламы.
- Рост числа зловредов для iOS.

Основные способы монетизации

Мобильные вредоносные программы продолжают эволюционировать в сторону монетизации – создатели вредоносного кода разрабатывают его с тем, чтобы получать деньги от своих жертв.

Кража денег с банковских счетов пользователей

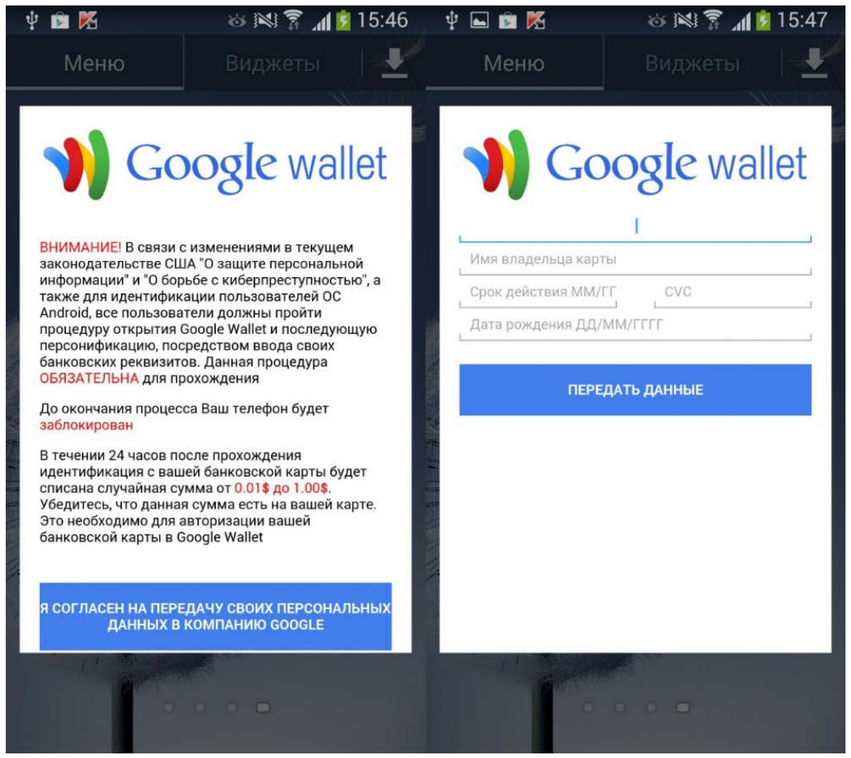
Продолжают развиваться мобильные троянцы, нацеленные на банковские счета пользователей – в 2015 году мы обнаружили 7030 новых мобильных банковских троянцев. Некоторые мобильные вредоносные программы работают в связке с Windows-троянцами и перехватывают пароли mTAN (одноразовые пароли двухфакторной аутентификации), которые служат для авторизации банковских транзакций. Многие мобильные программы, используемые для кражи денег с банковских счетов пользователей, действуют самостоятельно.

Некоторые вредоносные программы на мониторе устройства перекрывают открытое легитимное банковское приложение фишинговым окном, имитирующим это приложение. Самыми примечательными примерами таких программ могут служить троянец Trojan-SMS.AndroidOS.OpFake.cc и представители семейства Trojan-Banker.AndroidOS.Acecard. Одна из модификаций OpFake.cc умеет перекрывать интерфейс более 100 легитимных банковских и финансовых приложений. В свою очередь, семейство мобильных банкеров Acecard перекрывает более 30 банковских приложений, к тому же имеет функционал перекрытия любого приложения по команде от управляющего сервера.

А во втором квартале 2015 г. мы писали о программе Trojan-Spy.AndroidOS.SmsThief.fc, вредоносный код которой был добавлен в легитимное банковское приложение, при этом не влияя на его работу. Как следствие, пользователю самостоятельно обнаружить этот зловред довольно сложно.

Подход создателей мобильных зловредов к краже денег становится более комплексным: дело уже не ограничивается специальными банковскими троянцами, имеющими своей целью банковские приложения.

Пример такого приложения – Trojan-SMS.AndroidOS.FakeInst.ep. Этот зловред показывает пользователю сообщение, якобы от Google, с требованием открыть Google Wallet и ввести данные банковской карты (под предлогом борьбы с киберпреступностью). Окно с этим сообщением нельзя закрыть, пока пользователь не введёт данные банковской карты.



После того, как пользователь ввел требуемые данные, они отправляются злоумышленникам, и окно закрывается. А троянец продолжает воровать информацию и передает своим хозяевам дополнительную информацию о смартфоне и его владельце.

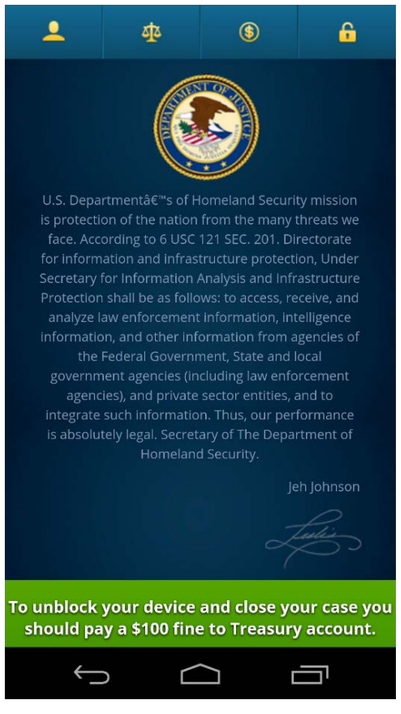
На фоне замедления роста числа специальных банковских троянцев растет общее число приложений, способных красть деньги у пользователей. При этом банковские троянцы становятся все более изощренными и универсальными – зачастую они способны атаковать пользователей десятков банков, расположенных в разных странах мира. Как следствие, злоумышленникам не требуется множество файлов для атак на пользователей разных банков.

Программы-вымогатели (RansomWare)

В 2015 году по сравнению с 2014 годом практически удвоилось количество найденных нами семейств троянцев класса Trojan-Ransom. Количество обнаруженных модификаций за тот же период выросло в 3,5 раза. Это значит, что некоторые злоумышленники переключаются на кражу денег пользователей с помощью троянцев-вымогателей, а те, кто этим уже занимался, продолжают активно создавать новые модификации таких зловредов. Еще одним важным показателем, говорящем про актуальность этого класса угроз, является количество атакованных пользователей: за 2015 год этот показатель вырос более чем в 5 раз.

Чаще всего троянцы, относящиеся к этому типу, блокируют устройство под предлогом якобы противоправных действий пользователя и вымогают деньги за разблокировку – от $12 до $100. Заблокированным устройством невозможно пользоваться – пользователь все время видит только экран, на котором открыто окно с требованием выкупа. Некоторые троянцы умеют перекрывать даже системные диалоги, такие как выключение телефона.

В конце года нам удалось обнаружить несколько троянцев типа Trojan-Downloader, которые в основном загружали в систему троянца-вымогателя Trojan-Ransom.AndroidOS.Pletor. Особенностью этих троянцев-загрузчиков стало то, что они используют уязвимости в системе, чтобы получить права суперпользователя на устройстве и установить Trojan-Ransom в системную папку. После этого установленный троянец практически невозможно удалить.



Окно, которое открывает троянец Fusob

Отправка SMS на премиум-номера и платные подписки

SMS-троянцы остаются актуальной угрозой, особенно в России. Эти программы отправляют с зараженного устройства платные сообщения без ведома пользователя. Хотя их доля в общем потоке мобильных угроз продолжает уменьшаться, число SMS-троянцев в абсолютном выражении остается значительным.

Некоторые SMS-троянцы не ограничиваются отправкой SMS на премиум-номера, они подключают пользователю платные подписки. На протяжении всего 2015 года мы следили за развитием Trojan-SMS.AndroidOS.Podec, который оставался одним из самых популярных у злоумышленников троянцев. Этот зловред обладает достаточно необычным функционалом. Основной способ монетизации для этого троянца – платные подписки. Он имеет возможность обходить Captcha, а в последних модификациях «утратил» способность отправлять SMS, его создатели сконцентрировались на подписках.

Агрессивная реклама

В 2015 году мы зафиксировали увеличение количества программ, которые используют рекламу как основное средство монетизации. Трендом года стали троянцы, использующие права суперпользователя. Если в первом квартале в рейтинге самых популярных мобильных вредоносных программ был всего один такой троянец, то по итогам 2015 года в TOP 20 их уже больше половины. Несмотря на то, что данные троянцы предназначены для загрузки и установки рекламных приложений без ведома пользователя, они могут принести очень много проблем. После установки они пытаются рутовать устройство и установить свои компоненты в систему, так чтобы их потом было очень сложно обезвредить. Некоторые из них не исчезают из смартфона даже после сброса к заводским настройкам. В результате их работы на устройстве пользователь видит большое количество назойливой рекламы. Также они устанавливают на устройство без ведома пользователя много разных программ, в том числе вредоносных. Были зафиксированы случаи, когда подобные программы распространялись в официальных прошивках устройств, а также были предустановлены на новые телефоны.

Вредоносные программы в официальных магазинах

В начале октября 2015 года нам удалось обнаружить несколько троянцев в официальном магазине приложений Google Play Store. Вредоносные программы воровали пароли пользователей российской социальной сети ВКонтакте. Это Trojan-PSW.AndroidOS.MyVk.a и Trojan-PSW.AndroidOS.Vkezo.a. Примерно через месяц мы задетектировали новую модификацию троянца Vkezo, которая также распространялась через Google Play Store. Злоумышленники с завидным упорством публиковали этих троянцев в официальном магазине приложений – в течение нескольких месяцев они были выложены под разными именами 10 раз. Число загрузок многих версий этих троянцев составляло от 100 000 до 500 000. Еще одни троянец, обнаруженный в Google Play Store, – троянец Trojan-Downloader.AndroidOS.Leech, число загрузок которого составило от 100 000 до 500 000.

Зловреды для iOS

Количество обнаруженных в 2015 году вредоносных программ для iOS по сравнению с 2014 годом выросло в 2,1 раза.

Недавнее появление вредоносных приложений в App Store в очередной раз показало, что, вопреки распространенному мнению, операционная система iOS не является неуязвимой для вредоносного ПО. Злоумышленники не взламывали App Store, а разместили в интернете вредоносную версию Apple's Xcode – бесплатного набора инструментов, с помощью которого разработчики создают приложения для iOS.

Apple's Xcode официально распространяется Apple, но неофициально его распространяют и третьи лица. Некоторые китайские разработчики предпочитают загружать подобные средства разработки с местных серверов. Кто-то разместил на стороннем веб-сервере в Китае версию Xcode, содержащую вредоносный код XcodeGhost. В любое приложение, скомпилированное таким Xcode, встраивался вредоносный код.

Вредоносная программа XcodeGhost заразила десятки приложений. Первоначально считалось, что процедуру проверки Apple обошли 39 зараженных приложений, которые и были успешно загружены в App Store. Самое популярное из них – WeChat, бесплатный мессенджер, который установлен у более чем 700 миллионов пользователей. Apple удалила зараженные приложения. Однако взломанная версия Xcode была доступна около шести месяцев, поэтому общее число

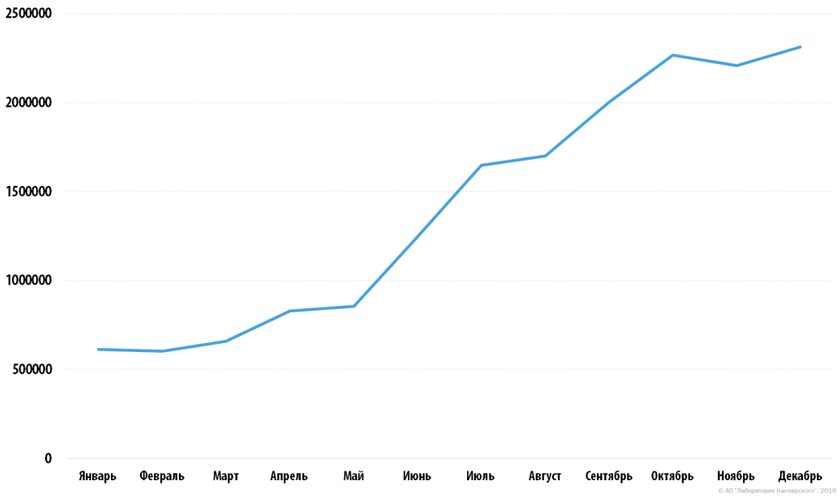
зараженных приложений, возможно, значительно больше – не в последнюю очередь потому, что исходный код XcodeGhost был опубликован на Github.

В начале июня был обнаружен зловред для iPhone – Trojan.IphoneOS.FakeTimer.a. Этот троянец, нацеленный на жителей Японии, может быть установлен на любой iPhone, из-за того, что злоумышленники использовали enterprise сертификат для подписи троянца. Вредоносная программа использует фишинг для кражи денег. Отметим, что уже несколько лет существует аналогичная версия этого троянца для Android – Trojan.AndroidOS.FakeTimer.a.

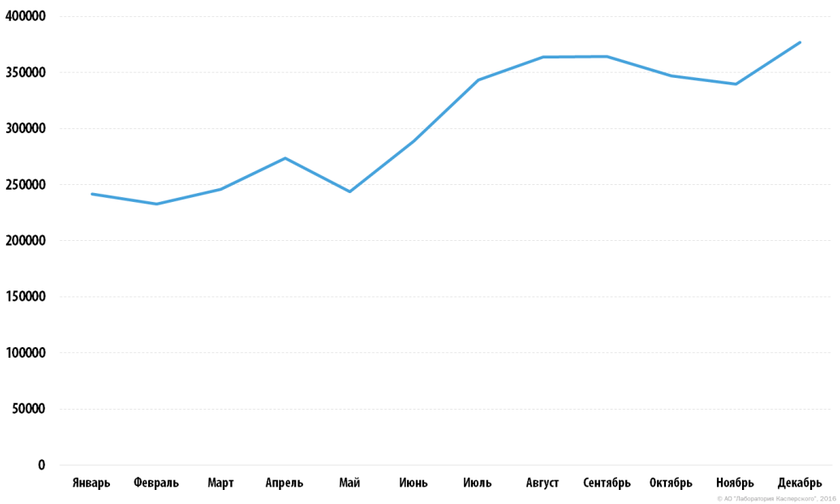
СТАТИСТИКА

В 2015 году продолжился существенный рост количества мобильных вредоносных программ. За 2004-2013 годы мы обнаружили почти 200 000 образцов мобильного вредоносного кода. В 2014 году – 295 539 новых мобильных вредоносных программ. А в 2015 году их число составило уже 884 774. Эти цифры не дают полной картины, поскольку на каждый образец вредоносной программы приходится несколько установочных пакетов: в 2015 году мы зафиксировали 2 961 727 вредоносных инсталляционных пакетов.

Всего в период с начала января 2015 по конец декабря 2015 «Лаборатория Касперского» отразила около 17 миллионов атак вредоносного мобильного ПО, защитив 2 634 967 уникальных пользователей Android-устройств.



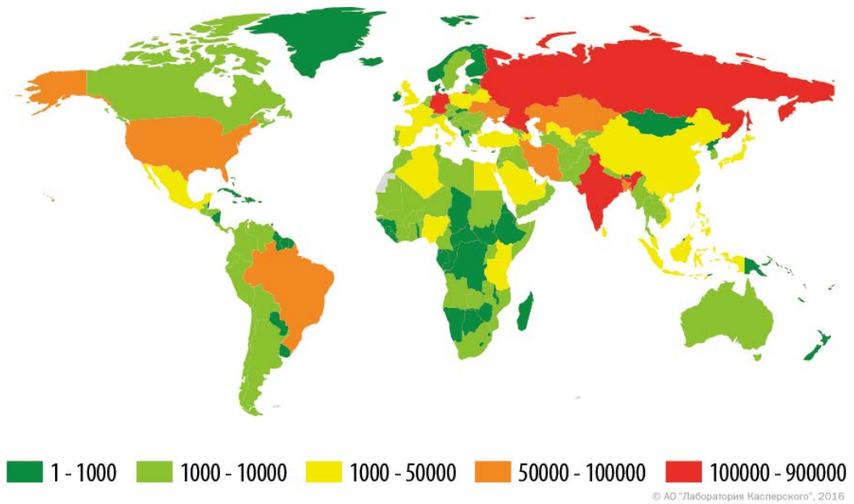
Количество атак, отраженных продуктами «Лаборатории Касперского»



Количество пользователей, защищенных продуктами «Лаборатории Касперского»

География мобильных угроз

Атаки мобильного вредоносного ПО зафиксированы более чем в 200 странах и территориях мира.



География мобильных угроз (количество атакованных пользователей, 2015)

Число зафиксированных атак во многом зависит от числа пользователей в стране. Чтобы оценить опасность заражения мобильными зловредами в разных странах, мы посчитали, какой процент наших пользователей сталкивались с вредоносными приложениями за 2015 год.

TOP 10 стран по проценту пользователей, атакованных мобильными зловредами:

	Страна	% атакованных пользователей*
1	Китай	37%
2	Нигерия	37%
3	Сирия	26%
4	Малайзия	24%
5	Кот-д'Ивуар	23%
6	Вьетнам	22%
7	Иран	21%
8	Россия	21%
9	Индонезия	19%
10	Украина	19%

** Из рейтинга мы исключили страны, где количество активных пользователей мобильного антивируса «Лаборатории Касперского» за отчетный период было менее 25000.*

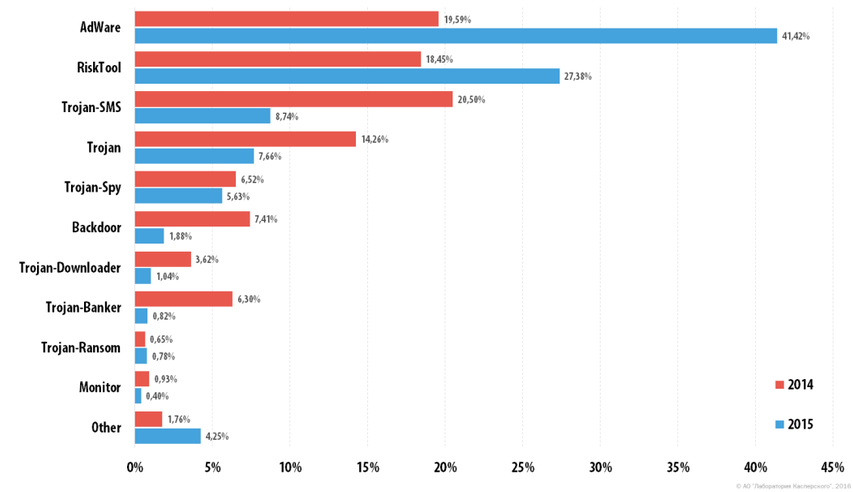
*** Процент уникальных пользователей, атакованных в стране, по отношению ко всем пользователям мобильного антивируса «Лаборатории Касперского» в стране.*

Лидером этого рейтинга стали Китай и Нигерия, где атакам хотя бы раз в течение года подверглись 37% пользователей нашего продукта. Большая часть атак на пользователей в Нигерии осуществляется рекламными троянцами, использующими права суперпользователя, такими как троянцы семейств Ztrorg, Leech, Rootnik и др, а также рекламными программами (AdWare).

В Китае значительную часть атак также составляют рекламные троянцы. Но большинство пользователей сталкивается с семейством RiskTool.AndroidOS.SMSreg. Невнимательное использование этих программ может привести к списанию денег с мобильного счета.

Типы мобильных вредоносных программ

За отчетный период стремительно выросло количество обнаруженных новых файлов AdWare и RiskTool. Как следствие, их доля в общем распределении мобильных угроз по классам также значительно увеличилась – с 19,6% и 18,4% до 41,4% и 27,4% соответственно.



Распределение новых мобильных угроз по типам в 2014 и в 2015 годах

При распространении рекламных программ (AdWare) используются весьма примитивные способы привлечения внимания пользователя к рекламе: создаются приложения с символикой (иконка и название) популярной игры или полезного приложения. Дело в том, что популярных игр и чистых приложений много, поэтому можно генерировать очень много фальшивых приложений с рекламой. Чем больше используется таких фальшивок, тем эффективнее монетизация от кликов. Другим вариантом распространения AdWare является встраивание рекламного модуля в чистое приложение. Это может сделать как сам автор приложения, так и те, кто хочет поживиться на популярности его приложения: когда рекламный модуль добавляется без ведома создателя чистого приложения, прибыль от рекламы получает не автор приложения, а те, кто добавил рекламу. В отличие от фальшивок, в таком комплексном приложении присутствует полезный функционал.

Рост количества программ типа AdWare обеспечивается все увеличивающейся конкуренцией среди их создателей. Легальные программы, которые используют различные рекламные модули, зачастую слишком агрессивны. Все чаще и чаще рекламные модули начинают забрасывать устройство пользователя рекламой, скачивать и инициировать установку различных новых приложений. Иногда

наличие на устройстве программы типа AdWare делает использование этого устройства практически невозможным, так как пользователю постоянно приходится бороться с рекламными окнами.

Программы типа RiskTool чрезвычайно популярны в Китае. Дело в том, что в этой стране весьма востребованы SMS платежи за контент. Поэтому почти любая игра, в которой есть так называемые внутренние покупки (например, дополнительные уровни в игре), содержит модуль оплаты посредством SMS сообщений. В большинстве случаев пользователь уведомлен о возможных рисках, связанных с такими платежами, однако мы считаем необходимым также уведомлять наших пользователей об этих рисках. Исходя из того, что игры довольно популярный контент, число таких приложений довольно велико и постоянно увеличивается. Основной вклад в увеличение количества файлов типа RiskTool внесли программы семейства RiskTool.AndroidOS.SMSReg.

Хотя программы типов AdWare и RiskTool не наносят прямого вреда пользователям, назойливая реклама вызывает раздражение, а программы типа RiskTool, установленные на мобильных устройствах, могут привести к финансовым потерям при их невнимательном использовании и могут использоваться злоумышленниками.

Доля Trojan-SMS в общем потоке мобильных угроз снизилась с 20,5% до 8,7%, практически в 2,4 раза. Однако новых файлов Trojan-SMS в 2015 году было обнаружено даже немного больше, чем в 2014. Активность вредоносных программ этого типа резко снизилось в середине 2014 года. Это стало следствием введения российскими операторами системы AoC (Advice-of-Charge), после чего сократилось количество «партнерских программ», распространявших Trojan-SMS, так как большая часть троянцев этого типа была нацелена на Россию.

TOP 20 мобильных вредоносных программ

В рейтинг вредоносных программ, приведенный ниже, не входят потенциально нежелательные программы, такие как RiskTool и рекламные программы (AdWare).

	Название	% от всех атакованных пользователей*
1	DangerousObject.Multi.Generic	44,2%
2	Trojan-SMS.AndroidOS.Podec.a	11,2%
3	Trojan-Downloader.AndroidOS.Leech.a	8,0%
4	Trojan.AndroidOS.Ztorg.a	7,6%
5	Trojan.AndroidOS.Rootnik.d	6,9%
6	Exploit.AndroidOS.Lotoor.be	6,1%
7	Trojan-SMS.AndroidOS.OpFake.a	5,6%
8	Trojan-Spy.AndroidOS.Agent.el	4,0%
9	Trojan.AndroidOS.Guerrilla.a	3,7%
10	Trojan.AndroidOS.Mobtes.b	3,6%
11	Trojan-Dropper.AndroidOS.Gorpo.a	3,6%
12	Trojan.AndroidOS.Rootnik.a	3,5%
13	Trojan.AndroidOS.Fadeb.a	3,2%
14	Trojan.AndroidOS.Ztorg.pac	2,8%
15	Backdoor.AndroidOS.Obad.f	2,7%
16	Backdoor.AndroidOS.Ztorg.c	2,2%
17	Exploit.AndroidOS.Lotoor.a	2,2%
18	Backdoor.AndroidOS.Ztorg.a	2,0%
19	Trojan-Ransom.AndroidOS.Small.o	1,9%
20	Trojan.AndroidOS.Guerrilla.b	1,8%

** Процент пользователей, атакованных данным зловредом, от всех атакованных пользователей.*

Первое место занимает вердикт DangerousObject.Multi.Generic (44,2%), используемый для вредоносных программ, обнаруженных с помощью облачных технологий. Эти технологии работают, когда в антивирусных базах еще нет ни сигнатуры, ни эвристики для детектирования вредоносной программы, но в облаке антивирусной компании уже есть информация об объекте. По сути, так детектируются самые новые вредоносные программы.

Trojan-SMS.AndroidOS.Stealer.a, занимавший в 2014 году первое место в TOP 20, в 2015 году оказался лишь на 28-м месте.

4 места из TOP 20 занимают троянцы, основным средством монетизации которых является опустошение мобильного счета или кража денег с банковских аккаунтов жертвы. К ним относятся Trojan-SMS.AndroidOS.Podec.a, Trojan-SMS.AndroidOS.OpFake.a, Trojan.AndroidOS.Mobtes.b и Backdoor.AndroidOS.Obad.f. Trojan-SMS.AndroidOS.Podec.a занял второе место в рейтинге (11,2%). Этот троянец входил в TOP3 мобильных угроз на протяжении всего 2015 года. Напомним, что последние версии этого троянца не отправляют платные SMS. Теперь этот зловред подписывает пользователя на платные подписки, используя для этого распознавание CAPTCHA. Trojan-SMS.AndroidOS.OpFake.a (5,6%) – на 7-м месте, это долгожитель рейтингов, он был на 8-м месте в аналогичном рейтинге прошлого года и не покидал TOP 20 на протяжении всего 2015 года.

Еще один троянец – Trojan-Ransom.AndroidOS.Small.o (1,9%) – блокирует телефон жертвы и вымогает деньги за разблокировку. Этот самый популярный на конец 2015 года мобильный Trojan-Ransom,

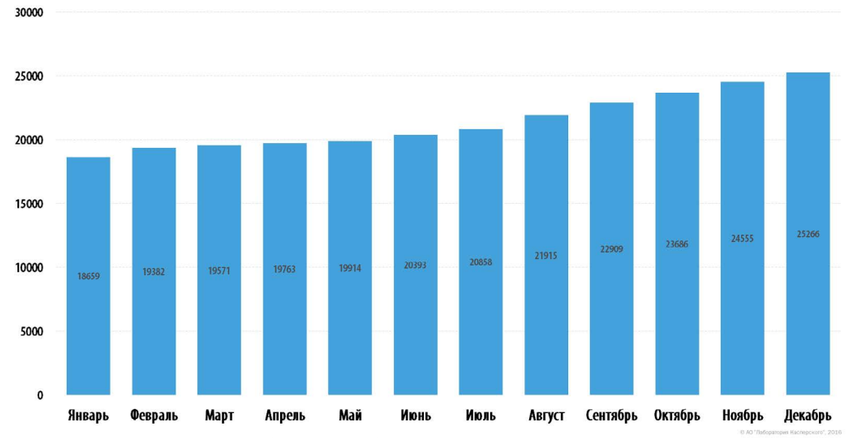
единственный из программ-вымогателей попал в TOP 20. Впервые он появился в рейтинге в третьем квартале 2015 года, заняв 11-ю строчку. По итогам года он оказался на 19-м месте. Распространяется троянец в основном под видом порно видеоплеера и нацелен на русскоязычную аудиторию.

Более половины мест, 12 из 20, занимают троянцы, основной способ монетизации которых – агрессивная реклама. Это Trojan-Downloader.AndroidOS.Leech.a, Trojan-Spy.AndroidOS.Agent.el, Trojan-Dropper.AndroidOS.Gorpo.a, Trojan.AndroidOS.Fadeb.a, по две модификации Trojan.AndroidOS.Guerrilla, Trojan.AndroidOS.Rootnik, Trojan.AndroidOS.Ztorg и Backdoor.AndroidOS.Ztorg. В отличие от обычных рекламных модулей эти программы не несут никакого полезного функционала. Их цель – доставить пользователю как можно больше рекламы различными способами, в том числе за счет установки новых рекламных программ. Эти троянцы могут воспользоваться правами суперпользователя для того, чтобы скрыться в системной папке, откуда удалить их будет очень сложно. Подобные троянцы встречались и раньше, в основном в Китае. В этом году мы наблюдаем настоящий бум таких программ: в большинстве своем это нацеленные на китайских пользователей троянцы, которые стали активно распространяться по всему миру. В коде троянцев часто встречается слово oversea.

Еще две строчки в рейтинге заняли модификации Exploit.AndroidOS.Lotoor. Это эксплойты, применяемые для получения локальных прав суперпользователя.

Мобильные банковские троянцы

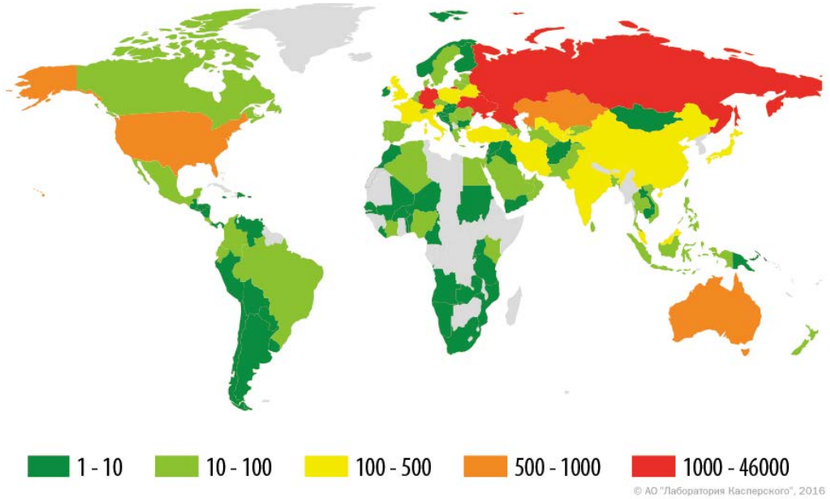
За отчетный период мы обнаружили 7 030 мобильных банковских троянцев – в 2,6 раз меньше, чем в 2014 году, когда с января по декабрь включительно было обнаружено 16 586 мобильных банковских троянцев. Отметим, что, хотя количество обнаруженных новых мобильных банковских троянцев уменьшилось по сравнению с 2014 годом, эти программы стали более умелыми и «злыми», а в сферу интересов злоумышленников попали банки из многих стран мира. Многие мобильные банковские троянцы действуют самостоятельно, без компьютерного компонента, и нацелены на пользователей десятков банков в разных странах мира.



Количество мобильных банковских троянцев в коллекции «Лаборатории Касперского» (2015 год)

Мобильными банковскими троянцами хотя бы раз в течение года были атакованы 56 194 пользователя.

География мобильных банкеров



География мобильных банковских угроз (количество атакованных пользователей, 2015)

TOP 10 стран, атакуемых банковскими троянцами, по количеству атакованных пользователей

	Страна	Количество атакованных пользователей
1	Россия	45690
2	Германия	1532
3	Украина	1206
4	США	967
5	Казахстан	804
6	Австралия	614
7	Республика Корея	527
8	Франция	404
9	Белоруссия	380
10	Польша	324

Россия, как и в прошлом году, занимает первое место в этом рейтинге. В TOP 10 в 2015 году вошли новые страны: Республика Корея, Австралия, Франция и Польша. Покинули первую десятку атакуемых стран Литва, Азербайджан, Болгария и Узбекистан.

Популярность банковских троянцев у злоумышленников в каждой стране можно оценить по проценту пользователей, атакованных мобильными банкерами, от всех атакованных мобильными зловредами пользователей.

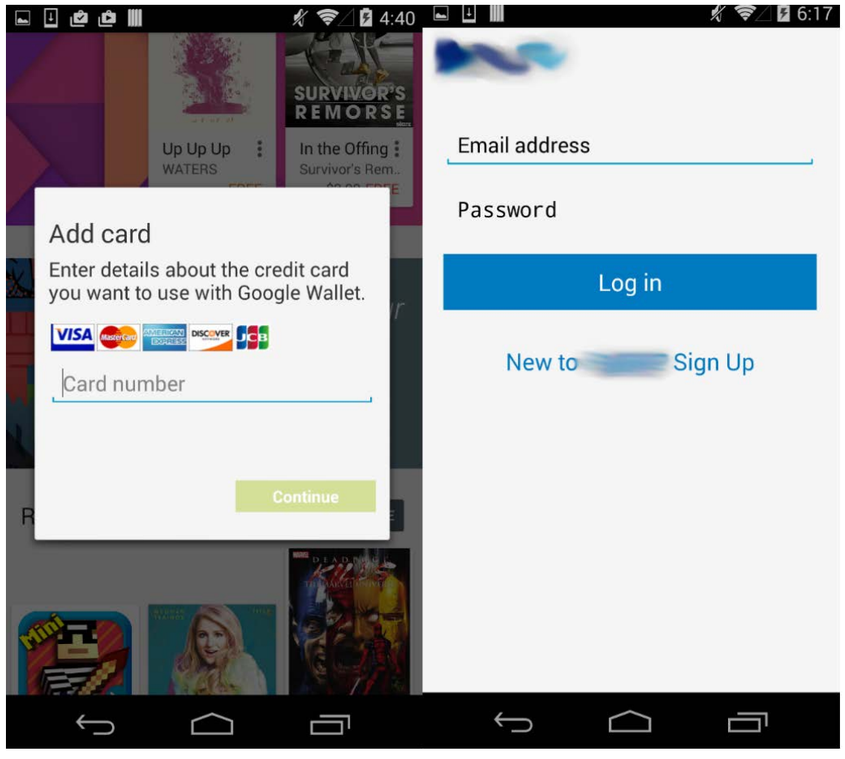
TOP 10 стран по доле пользователей, атакованных мобильными банкерами, среди всех атакованных пользователей

	Страна	% от всех атакованных пользователей*
1	Республика Корея	13,8%
2	Австралия	8,9%
3	Россия	5,1%
4	Австрия	3,0%
5	Белоруссия	1,9%
6	США	1,8%
7	Таджикистан	1,7%
8	Украина	1,6%
9	Франция	1,6%
10	Узбекистан	1,6%

** Процент пользователей, атакованных банковскими троянцами, от всех атакованных в стране пользователей мобильных продуктов «Лаборатории Касперского».*

Значительная часть атак мобильными банкерами в Корее приходится на троянцев семейства Trojan-Banker.AndroidOS.Wroba. Эти троянцы нацелены на кражу аккаунтов мобильного банка крупнейших корейских банков, а также на кражу mTan.

В Австралии первое место по попыткам заражений занимает семейство Trojan-Banker.AndroidOS.Acecard. Это семейство – новый этап развития Backdoor.AndroidOS.Torec.a – первого Android-троянца, использовавшего TOR, которого мы обнаружили еще в начале 2014 года. Первые же банковские модификации этого зловреда относятся к середине 2014 года. Тогда этот троянец распространялся в основном в России, и только в 2015 году стал активно распространяться в Австралии. Одна из обнаруженных нами модификаций этого троянца, относящаяся к ноябрю 2015 года, умеет перекрывать фишинговым окном интерфейс 24-х банковских приложений. Пять приложений относятся к австралийским банкам, по четыре - к гонконгским, австрийским и новозеландским, по три приложения пришлось на немецкие и сингапурские банки и еще одно приложение PayPal. Кроме того, существую модификации, нацеленные на американские и российские банки.



Фишинговые окна троянца Acecard

Отметим, что функционал кражи логина и пароля с использованием перекрывания оригинальных приложений фишинговым окном не нов. Впервые мы этот функционал встретили в троянце Trojan-SMS.AndroidOS.Svpeng еще в 2013 году. В отчете за первый квартал 2015 года мы упоминали троянец Trojan-SMS.AndroidOS.OpFake.cc, который был способен атаковать как минимум 29 банковских и финансовых приложений. Самая последняя версия этого троянца способна атаковать уже **114** банковских и финансовых приложений. Его основная цель – украсть логин и пароль к банковскому аккаунту. Он также перекрывает окна и нескольких популярных почтовых приложений.

В России, занимающей третье место в этом рейтинге, самыми популярными у злоумышленников были Trojan-Banker.AndroidOS.Faketoken и Trojan-Banker.AndroidOS.Marcher. Начиная с апреля, мы наблюдали резкое падение количества попыток заражения пользователей представителями семейства Trojan-Banker.AndroidOS.Marcher. За 5 месяцев с апреля по август количество атак этим троянцем упало в 5 раз. Возможно, в этот период злоумышленники готовились к атакам на пользователей других стран: до сентября 2015 года это семейство распространялось практически только в России. Начиная же с сентября, около 30% атак этим троянцем приходятся на Австралию, Германию и Францию.

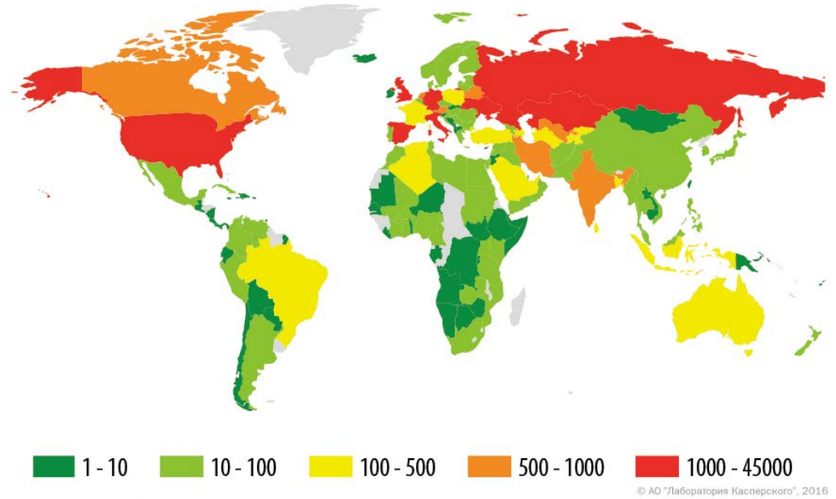
Упомянутый выше Trojan-Spy.AndroidOS.SmsThief.fc распространялся в России. Злоумышленники добавили свой код в оригинальное банковское приложение, не нарушив его работоспособность, в результате этого троянца было сложнее обнаружить.

Мобильные Trojan-Ransom

В 2015 году по сравнению с 2014 годом практически удвоилось количество найденных нами семейств троянцев класса Trojan-Ransom. Количество обнаруженных модификаций за тот же период выросло в 3,5 раза и составило 6924.

За отчетный период мобильные программы-вымогатели атаковали 94 344 уникальных пользователей, что в 5 раза больше, чем в прошлом году (18 478). Доля же уникальных пользователей, атакованных Trojan-Ransom, среди всех пользователей, атакованных мобильными зловредами, за год выросла с 1,1% до 3,8%.

Атаки мобильных программ вымогателей хотя бы раз в течение года были зафиксированы в 156 странах и территориях мира.



География мобильных программ-вымогателей (количество атакованных пользователей, 2015)

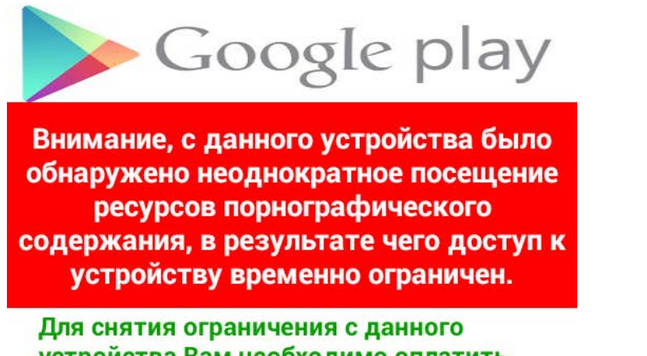
TOP 10 стран по числу пользователей, атакованных Trojan-Ransom

	Страна	Количество атакованных пользователей
1	Россия	44951
2	Германия	15950
3	Казахстан	8374
4	США	5371
5	Украина	4250
6	Великобритания	2878
7	Италия	1313
8	Испания	1062
9	Иран	866
10	Индия	757

Самыми атакуемыми программами-вымогателями странами являются Россия, Германия и Казахстан.

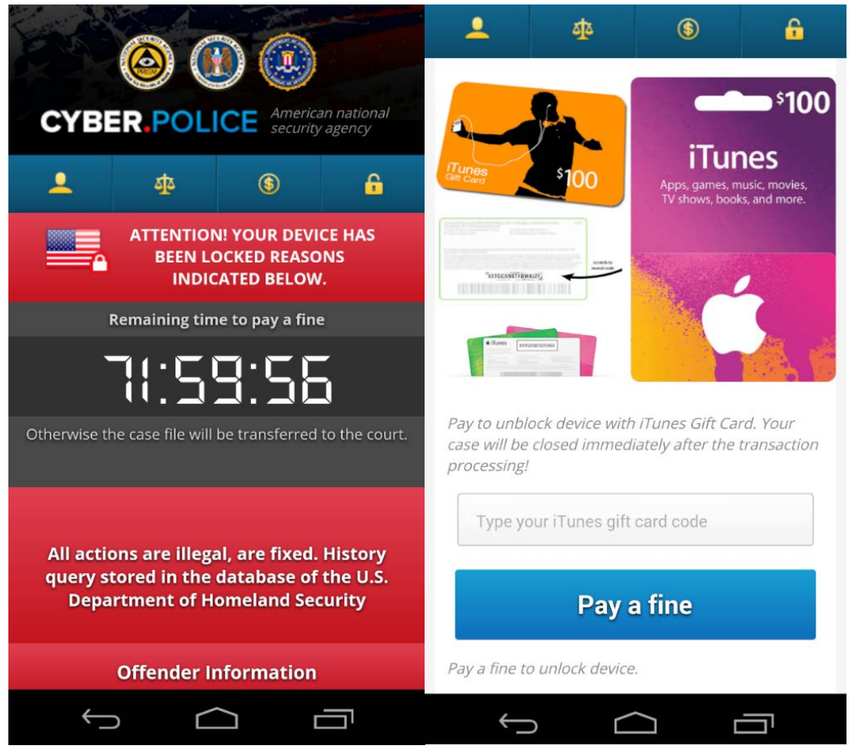
В России и Казахстане активнее всего распространяется семейство Trojan-Ransom.AndroidOS.Small, в частности модификация Trojan-Ransom.AndroidOS.Small.o, являющаяся самой популярной в 2015 году среди всех Trojan-Ransom.

Также на протяжении всего 2015 года оставалось популярным семейство Trojan-Ransom.AndroidOS.Pletor – первый мобильный шифровальщик. Интересно то, что он был создан той же группой злоумышленников, что и Trojan-Banker.AndroidOS.Acecard.



Окно, которое открывает Trojan-Ransom.AndroidOS.Small.o

В Германии же активнее всего распространяется семейство Trojan-Ransom.AndroidOS.Fusob.



Окна, которые открывает троянец Fusob

США заняли 4-е место в рейтинге. В этой стране наиболее активно используется семейство Trojan-Ransom.AndroidOS.Fusob, но также достаточно много атак приходится на семейство Trojan-Ransom.AndroidOS.Svpeng.

Во многом этот рейтинг зависит от количества пользователей в каждой стране, поэтому интересно посмотреть другой рейтинг по доле пользователей, атакованных Trojan-Ransom, среди всех атакованных пользователей в стране.

TOP 10 стран по доле пользователей, атакованных Trojan-Ransom, среди всех атакованных пользователей

	Страна	% от всех атакованных пользователей*
1	Казахстан	15,1%
2	Германия	14,5%
3	США	10,3%
4	Канада	8,9%
5	Нидерланды	8,8%
6	Великобритания	8,3%
7	Швейцария	6,9%
8	Австрия	6,4%
9	Украина	5,9%
10	Австралия	5,5%

** Процент пользователей, атакованных Trojan-Ransom, от всех атакованных в стране пользователей мобильных продуктов «Лаборатории Касперского»*

В этом списке уже отсутствует Россия, на которую приходится наибольшее количество атакованных пользователей. Первые места в нем занимают Казахстан, Германия и США.

ЗАКЛЮЧЕНИЕ

Несмотря на то, что первые рекламные троянцы, использующие права суперпользователя для своих целей, появились несколько лет назад, именно в 2015 году их стало очень много, и распространяются они весьма активно. Если еще в первом квартале 2015 года в топе угроз был только один такой троянец, то по итогам года такие программы составили больше половины TOP 20. Распространяются они всеми доступными способами – через другие рекламные программы, через магазины приложений, они встречаются даже предустановленными в некоторых устройствах. Скорее всего, в 2016 году количество рекламных троянцев, использующих права суперпользователя, продолжит расти.

Мы уже фиксировали случаи, когда такие рекламные троянцы использовались для распространения вредоносных мобильных программ. Есть все основания предполагать, что злоумышленники будут все активнее использовать рекламных троянцев для заражения мобильных устройств пользователей вредоносными программами.

Отметим также, что мы встречали случаи использования прав суперпользователя и другими типами вредоносных программ, в первую очередь Trojan-Ransom.

В 2016 году троянцы типа Trojan-Ransom с высокой долей вероятности продолжат свое развитие. Мы ожидаем рост популярности у злоумышленников троянцев-вымогателей и расширение их географии.

Еще один тип троянцев, за которыми мы продолжим внимательно наблюдать в 2016 году, – Trojan-Banker. Уже существует большое количество банковских троянцев, которым не требуется программа-компаньон на компьютере жертвы. Такие троянцы действуют самостоятельно, и им для осуществления кражи денег пользователя достаточно заразить телефон. Эти троянцы умеют воровать логин и пароль к мобильному банкингу, перекрывая интерфейс легитимных банковских приложений фишинговым окном. Они умеют воровать данные кредитной карты пользователя, используя фишинговые окна. Кроме того, у них достаточно возможностей, чтобы перехватывать коммуникации банка с клиентом – они могут воровать входящие SMS и перенаправлять злоумышленнику вызовы. В 2016 году банковские троянцы станут атаковать еще больше банковских организаций, будут использоваться новые векторы распространения и новые технологии кражи данных.

По мере развития возможностей мобильных устройств и мобильных сервисов, растут и аппетиты злоумышленников, наживающихся на мобильных вредоносных программах. Вирусописатели продолжат совершенствовать свои творения, создавать новые технологии и искать новые способы распространения мобильных зловредов. Их главный интерес – деньги пользователей. И пренебрегать защитой мобильных устройств в таких условиях весьма рискованно.

О «ЛАБОРАТОРИИ КАСПЕРСКОГО»

«Лаборатория Касперского» – крупнейшая в мире частная компания, работающая в сфере информационной безопасности, и один из наиболее быстро развивающихся вендоров защитных решений. Компания входит в четверку ведущих мировых производителей решений для обеспечения IT-безопасности пользователей конечных устройств (IDC, 2014). С 1997 года «Лаборатория Касперского» создает инновационные и эффективные защитные решения и сервисы для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей. «Лаборатория Касперского» – международная компания, работающая почти в 200 странах и территориях мира; ее технологии защищают более 400 миллионов пользователей по всему миру. Более подробная информация доступна на сайте www.kaspersky.ru.

Securelist, ресурс экспертов «Лаборатории Касперского» с актуальной информацией о киберугрозах

Сайт «Лаборатории Касперского»

B2B блог «Лаборатории Касперского»

Блог Евгения Касперского

B2C блог «Лаборатории Касперского»

Новостная служба «Лаборатории Касперского»

Блог Kaspersky Academy

Москва, 125212

Ленинградское шоссе, д.39А, стр.3

БЦ «Олимпия Парк»

Телефон: +7-495-797-8700

+7-495-737-3412