KASPERSKY SECURITY BULLETIN 2013

Гарнаева Мария Александровна,
Кристиан Функ

Данный отчет сформирован на основе данных, полученных и обработанных при помощи Kaspersky Security Network. KSN использует «облачную» архитектуру в персональных и корпоративных продуктах и является одной из важнейших технологий «Лаборатории Касперского». Статистика в отчете основана на данных, полученных от продуктов «Лаборатории Касперского», пользователи которых подтвердили свое согласие на передачу статистических данных.

Цифры года

- По данным KSN, в 2013 году продукты «Лаборатории Касперского» заблокировали **5 188 740 554** вредоносных атак на компьютерах и мобильных устройствах пользователей.
- Обнаружено **104 427** новых модификаций вредоносных программ для мобильных устройств.
- Решения «Лаборатории Касперского» отразили **1 700 870 654** атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира.
- Антивирусные решения обнаружили почти **3 миллиарда** вирусных атак на компьютерах пользователей. Всего в данных инцидентах было зафиксировано **1,8 млн.** вредоносных и потенциально нежелательных программ.
- 45% веб-атак, заблокированных продуктами ЛК, проводились с использованием вредоносных веб-ресурсов, расположенных в США и России.

Мобильные угрозы

В прошлом году проблема безопасности мобильных устройств проявлялась очень остро. Это связано и с количественным, и с качественным ростом мобильных угроз. Мир мобильных зловредов становится все более похожим на мир угроз для персональных компьютеров, а скорость развития этой сферы настораживает.

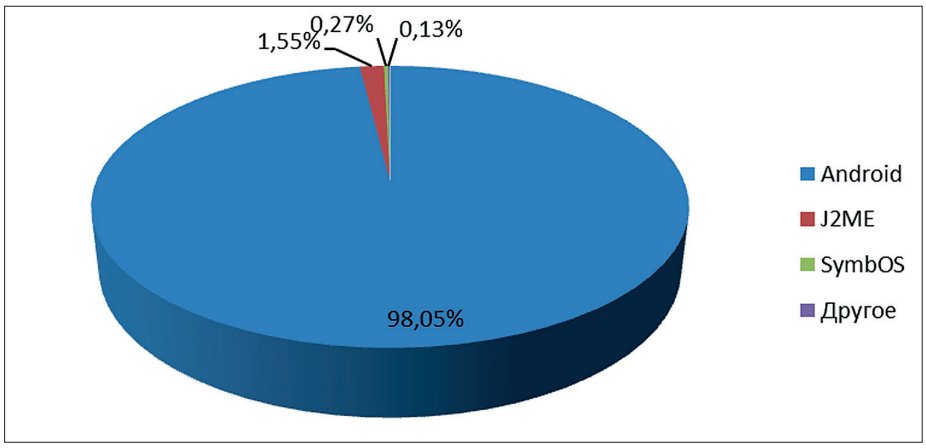
Мобильные ботнеты стали активно использоваться киберпреступниками для обогащения. На поверку оказывается, что мобильные ботнеты имеют значительные преимущества по сравнению с традиционными. Мобильный ботнет более стабильный: смартфоны редко отключаются, поэтому почти все его узлы всегда доступны и готовы выполнять новые инструкции. Наиболее распространенные задачи, выполняемые с помощью традиционных ботнетов, — это массовая рассылка спама, проведение DDoS-атак и массовое отслеживание личной информации пользователей. Все эти задачи легко реализуемы на смартфонах.

Значимые события в 2013 г.

1. Мобильные банковские троянцы. К ним относится мобильный фишинг, кража информации о кредитных картах, проверка баланса банковского счёта жертвы, перевод денег с банковских карт на счёт мобильного телефона, а оттуда – в кошелек QIWI.
2. Мобильные ботнеты. По нашим оценкам, около 60% мобильных вредоносных программ представляют собой элементы больших и малых мобильных ботнетов.
3. Backdoor.AndroidOS.Obad. Этот зловред, пожалуй, самый универсальный из всех, зарегистрированных. Он включает три эксплойта, бэкдор, SMS-троянец, предоставляет функциональные возможности бота и другие. Это, по сути, швейцарский армейский нож, оснащенный разнообразными инструментами. Троянец распространяется разными способами, в том числе через уже существующий мобильный ботнет - со смартфонов, зараженных троянцем Opfake.
4. Контроль ботнетов через Google Cloud Messaging (GCM). Выполнение команд, получаемых через GCM, невозможно заблокировать непосредственно на зараженном устройстве.
5. APT-атаки против уйгурских активистов. В арсенал злоумышленников добавлены вредоносные APK-файлы, отслеживающие личную информацию, хранящуюся на устройстве-жертве, а также передающие данные о его местонахождении.
6. Эксплойты, направленные на Android.
7. Атака на ПК при помощи Android-устройства.

Статистика

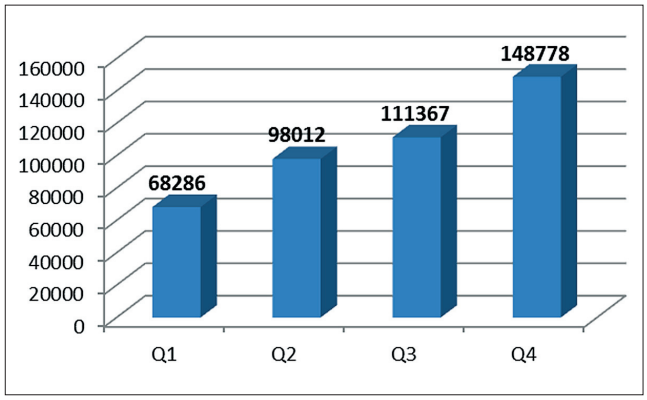
Android по-прежнему остаётся основной целью для вредоносных атак. Причиной тому – ведущие позиции Android на рынке, преобладание сторонних магазинов приложений и в значительной степени открытая архитектура этой платформы, благодаря чему для нее легко создавать вредоносные программы. Мы не думаем, что эта тенденция в ближайшем будущем изменится.



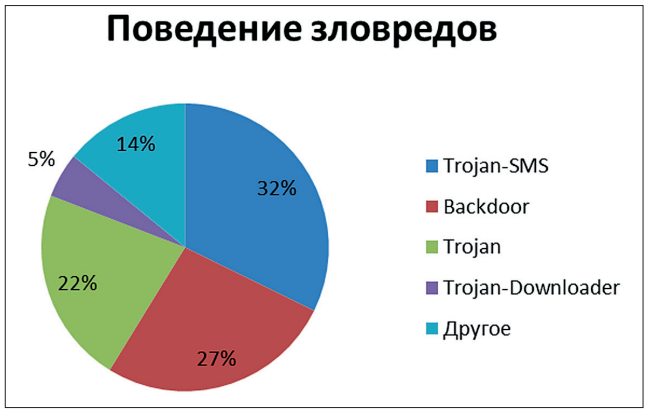
Распределение мобильных вредоносных программ по платформам

На сегодняшний день нам удалось собрать 8 260 509 уникальных вредоносных установочных пакетов. Отметим, что разные установочные пакеты могут устанавливать программы с одним и тем же функционалом, разница может заключаться лишь в интерфейсе вредоносного приложения и, например, содержимом отправляемых им SMS.

Общее число образцов мобильных зловредов в нашей коллекции составляет 148 778, из них 104 427 обнаружены в 2013 году. Тенденция к интенсивному росту количества мобильных вредоносных программ очевидна:



Количество образцов в нашей коллекции



Распределение мобильных вредоносных программ по поведениям

Среди мобильных зловредов по-прежнему лидируют SMS-троянцы. Однако почти все зловреды этой категории эволюционировали в ботов, поэтому можно смело объединить двух лидеров диаграммы в одну категорию — Backdoor. Таким образом, 59% вредоносных приложений являются элементами мобильных ботнетов.

Выводы

1) Все техники и механизмы инфицирования, сокрытия деятельности вредоносных программ очень быстро перебираются с PC на платформу Android. Этому способствует ее открытость и популярность.

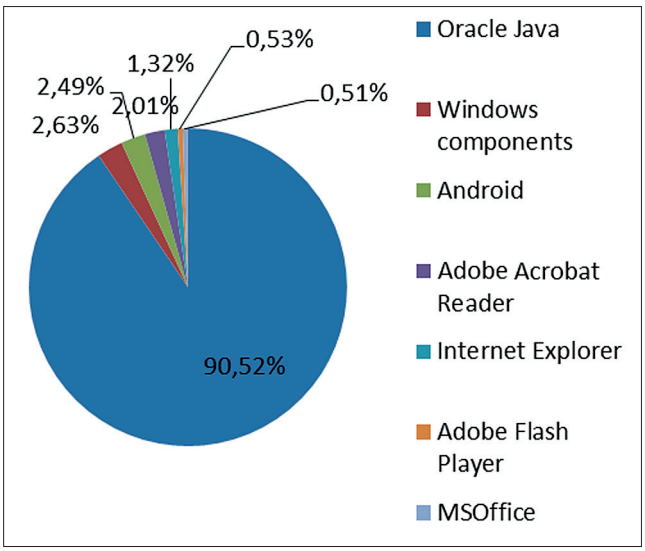
2) Большинство мобильных вредоносных приложений ориентировано на кражу денег и только во вторую очередь на кражу личной информации.

3) Большинство мобильных вредоносных приложений представляют собой ботов с богатым функционалом. В ближайшее время начнется торговля мобильными ботнетами.

4) Явно прослеживается «банковская» направленность развития мобильных зловредов. Вирусописатели следят за развитием сервисов мобильного банкинга. При успешном инфицировании смартфона зловред сразу проверяет, привязан ли телефон к банковской карте.

Уязвимые приложения, используемые злоумышленниками

Рейтинг уязвимых приложений, приведенный ниже, построен на основе данных о заблокированных нашими продуктами эксплойтах, используемых злоумышленниками как в атаках через интернет, так и при компрометации локальных приложений, в том числе на мобильных устройствах пользователей.



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений

Уязвимости в Oracle Java эксплуатируются в ходе drive-by атак через интернет, и новые Java-эксплойты входят в состав множества эксплоит-паков.

Уязвимости в Android используют злоумышленники (а иногда и сами пользователи), чтобы получить root-привилегии, которые дают практически неограниченные возможности для манипуляций над системой.

Вредоносные программы в интернете

Количество атак с интернет-ресурсов, размещенных в разных странах мира, за год увеличилось с 1 595 587 670 до **1 700 870 654**. Таким образом, наши продукты защищали пользователей при серфинге в интернете в среднем 4 659 920 раз в день.

Drive-by атаки с использованием эксплойтов дают злоумышленникам практически гарантированную возможность заражения компьютеров, если на них не установлена защита и имеется хотя бы одно популярное и уязвимое (не обновленное) приложение.

> Drive-by атаки — самый популярный способ проникновения вредоносных программ через интернет.

Из всех вредоносных программ, участвовавших в интернет-атаках на компьютеры пользователей, на 20 наиболее активных пришлось 99,9% всех атак.

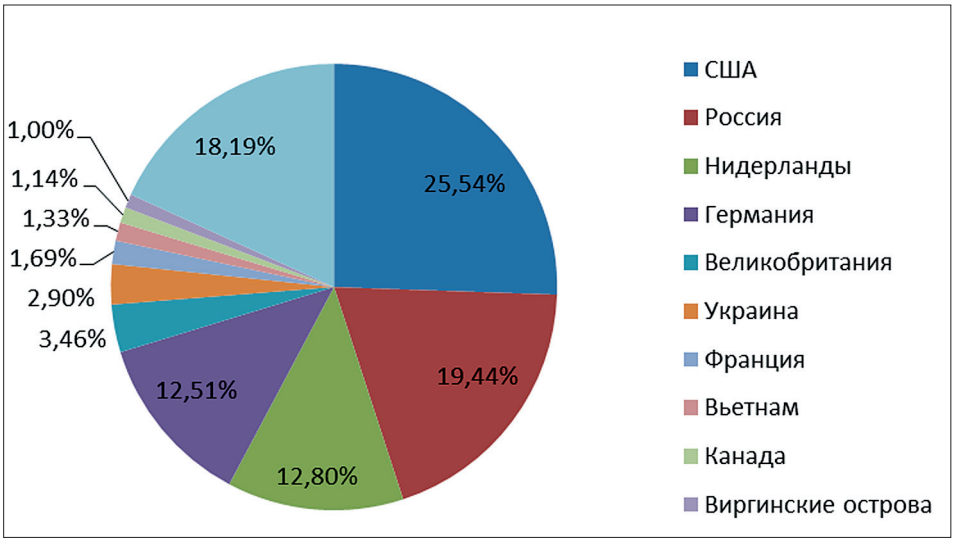
93% вердиктов веб-антивируса из TOP 20 связанно с блокированием ссылок на вредоносные сайты. Значительная часть таких детектов приходится на сайты с эксплойтами и на сайты, перенаправляющие на эксплойты.

> В 2013 году в мире 41,6% компьютеров пользователей интернета хотя бы раз подвергались веб-атаке.

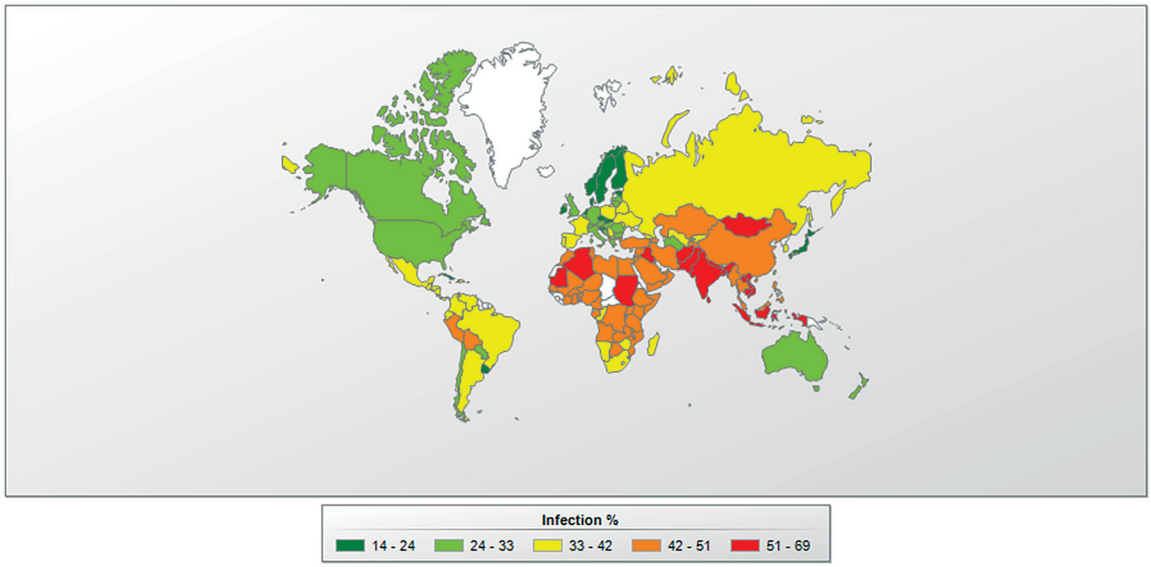
Вердикты, которые присваиваются зловредам, используемым в drive-by атаках, заняли еще 7 из 20 мест в нашем рейтинге.

Страны - источники веб-атак

Для проведения **1 700 870 654** атак через интернет злоумышленники воспользовались 10 604 273 уникальными хостами, что на 4 с небольшим миллиона больше, чем в 2012 году. 82% нотификаций о заблокированных веб-атаках были получены при блокировании атак с веб-ресурсов, расположенных в десяти странах мира.



Распределение по странам источников веб-атак



Из первой десятки выбыл Китай, занимавший первое место в рейтинге до 2010 года.

Все страны мира можно распределить по степени риска заражения при серфинге в интернете.

1. **Группа повышенного риска**. В эту группу с результатом 41-60% вошли 15 стран. Это Россия, Австрия, Германия, большинство стран постсоветского пространства и страны Азии. За год эта группа уменьшилась более чем вдвое.
2. **Группа риска**. В эту группу с показателями 21-40,99% попали 118 стран.
3. **Группа самых безопасных при серфинге в интернете стран** (0-20,99%). В эту группу попали 25 стран. В нее входят Чехия (20,3%), Словакия (19,7%), Сингапур (18,5%) и ряд африканских стран.

Локальные угрозы

Наши антивирусные решения успешно обнаружили почти **3 миллиарда** вирусных инцидентов на пользовательских компьютерах, участвующих в Kaspersky Security Network.Всего в данных инцидентах было зафиксировано 1**,8 миллиона** вредоносных и потенциально нежелательных программ, которые проникли на компьютеры **не** через интернет, почту или сетевые порты.

Данные получены на основе работы антивируса, сканирующего файлы на жестком диске в момент их создания или обращения к ним, и при сканировании различных съемных носителей информации.

Риск локального заражения в разных странах

ТОР 20 стран по уровню зараженности компьютеров состоит из стран Африки, Ближнего Востока и Юго-Восточной Азии.

В среднем в группе стран из ТОР 20 вредоносный объект хотя бы раз был обнаружен на компьютере — на жестком диске или на съемном носителе, подключенном к нему, — у 60,1% пользователей, тогда как в 2012 году – у 73,8%.

В случае локальных угроз все страны мира можно разделить на несколько категорий.

1. Максимальный уровень заражения (более 60%) зафиксирован в 4 странах: Вьетнам (68,1%), Бангладеш (64,9%), Непал (62,4%), Монголия (60,2%).
2. Высокий уровень заражения (41-60%): 67 стран мира.
3. Средний уровень заражения (21-40,99%): 78 стран.
4. Наименьший уровень заражения (0-20,99%): 9 стран мира.

В десятку самых безопасных по уровню локального заражения стран согласно занятым местам вошли: Дания, Чехия, Финляндия, Куба, Япония, Словакия, Словения, Норвегия, Сейшельские острова, Мальта.

В среднем в указанной десятке стран мира хотя бы раз в течение года было атаковано 18,8% компьютеров пользователей. По сравнению с 2012 годом этот показатель уменьшился на 6,6%.