Отчет

Отчет McAfee об угрозах за первый квартал 2012 года

McAfee Labs™

Содержание

Древнегреческий философ Гераклит, известный своим учением об изменении как о центральном принципе Вселенной, однажды написал, что «все течет, ничто не стоит на месте». Первый квартал 2012 года стал иллюстрацией учения Гераклита почти во всех категориях угроз безопасности. Несмотря на то, что в конце 2011 года наблюдалось сокращение числа вредоносных программ и угроз безопасности во многих категориях, первый квартал 2012 года оказался почти полной противоположностью. Число вредоносных программ для ПК давно уже не росло такими огромными темпами, как в этом квартале. То же самое касается вредоносных программ для мобильных устройств. Мы стали свидетелями увеличения числа руткитов уже известных типов, а также появления ряда новых семейств руткитов. Многие из уже знакомых вредоносных программ, которые мы уже давно анализируем и с которыми мы уже давно боремся, в этом квартале вернули себе прежние позиции. Прежде всего это касается троянских коней, предназначенных для кражи паролей. В данном выпуске *Отчета об угрозах* мы впервые представляем вашему вниманию результаты слежения за такими новыми угрозами безопасности, как руткит ZeroAccess и вредоносные программы с цифровыми подписями. Помимо этого мы подготовили самую подробную на сегодняшний день статистику сетевых атак.

Объем нежелательных сообщений немного вырос в начале квартала, однако потом опять начал снижаться. Наблюдался рост количества вредоносных программ, предназначенных для компьютеров Macintosh. Эту тенденцию нельзя назвать ярко выраженной, однако рост налицо.

Несмотря на то, что количество спама в глобальном масштабе по-прежнему невелико, в отдельных регионах, как, например, в Германии и Китае, продолжает наблюдаться многообразие и рост числа нежелательных сообщений. Число новых случаев заражения компьютеров бот-сетями на протяжении отчетного периода оставалось на одном уровне, хотя в некоторых странах, особенно в Испании и Японии, наблюдался рост.

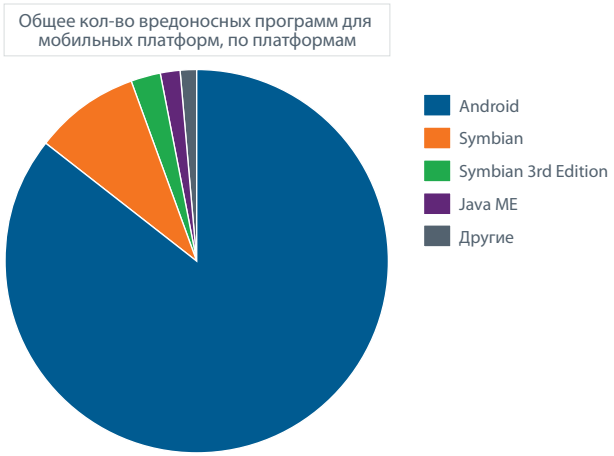
США опять стали страной, в которой размещено самое большое количество вредоносного веб-содержимого в мире. Об этой тенденции пойдет речь в разделе, посвященном сетевым атакам. В этот раз этот раздел расширен и содержит подробные статистические данные о географическом местоположении злоумышленников и их жертв. Продолжился рост числа активных вредоносных URL-адресов, ставший заметным еще в предыдущем квартале. Всемирная паутина — опасное место для неосведомленных и незащищенных.

Особой популярностью в отчетном квартале пользовались инструменты и наборы инструментов для создания вредоносных программ, использующие уязвимости Java и Flash. Правоохранительные органы провели ряд значительных операций и задержали несколько серьезных киберпреступников и «хактивистов». Наибольший резонанс вызвали, пожалуй, закрытие бот-сети kelihos/waledac и широко освещенные в прессе аресты членов групп Anonymous и LulzSec. Мы всегда рады видеть торжество закона в данных областях, хотя это не избавляет нас от других угроз безопасности.

Угрозы продолжают эволюционировать, а злоумышленники продолжают изобретать все новые и новые ухищрения. Поэтому в борьбе с ними мы всегда на чеку.

Угрозы безопасности мобильных устройств

В отчетном квартале наблюдалось значительное увеличение числа вредоносных программ для мобильных устройств. Данный скачок относился почти исключительно к вредоносным программам для платформы Android. Если в середине 2011 года количество угроз для Android исчислялось сотнями, то в начале этого года их было уже несколько тысяч. Между тем мы научились лучше собирать, обрабатывать и обнаруживать вредоносные программы для мобильных устройств, и в первом квартале этого года список продолжил расти: число угроз для Android теперь достигает почти 7 000, при том что общее число вредоносных программ для мобильных устройств в нашей базе данных составляет 8 000.



Источником и объектом абсолютного большинства атак (и используемых в них вредоносных программ) являются сторонние магазины приложений, особенно те, которые расположены в Китае и России. В большинстве случаев такие вредоносные программы не встречаются в официальном магазине приложений для Android. С магазином приложений Google было связано несколько инцидентов, однако их число пока незначительно. McAfee Labs рекомендует клиентам устанавливать программное обеспечение только из официального магазина приложений. Такая мера предосторожности позволяет значительно снизить риск взлома вашего устройства Android.

В отчетном квартале наблюдалось значительное число новых программ для показа рекламы и вредоносных программ-бэкдоров для мобильных устройств, а также очень простых вредоносных программ для рассылки платных SMS. Под программами для показа рекламы понимаются программы, показывающие рекламу на телефоне пользователя без его согласия (сюда не относятся игры и приложения, финансируемые за счет показа рекламы). Диапазон программ для показа рекламы простирается от обоев с коммерческими предложениями (Android/Nyearleaker.A) до поддельных версий игр, перенаправляющих посетителей на рекламные сайты (Android/Steek.A). Программы для показа рекламы не обязательно понижают уровень безопасности пользователей, но являются источником нежелательной рекламы.

Троянские кони, создающие «черные ходы» на устройствах с Android, стали значительно более изощренными. Вместо выполнения одного единственного действия они с помощью средств использования уязвимостей получают права суперпользователя и запускают другие вредоносные программы. Android/FoncyDropper.A, например, содержит средство использования уязвимости, позволяющее получить права суперпользователя, перехватить управление телефоном и запустить IRC-бот для получения команд от злоумышленника, от которого исходит данная атака. Также осуществляется рассылка SMS на платные номера в той стране, к которой относится SIM-карта.

Похожим образом, Android/Rootsmart.A с помощью средства использования уязвимости получает права суперпользователя и загружает Android/DrdLive.A — троянского коня, рассылающего SMS на платные номера и принимающего команды с командно-контрольного сервера.

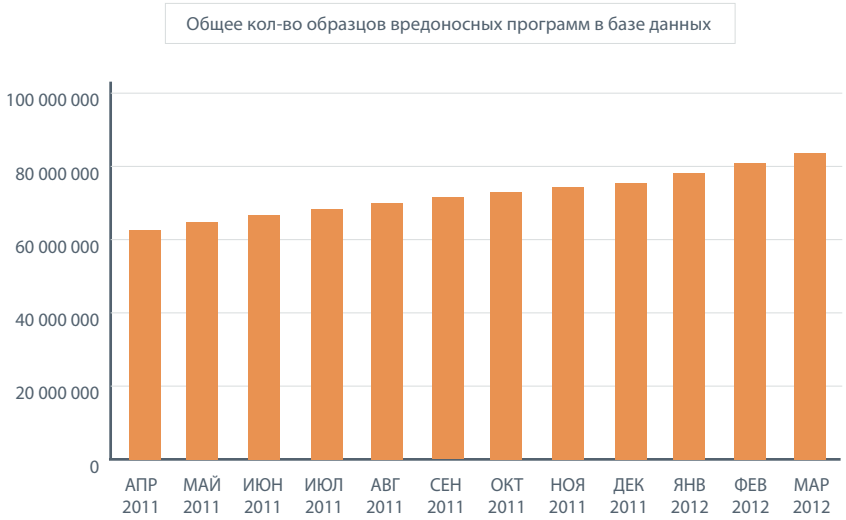
Android/Stiniter.A с помощью средства использования уязвимости получает права суперпользователя, загружает дополнительные вредоносные программы и пересылает информацию с телефона на сайты, находящиеся под контролем злоумышленника. Он также посылает текстовые сообщения на платные номера. Злоумышленник посредством командно-контрольного сервера может менять текст сообщений и указывать номер, на который взломанный телефон посылает эти сообщения.

В отчетном квартале авторы вредоносных программ создали одного из первых троянских коней для Android с разрушительным действием. Android/Moghava.A разрушает не приложения или другие исполняемые файлы, а фотографии. Moghava.A выполняет обнаружение находящихся на SD-карте фотографий и добавляет к каждой их них изображение аятоллы Хомейни. Более того, эта вредоносная программа функционирует с некоторыми сбоями, в результате чего изображения Хомейни добавляются к фотографиям до тех пор, пока на карте памяти не закончится место.

Мораль всего этого очевидна: мы должны обеспечить защиту всех устройств — мобильных и прочих, — на которых находятся ценные данные. В противном случае этими ценными данными с удовольствием займутся современные киберпреступники.

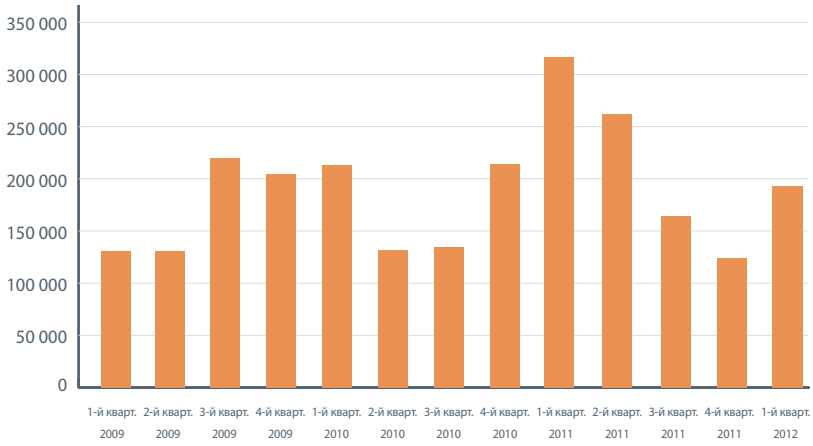
Вредоносные программы

Разговор о вредоносных программах можно начать словами из песни группы Thin Lizzy: «парни снова в городе». На протяжении последних двух кварталов 2011 года McAfee Labs наблюдала спад общих темпов роста числа вредоносных программ для ПК. Похоже, что эта передышка закончилась. Более того, она не просто закончилась: число обнаруженных в отчетный период вредоносных программ превысило все квартальные показатели за последние четыре года! К началу 2012 года в нашем «зоопарке вредоносных программ» накопилось более 75 млн образцов, однако огромные темпы роста в первом квартале привели к тому, что их число на сегодняшний день уже превысило 83 млн экземпляров. Неизвестно, когда мы преодолеем отметку в 100 млн, однако можно с уверенностью сказать, что это случится уже через несколько кварталов. Рост числа руткитов и имеющихся в них функций, появление вредоносных программ с цифровыми подписями и безудержный темпы роста в большинстве других категорий угроз безопасности могут привести к тому, что 2012 год станет очень непростым годом с точки зрения обеспечения безопасности.

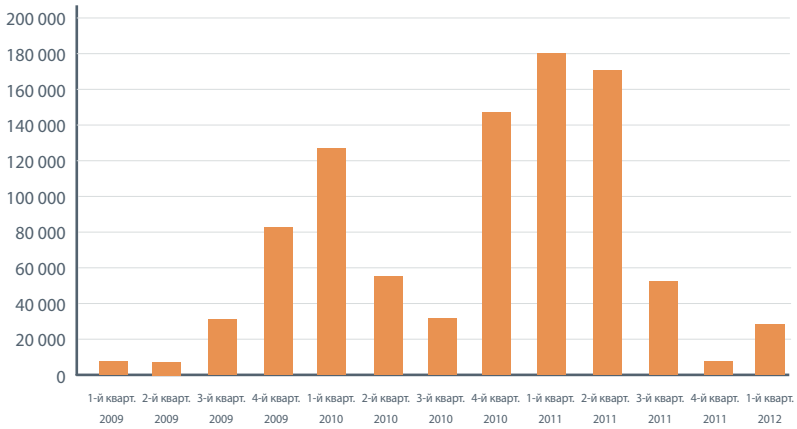


В отчетном квартале темпы роста и распространения руткитов замедлились. Немного активнее вел себя Koutodoor, хотя это не идет ни в какое сравнение с его активностью год назад. В настоящем отчете мы впервые приводим отдельные статистические данные по руткиту ZeroAccess. Эта вредоносная программа уже начала пользоваться популярностью у киберпреступников и других злоумышленников. Руткиты, или программы-невидимки, являются одной из самых опасных категорий вредоносных программ. Руткиты оказали значительное влияние почти на все другие категории вредоносных программ. Их разрабатывают таким образом, чтобы они могли оставаться незамеченными и длительное время «жить» в системе.

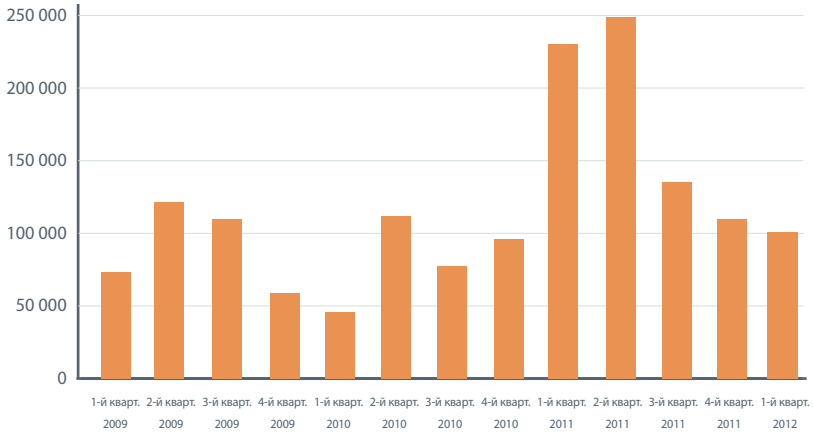
Кол-во обнаруженных уникальных образцов руткитов



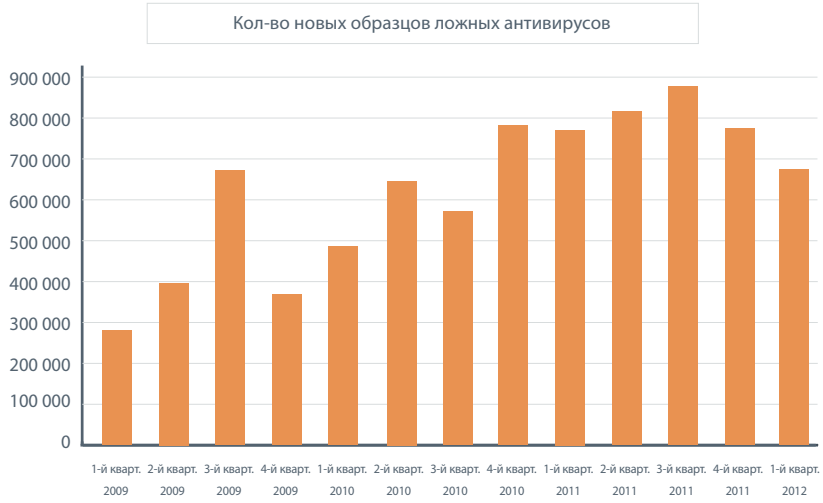
Кол-во новых образцов Koutodoor

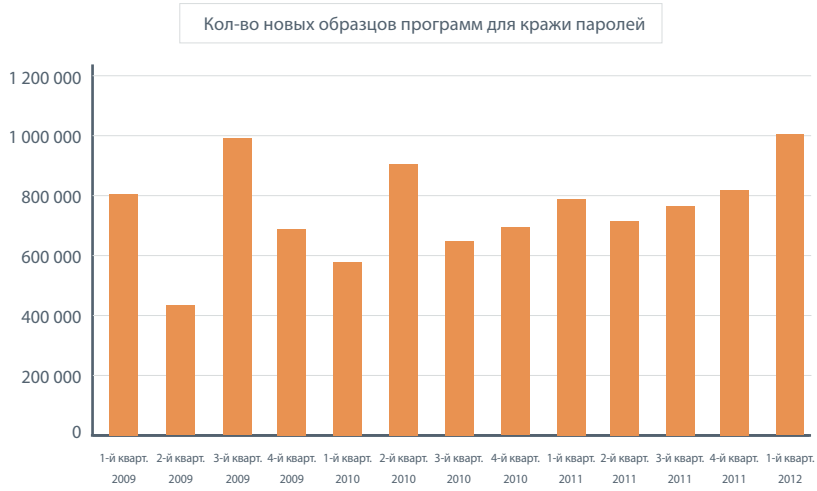


Кол-во новых образцов TDSS



Давайте поговорим о других наших «любимчиках» — ложных антивирусах (поддельных защитных программах), вредоносных программах с автозапуском и троянских конях для кражи паролей. Они по-прежнему с нами. В первых двух категориях темпы роста продолжают медленно падать, а вот в категории программ для кражей паролей в отчетном квартале наблюдался сильный скачок.



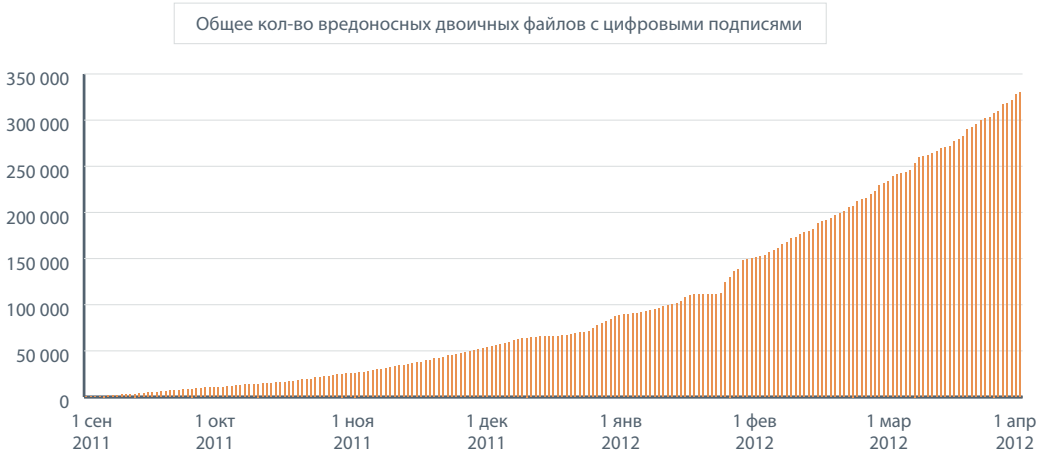


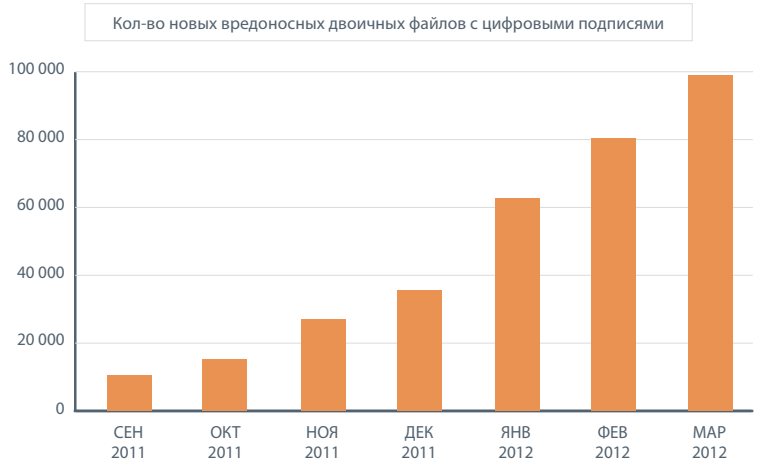
Вредоносные программы с цифровыми подписями

Старший аналитик McAfee Labs Крейг Шмугар (Craig Schmugar) в блоге McAfee Labs пишет о том, почему создатели вредоносных программ используют в своих программах цифровые подписи:

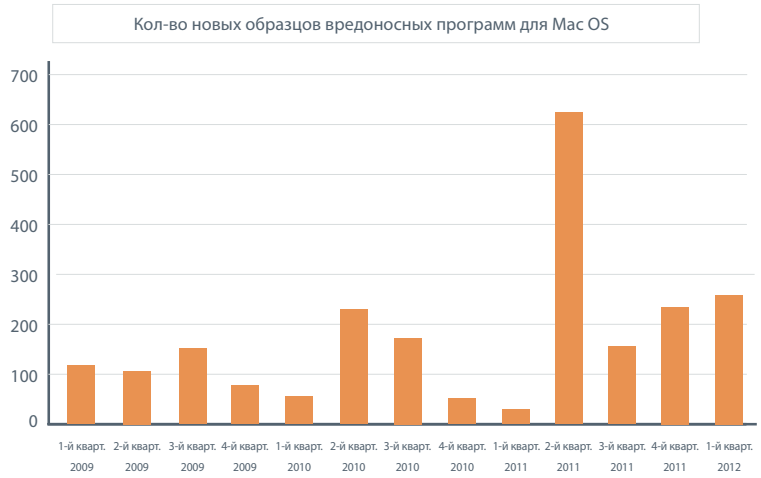
«Злоумышленники подписывают вредоносные программы, пытаясь тем самым внушить пользователям и администраторам доверие к файлу, а также избежать обнаружения файла защитными программами и обойти системные политики. Многие из таких вредоносных программ подписываются с помощью украденных сертификатов, хотя встречаются и двоичные файлы с самоподписанными сертификатами или с „тестовой подписью". Тестовая подпись иногда используется в сочетании с методами социальной инженерии».[1]

В отчетном квартале было обнаружено более 200 000 новых, неповторяющихся двоичных файлов вредоносных программ, имеющих действительные цифровые подписи. В нашем *Прогнозе угроз на 2012 год* отмечалось, что в свете успеха бот-сетей Duqu и Stuxnet популярность этого метода будет расти.[2] Спустя три месяца мы видим, что этот прогноз действительно начинает сбываться.

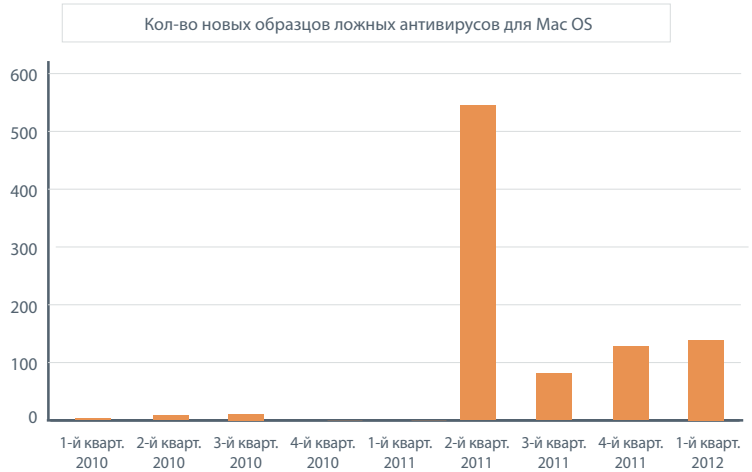




Число вредоносных программ для компьютеров Macintosh компании Apple по-прежнему стабильно растет. По сравнению с вредоносными программами для ПК вредоносные программы для Macintosh традиционно производят впечатление довольно безвредных. Однако вредоносную программу можно написать для любой операционной системы и платформы, поэтому меры предосторожности необходимо принимать всем пользователям.

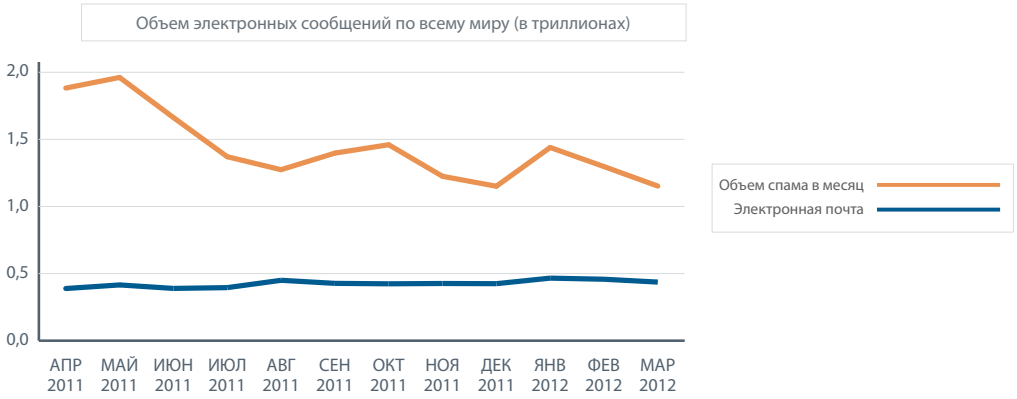


После большого скачка в середине прошлого года темпы роста числа ложных антивирусов для Macintosh, по-видимому, несколько стабилизировались.



Опасные сообщения

В прошлом отчете мы отметили, что в конце 2011 года объем нежелательных сообщений достиг рекордно низких показателей. Несмотря на очередной скачок в январе, к концу квартала объем нежелательных сообщений опять достиг низких показателей предыдущего периода. За последние три месяца рост объемов спама наблюдался в Китае, Германии, Польше, Испании и Великобритании; в то время как в Бразилии, Индонезии и России объемы спама сокращались. Несмотря на то, что в глобальном масштабе объемы спама сокращаются, опасность целенаправленного фишинга и нежелательных сообщений по-прежнему велика, поэтому потребителям и компаниям необходимо постоянно быть начеку. Степень изощренности наблюдаемых на сегодняшний день угроз безопасности по-прежнему высока.

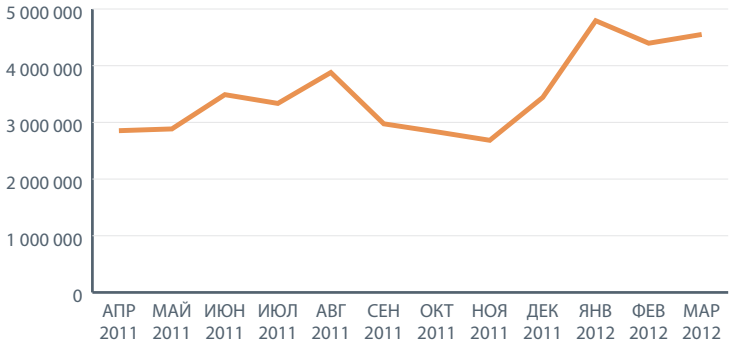



Объем спама
Индия
100 000 000
80 000 000
60 000 000
40 000 000
20 000 000
0
Индонезия
80 000 000
70 000 000
60 000 000
50 000 000
40 000 000
30 000 000
20 000 000
10 000 000
0
Испания
16 000 000
14 000 000
12 000 000
10 000 000
8 000 000
6 000 000
4 000 000
2 000 000
0
Италия
12 000 000
10 000 000
8 000 000
6 000 000
4 000 000
2 000 000
0
Китай
25 000 000
20 000 000
15 000 000
10 000 000
5 000 000
0
Колумбия
18 000 000
16 000 000
14 000 000
12 000 000
10 000 000
8 000 000
6 000 000
4 000 000
2 000 000
0
Республика Корея
50 000 000
45 000 000
40 000 000
35 000 000
30 000 000
25 000 000
20 000 000
15 000 000
10 000 000
5 000 000
0
Россия
100 000 000
90 000 000
80 000 000
70 000 000
60 000 000
50 000 000
40 000 000
30 000 000
20 000 000
10 000 000
0
США
250 000 000
200 000 000
150 000 000
100 000 000
50 000 000
0
Япония
2 500 000
2 000 000
1 500 000
1 000 000
500 000
0
АПР 2011
МАЙ 2011
ИЮН 2011
ИЮЛ 2011
АВГ 2011
СЕН 2011
ОКТ 2011
НОЯ 2011
ДЕК 2011
ЯНВ 2012
ФЕВ 2012
МАР 2012

Статистика активности бот-сетей

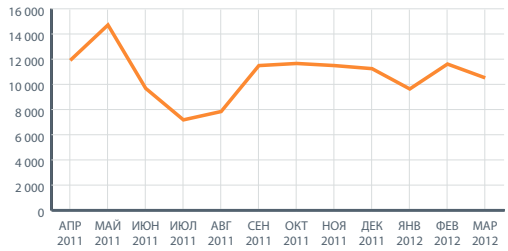
Совокупные темпы роста бот-сетей для рассылки нежелательных сообщений резко подскочили по сравнению с предыдущим кварталом. Темпы заражения росли в Колумбии, Японии, Польше, Испании и Соединенных Штатах. В Индонезии, Португалии и Южной Корее темпы заражения продолжали падать.

Кол-во обнаруженных случаев заражения бот-сетями по всему миру

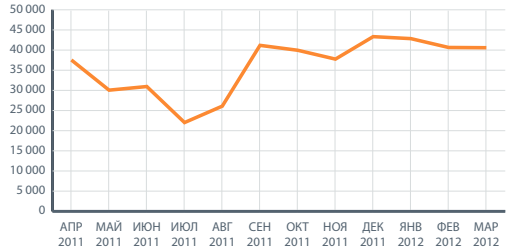


Кол-во новых отправителей в бот-сетях

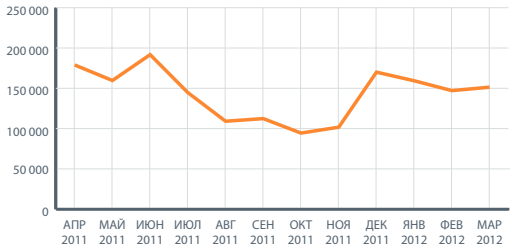
Австралия



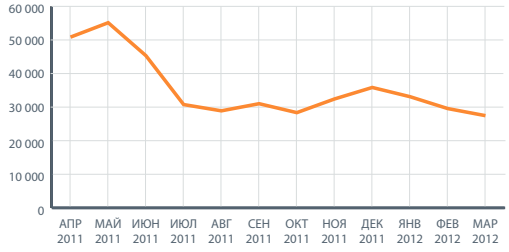
Аргентина



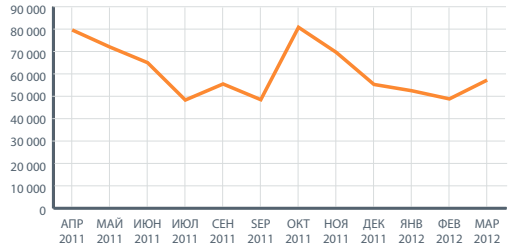
Бразилия



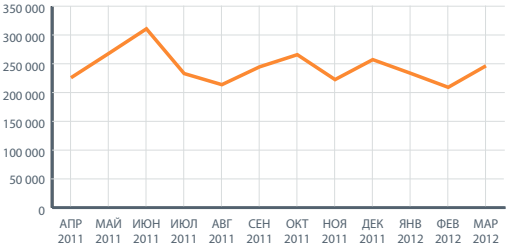
Великобритания

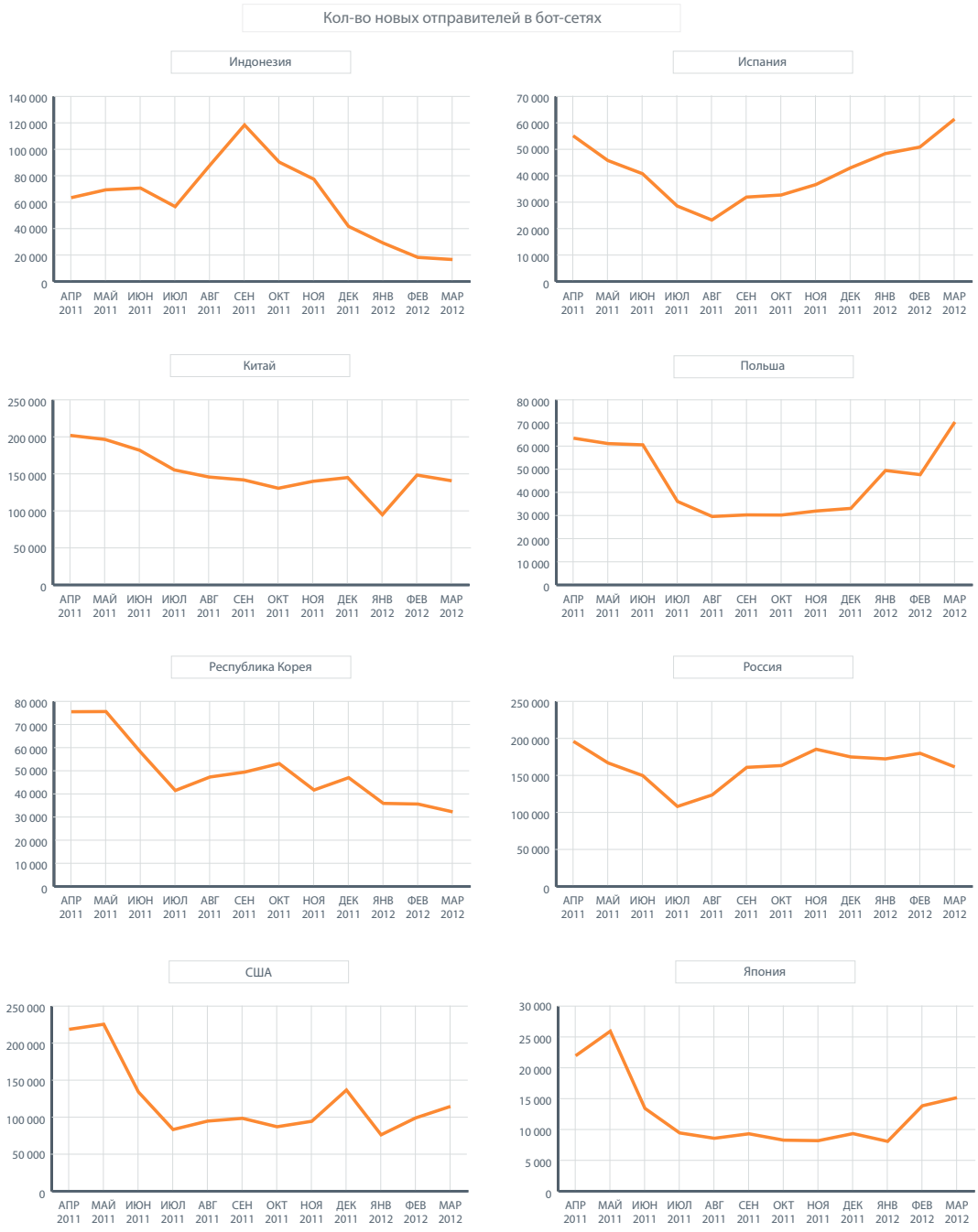


Германия

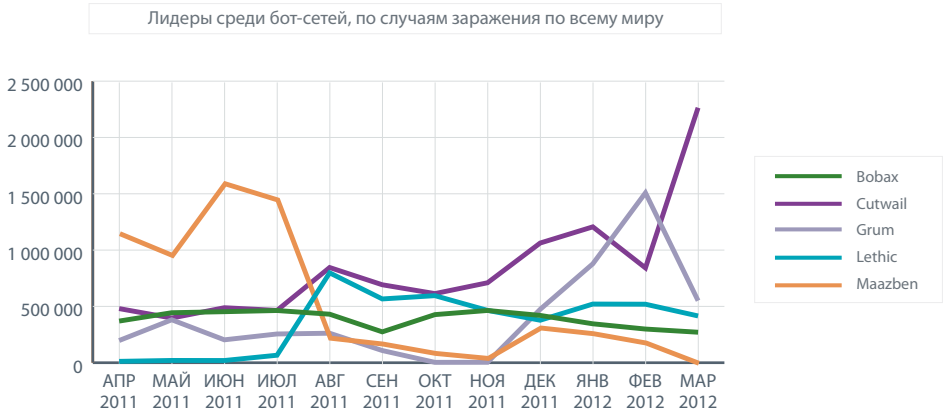


Индия

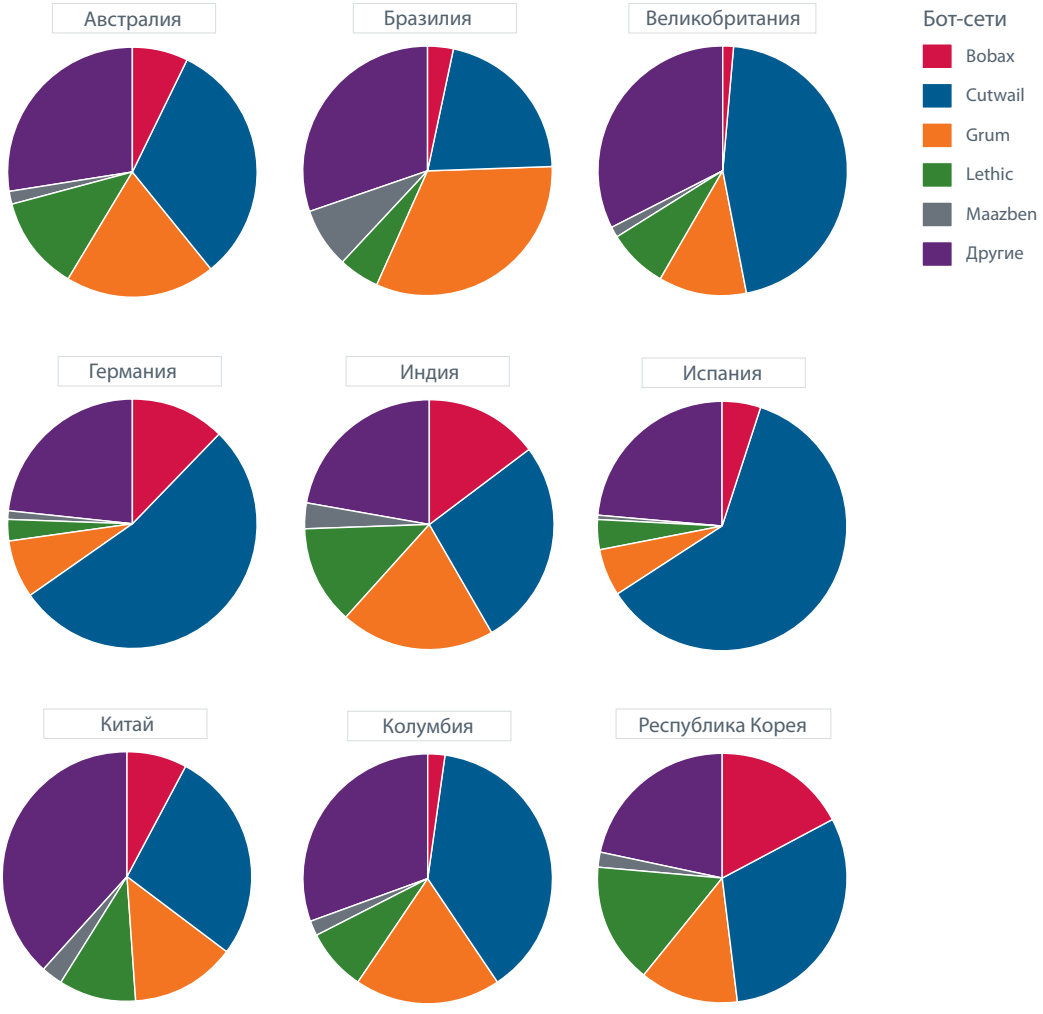


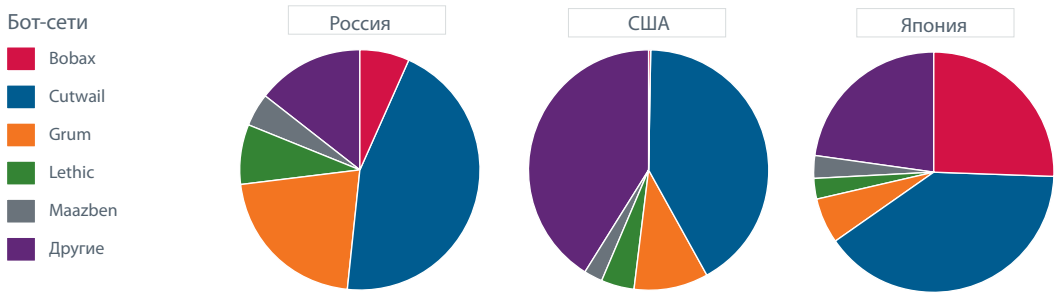

Кол-во новых отправителей в бот-сетях
Индонезия
140 000
120 000
100 000
80 000
60 000
40 000
20 000
0
Испания
70 000
60 000
50 000
40 000
30 000
20 000
10 000
0
Китай
250 000
200 000
150 000
100 000
50 000
0
Польша
80 000
70 000
60 000
50 000
40 000
30 000
20 000
10 000
0
Республика Корея
80 000
70 000
60 000
50 000
40 000
30 000
20 000
10 000
0
Россия
250 000
200 000
150 000
100 000
50 000
0
США
250 000
200 000
150 000
100 000
50 000
0
Япония
30 000
25 000
20 000
15 000
10 000
5 000
0
АПР 2011
МАЙ 2011
ИЮН 2011
ИЮЛ 2011
АВГ 2011
СЕН 2011
ОКТ 2011
НОЯ 2011
ДЕК 2011
ЯНВ 2012
ФЕВ 2012
МАР 2012

Многие из ведущих бот-сетей для рассылки вредоносных сообщений показали незначительные темпы роста или даже снижение числа новых заражений. Исключение составляет бот-сеть Cutwail, значительно увеличившаяся в размерах.

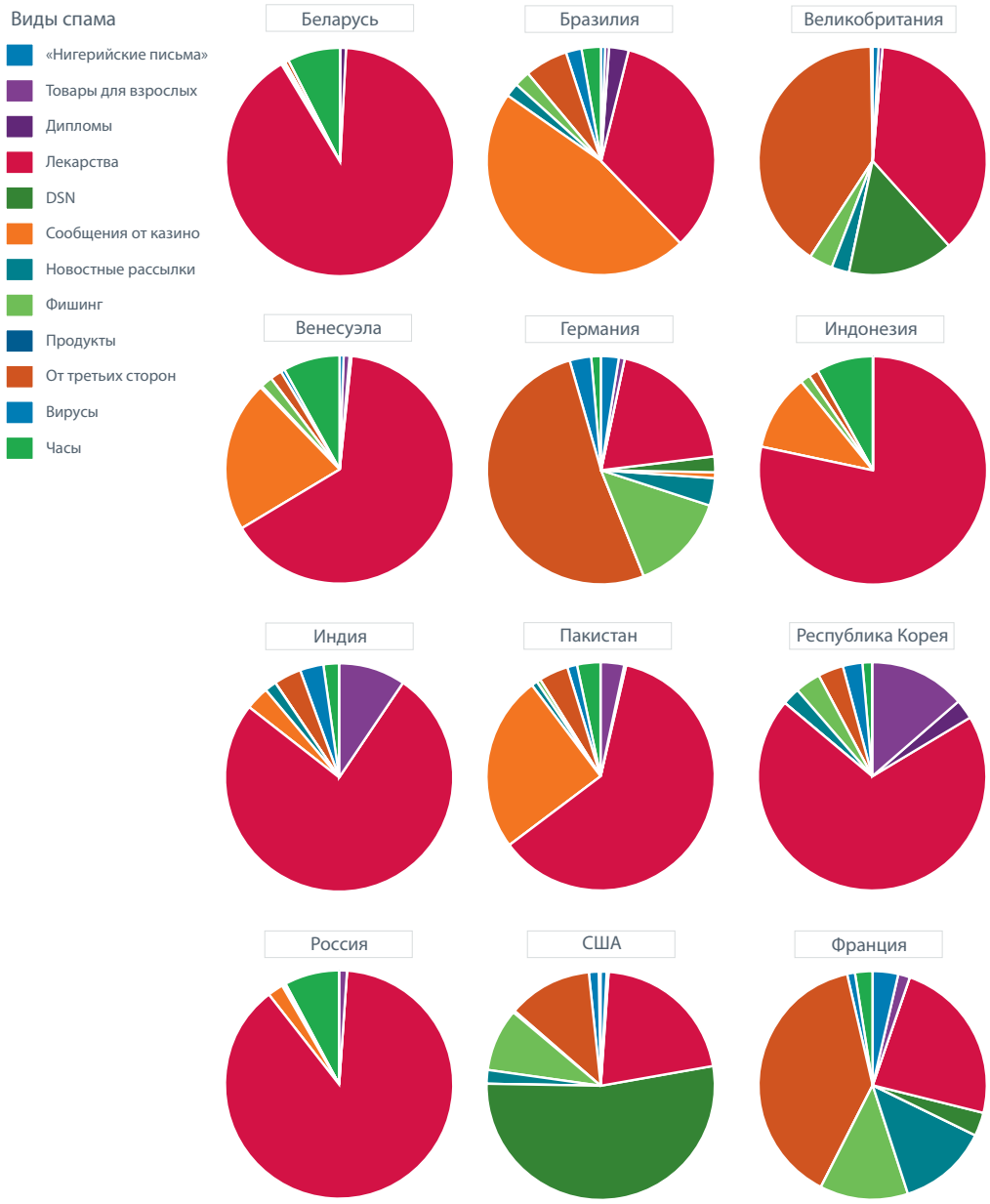


Не стоит забывать, что наличие *новых* случаев заражения не означает, что ранее зараженные компьютеры перестали быть зараженными. Приведенные нами результаты анализа активности бот-сетей по странам показывают, что многие из этих бот-сетей по-прежнему довольно активны в мировом масштабе, даже несмотря на то, что число заражаемых ими компьютеров снижается. По числу новых случаев заражения и по общему количеству зараженных компьютеров первое место в мире занимает Cutwail. Исключением стала Бразилия, где самой распространенной бот-сетью является Grum.





Как и прежде, методы социальной инженерии в разных регионах мира сильно отличаются друг от друга в том, что касается используемых в нежелательных сообщениях приманок и тем. Приманки меняются в зависимости от месяца и времени года; часто они бывают привязаны к праздникам, спортивным мероприятиям и трагическим событиям. В Бразилии особой популярностью пользовались нежелательные сообщения, связанные с игорным бизнесом, в то время как во многих других странах основной тематикой нежелательных сообщений были медикаменты. Что касается США, то там были особенно распространены ложные уведомления о состоянии доставки (DSN, Delivery Status Notification). Это свидетельствует о том, что в разных культурах работают разные приманки.



Сетевые угрозы безопасности

Действительно ли большинство кибератак исходит из США? Определить, откуда исходят атаки и кто за ними стоит, — очень сложная задача. Еще пару лет назад большинство клиентов как в потребительском, так и в корпоративном сегменте не задавало нам вопросов о том, откуда исходят те или иные атаки и кто за ними стоит. Сегодня же нас регулярно об этом спрашивают, однако давать точные ответы на такие вопросы непросто. В большинстве случаев определение автора и источника атаки приходится проводить только на основе IP-адресов и базовых географических функций. Полученная таким образом информация может служить хорошей отправной точкой, но это не более чем отправная точка, потому что географическое положение и IP-адрес не помогают в определении конкретных действующих лиц.

Во многих случаях взломанный компьютер используется в качестве прокси для рассылки нежелательных сообщений, расширения бот-сетей, проведения атак типа «отказ в обслуживании» или иных видов вредоносных действий. Такие компьютеры могут находиться в любой точке мира, и судя по данным за отчетный квартал, многие из них находятся в США.

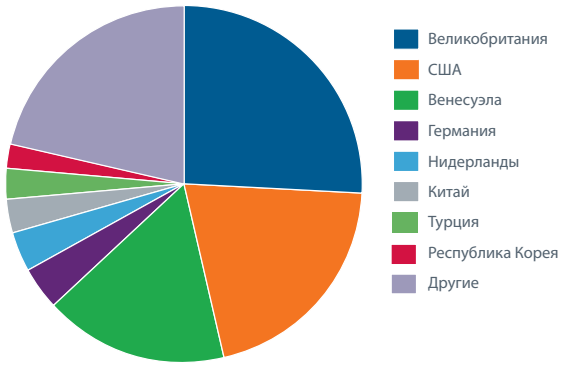
Давайте поподробнее остановимся на некоторых категориях угроз безопасности, информация о которых собирается и анализируется с помощью сети McAfee Global Threat Intelligence™. При подготовке данного «Отчета об угрозах» мы значительно расширили объем информации, включаемой нами в аналитические отчеты об активности сетей.

Среди сетевых угроз безопасности опять лидируют атаки с использованием службы удаленных вызовов процедур и атаки с внедрением SQL-кода. Количество атак с использованием межсайтовых сценариев довольно сильно сократилось — с 19 процентов в предыдущем квартале до 8 процентов в отчетном квартале.

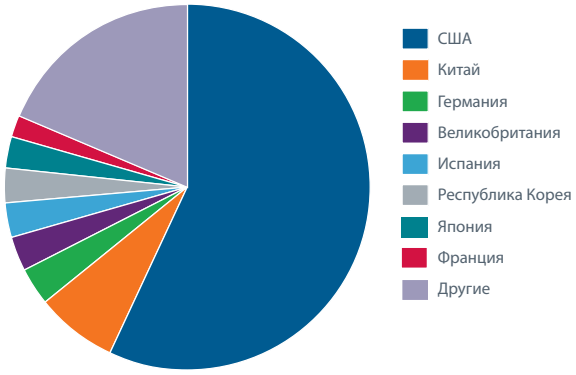
Лидеры среди сетевых угроз безопасности

Что касается атак с внедрением SQL-кода, то здесь США заняли первое место как по количеству атак, исходящих из этой страны, так и по количеству объектов атак, находящихся в этой стране.

Страны, из которых исходит большинство атак с внедрением SQL-кода

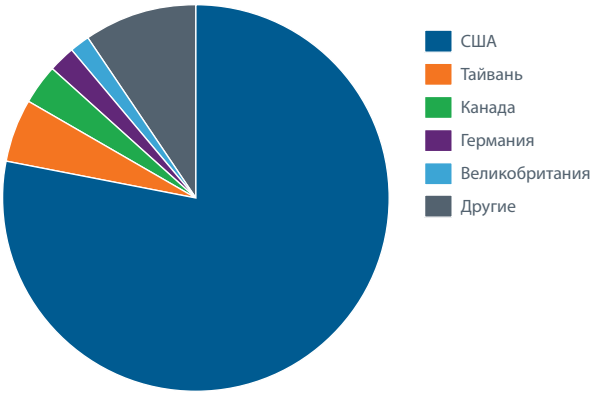


Страны, наиболее подверженные атакам с внедрением SQL-кода

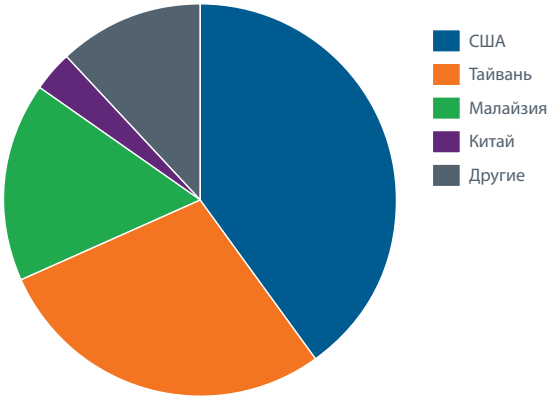


В отчетном квартале США намного опередили все другие страны в качестве источника атак с использованием межсайтовых сценариев (XSS), а также стали первой страной по количеству жертв подобных атак. Второе место по этому показателю занимает Тайвань.

Страны, из которых исходит большинство межсайтовых атак с внедрением сценария (XSS)

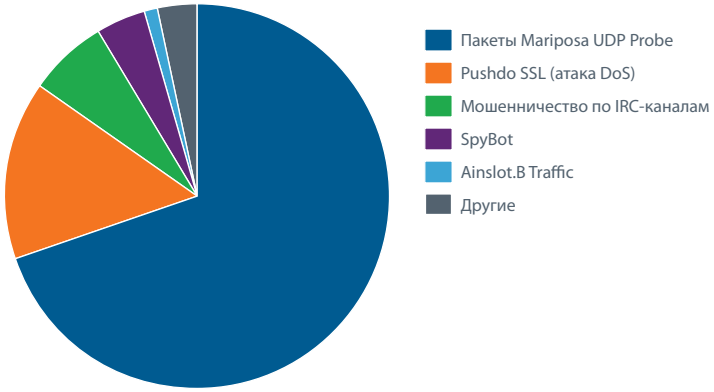


Страны, наиболее подверженные межсайтовым атакам с внедрением сценария (XSS)



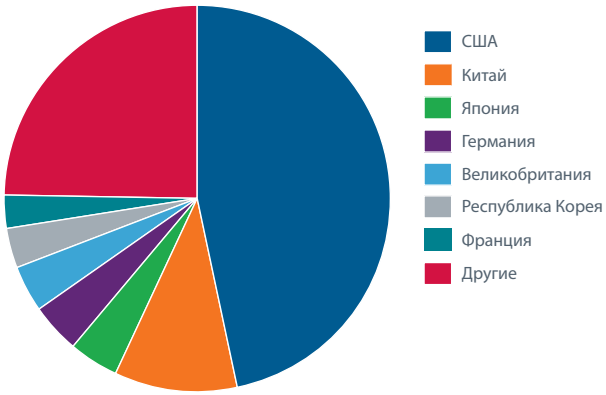
В этот раз мы также включили в отчет список самых часто обнаруживаемых бот-сетей с сетевыми угрозами. Бесспорным лидером стала бот-сеть Mariposa — финансовая бот-сеть для кражи данных о кредитных карточках и банковских счетах. Второй в этом списке с большим отставанием идет Pushdo (другое название бот-сети Cutwail).

Лидеры среди обнаруженных бот-сетей



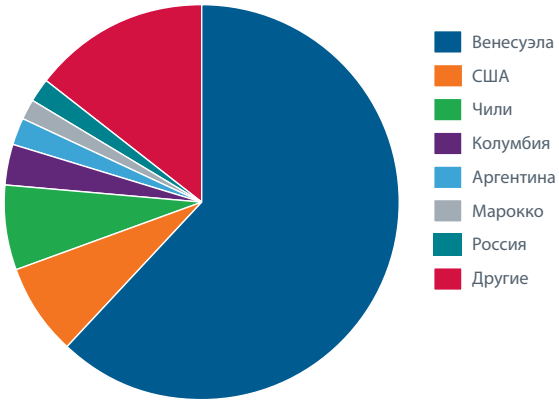
США возглавили еще один из наших списков сетевых угроз. Почти половина всех новых серверов для управления бот-сетями, обнаруженных с помощью McAfee Global Threat Intelligence, находится в США.

Лидеры по количеству управляющих серверов бот-сетей



Жертв бот-сетей (тоже новый раздел в нашем отчете) больше всего было в Венесуэле, на втором месте — США (со значительным отставанием).

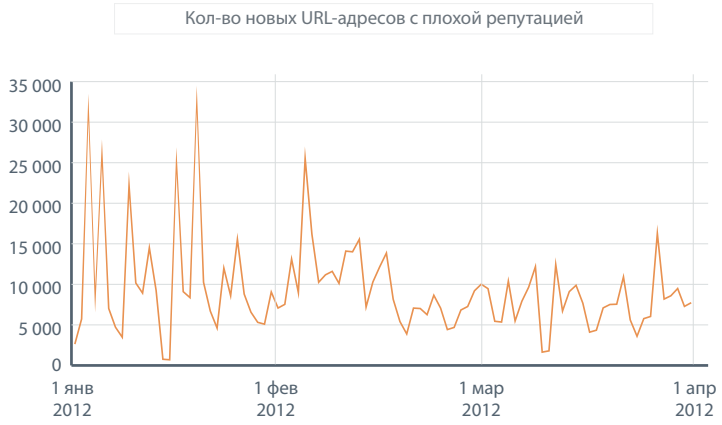
Страны, наиболее подверженные бот-сетям



Веб-угрозы

Веб-сайты могут приобрести репутацию плохих или вредоносных по целому ряду причин. Репутация может определяться на основе полных доменов и любого количества субдоменов, а также на основе одного IP-адреса или даже конкретного URL-адреса. Сайт может получить репутацию вредоносного, если на нем размещены вредоносные или потенциально нежелательные программы, или если сайт создан для фишинга. Часто мы наблюдаем те или иные сочетания сомнительного кода и сомнительных функций. Это только некоторые из факторов, на основе которых мы определяем репутацию сайта.

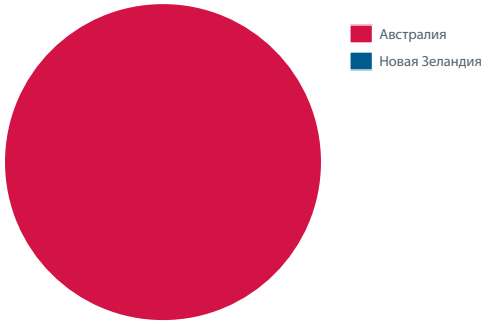
В предыдущем квартале McAfee Labs ежедневно обнаруживала в среднем 9 300 новых сайтов с плохой репутацией. Если учитывать URL-адреса в нежелательных сообщениях, рассылаемых по электронной почте, то этот показатель достиг отметки 11 000 обращений в день. В течение отчетного периода, однако, данный показатель упал до 9 000 обращений в день.



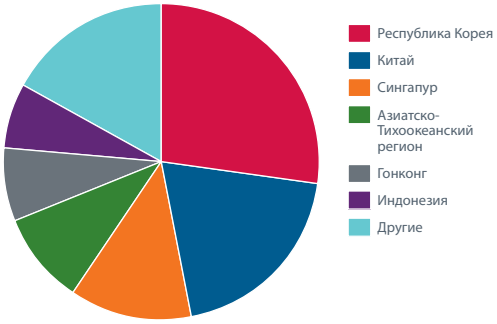
Несмотря на снижение количества URL-адресов с плохой репутацией, число наших клиентов, сталкивающихся с перенаправлениями на вредоносные веб-сайты, растет. В предыдущем квартале McAfee ежедневно приходилось защищать от веб-атак с использованием вредоносных программ в среднем каждого восьмого из своих клиентов (остальные 7 клиентов не посещали опасные веб-сайты). В отчетный квартал защищать пришлось уже каждого шестого клиента. Оставаясь неизменным на протяжении всего квартала, это соотношение служит показателем того, насколько успешно киберпреступникам удается перенаправлять пользователей на свои вредоносные сайты. Подавляющее большинство новых вредоносных сайтов находится в США. Статистика по регионам показывает, что в глобальной Сети нет области, не подверженной риску.

Местоположение серверов с вредоносным содержимым

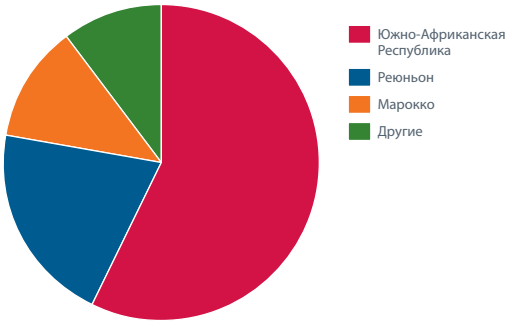
Австралия и Новая Зеландия



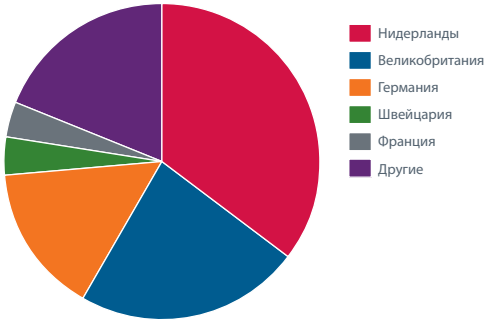
Азиатско-Тихоокеанский регион



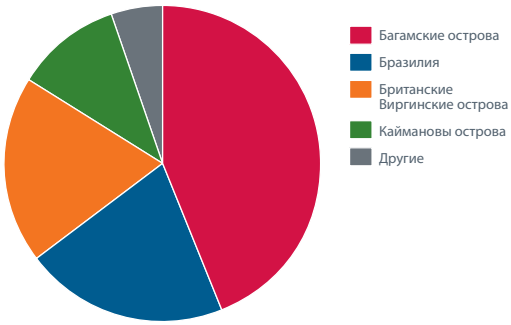
Африка



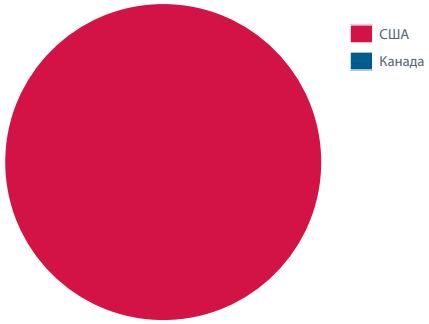
Европа и Ближний Восток



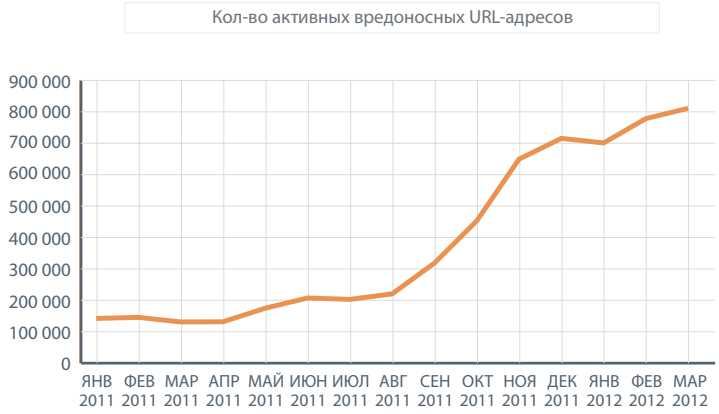
Латинская Америка



Северная Америка



Число веб-сайтов, на которых расположены вредоносные файлы для загрузки или средства использования уязвимостей веб-обозревателей, по-прежнему растет.



В отчетном квартале примерно на треть сократилось число веб-сайтов, на которых расположены вредоносные и потенциально нежелательные программы. В четвертом квартале 2011 года ежедневно появлялось в среднем 6 500 подобных сайтов, а в отчетном квартале — около 4 200.

Ситуация с сайтами для фишинга с прошлого квартала не изменилась. В отчетном квартале число ежедневно обнаруживаемых новых фишинговых URL-адресов в среднем опять составило около 2 200. Фишинговые сайты по-прежнему представляют значительную опасность для всех, кто пользуется Интернетом. Число фишинговых сайтов превышает число сайтов, содержащих только вредоносные файлы и нежелательные сообщения.

Киберпреступность

Инструменты для создания вредоносных программ

Помимо очередных обновлений наборов средств использования уязвимостей в отчетном квартале появилось большое количество совершенно новых инструментов для создания преступных программ. Сначала в них активно использовалась обнаруженная в октябре 2011 года уязвимость Java Rhino (CVE-2011-3544), но вскоре они переключились на две уязвимости текущего года:

- уязвимость, связанная с обработкой MIDI-файла библиотекой мультимедиа Windows (CVE-2012-0003); устранена в январе с помощью критического обновления MS12-004;
- уязвимость, связанная с выполнением Java-кода за пределами «песочницы» JRE (CVE-2012-0507); устранена в середине февраля в рамках критического обновления Oracle Java SE.[3] Данный эксплойт известен под названием Java AtomicReferenceArray.

Среди приведенных ниже в таблице наборов только набор эксплойтов Phoenix содержит средство использования уязвимости CVE-2012-0507 (Java Atomic). Однако в блогах и форумах пишут о том, что похожие средства использования данной уязвимости появились также в BlackHole, Eleonore и Incognito. Следует ожидать, что в ближайшие месяцы средства использования данной уязвимости будут включены и во многие другие наборы.

Название	Происхождение	Используемые уязвимости
Sakura 1.0	Россия или Восточная Европа	Три уязвимости, включая Java Rhino (CVE-2011-3544)
Hierarchy	Россия или Восточная Европа	16 уязвимостей, две из которых были обнаружены в 2011 году: • Flash 10 (CVE-2011-0611) • Java Rhino
Yang Pack **Январь**	Китай	Четыре уязвимости, включая следующие: • Flash 10.3.181.x (CVE-2011-2110) • Flash 10.3.183.x (CVE-2011-2140) • Java Rhino
Zhi Zhu **Февраль**	Китай	Пять уязвимостей, включая следующие: • HTML+TIME (CVE-2011-1255) • Flash 10.3.181.x • Flash 10.3.183.x • WMP MIDI (CVE-2012-0003)
Gong Da Pack **Февраль**	Китай	Три уязвимости: • Flash 10.3.183.x • Java Rhino • WMP MIDI
Phoenix Exploit Kit 3.1 **Март**	Россия	В нашем «Отчете об угрозах» за IV квартал 2011 года была упомянута версия 3.0, в которую входило средство использования уязвимости Java Rhino (CVE-2011-3544). Версия 3.1 включает в себя Java Atomic (CVE-2012-0507).

Для получения дополнительной информации, касающейся вышеуказанных наборов из Китая, рекомендуем блог Kahu Security[4].

Боты и бот-сети

На подпольных форумах активно рекламируются пакеты для создания бот-сетей. Как показано в приведенной ниже таблице, некоторые бот-сети даже продаются с наценкой:

Название	Цены (в долларах США)
Darkness, автор SVAS/Noncenz **Бот для проведения атак типа «распределенный отказ в обслуживании» (DDoS)**	Обновление до версии 10 в январе: 120 $ Пакеты • Minimum: бот для DDoS, без бесплатных обновлений, без модулей = 450 $ • Standard: бот для DDoS, 1 месяц бесплатных обновлений, модуль для захвата паролей = 499 $ • Bronze: бот для DDoS, 3 месяца бесплатных обновлений, модуль для захвата паролей, 1 бесплатная пересборка = 570 $ • Silver: бот для DDoS, 6 месяцев бесплатных обновлений, модуль для захвата паролей, 3 бесплатных пересборки = 650 $ • Gold: бот для DDoS, неограниченное количество бесплатных обновлений, модули для захвата паролей и редактирования «узлов», 5 бесплатных пересборок, 8-процентная скидка на другие продукты = 699 $ • Platinum: бот для DDoS, неограниченное количество бесплатных обновлений, модуль для захвата паролей, неограниченное количество бесплатных пересборок, 20-процентная скидка на другие продукты = 825 $ • Brilliant: бот для DDoS, неограниченное количество бесплатных обновлений, неограниченное количество бесплатных пересборок, все модули бесплатно, 25-процентная скидка на другие продукты = 999 $ Прочее: • Пересборка (изменение URL-адреса) = 35 $ • Исходники = 3 500–5 000 $ • Повторная установка веб-панели (первый раз бесплатно) = 50 $
Citadel[5] **Вариант бот-сети Zeus, финансовая бот-сеть**	• Сборщик ботов и панель администратора = 2 399 $ + 125 $ в месяц за «аренду» (цена на декабрь 2011 года) • Возможность автоматической установки обновлений средств сокрытия бота от антивирусов = 395 $. Каждое обновление стоит 15 $.
THOR, автор TheGrimReap3r **Пиринговая бот-сеть широкого назначения**	• 8 000 $ за пакет без модулей. Скидка 1 500 $ для первых 5 покупателей. • В разработке находятся модули для закрытия ботов, проведения DDoS-атак, захвата формуляров, отслеживания нажатий клавиш, кражи паролей, массовых рассылок.
Carberp **Финансовая бот-сеть**	• Загрузчик, модули захвата, все базовые функции (за исключением нижеследующих) = 2 500 $ • Вышеуказанное + 500 подключений для бэк-коннекта и средства внедрения кода для Internet Explorer и Mozilla FireFox = 5 000 $ • Вышеуказанное + скрытый веб-обозреватель (аналогично VNC) = 8 000 $

Ценовое предложение бот-сети Carberp вызывает удивление. Оно было опубликовано 21 марта, хотя 20 марта российские правоохранительные органы объявили об аресте членов банды Carberp (подробнее см. в следующем разделе).

Борьба с киберпреступностью

В отчетном квартале правоохранительным органам и другим организациям удалось провести ряд значительных мероприятий по закрытию бот-сетей и поимке киберпреступников. В январе корпорация Microsoft направила в суд жалобу на российского программиста, жителя Санкт-Петербурга, обвиняемого ею в управлении бот-сетью Kelihos (известной также под названием Waledac).[6] По словам Брайана Кребса (Brian Krebs), известного эксперта в области безопасности, с 2005 по 2007 год подозреваемый работал старшим системным разработчиком и менеджером проекта в российской компании Agnitum, занимающейся разработкой антивирусов.[7] В интервью новостному порталу Gazeta.ru российский программист отрицает предъявленные ему обвинения.[8]

Гражданин России, задержанный в Цюрихе (Швейцария) в марте 2011 года, в январе этого года был экстрадирован в Нью-Йорк. Ему и его сыну, который остался на свободе, предъявили обвинение в девяти случаях заговора, мошенничества с использованием почты, мошенничества с использованием электронных средств сообщения, компьютерного мошенничества, кражи персональных данных при отягчающих обстоятельствах и мошенничества с ценными бумагами посредством поддельных веб-сайтов за период с 2005 года.[9]

16 марта Секретная служба США в сотрудничестве с Бюро по контролю за соблюдением иммиграционного и таможенного законодательства США объявила о результатах операции «Открытый рынок» по задержанию 50 человек, обвиняемых в краже персональных данных и продаже контрафактных кредитных карточек.[10] Подозреваемые были связаны с международной преступной группировкой, работающей на нескольких киберплатформах и занимающейся покупкой и продажей краденной персональной и финансовой информации в интернет-форумах. Сообщается, что все подзащитные являются членами, сообщниками или сотрудниками преступной организации, носящей название Carder.su (включая следующие варианты: Carder.info, Crdsu.su, Carder.biz и Carder.pro).

20 марта Министерство внутренних дел Российской Федерации и Федеральная служба безопасности Российской Федерации объявили о задержании восьми подозреваемых, обвиняемых в краже денег с банковских счетов при помощи троянского коня Carberp. Предполагается, что они совершили не менее 90 хищений на общую сумму более 60 млн рублей.[11]

Двум мужчинам, задержанным в мае 2011 года в Великобритании, в марте было предъявлено обвинение во взломе компьютеров корпорации Sony Music и в хищении музыки на сумму около 160 млн фунтов стерлингов.[12] Британское агентство по борьбе с особо опасной организованной преступностью заявило, что согласно имеющейся информации данный инцидент произошел в прошлом году, когда другие хакеры получили доступ к сети PlayStation Network и похитили персональные данные 77 млн зарегистрированных пользователей. Считается, что данный случай не связан с атаками Anonymous и LulzSec.

Ряд проведенных за отчетный квартал операций правоохранительных органов был нацелен на задержание членов и сообщников группы Anonymous. После того, как член группы LulzSec, носящий псевдоним Sabu, в августе 2011 года признал свою вину и начал сотрудничать с ФБР, сотрудникам правоохранительных органов удалось поймать других ключевых членов этой группы, занимающейся взломом компьютеров. Обвиняемые, среди которых два жителя Великобритании, два жителя Ирландии и два жителя США, предстали перед судом в Южном округе Нью-Йорка.[13] Ранее Интерпол объявил о задержании 25 предполагаемых членов группы Anonymous в Аргентине, Чили, Колумбии и Испании.[14] 20 марта в США были задержаны W0rmer и Kahuna – два члена хакерской группы CabinCr3w, близкой к Anonymous.[15]

Отчетный квартал показал, что пресекать действия киберпреступников может не только полиция. В январе известный аналитик Данчо Данчев (Dancho Danchev) в своем блоге опубликовал персональные и другие данные гражданина России, связанного с бандой, стоящей за деятельностью Koobface.[16] Спустя несколько дней газета *The New York Times* раскрыла имена еще четырех человек, над разоблачением которых работала группа специалистов по безопасности.[17]

В завершение расскажем о проведенной корпорацией Microsoft «Операции B71», целью которой было закрытие бот-сетей, созданных с помощью различных вариантов программных пакетов Zeus, SpyEye и Ice-IX. 23 марта корпорация Microsoft сообщила о подаче коллективного иска совместно с Центром анализа и обмена информацией между финансовыми службами (Financial Services - Information Sharing and Analysis Center) и Национальной ассоциацией автоматизированных расчетных палат (National Automated Clearing House Association, NACHA). Корпорация Microsoft и ее посредники проанализировали четыре часа сетевого трафика и арестовали серверы, находившиеся в двух хостинговых центрах в Пенсильвании и Иллинойсе. Помимо этого был проведен анализ более 1 700 доменных имен для выяснения их причастности к работе данных бот-сетей.[18]

Хактивизм

Помимо событий, связанных с арестом Sabu, в сфере хактивизма в отчетный период особое внимание привлекли к себе атаки, проведенные в ответ на принудительное закрытие сайта Megaupload. Группа Anonymous в своих пресс-релизах и сообщениях в Twitter утверждала, что в проводимых в рамках операции OpMegaupload атаках на веб-сайты Министерства юстиции США, Американской ассоциации звукозаписывающих компаний, Американской ассоциации кинокомпаний, BMI и ФБР приняли участие тысячи людей. Более интересно, пожалуй, то, что в Европе группе Anonymous удалось вывести своих сторонников на улицы. Используя в качестве предлога закрытие Megaupload, группа Anonymous организовала демонстрации против принятия законов по борьбе с пиратством SOPA, PIPA и ACTA, прошедшие 11 и 25 февраля в более чем ста городах пятнадцати стран мира. В результате мы получили интересное смешение цифрового «хактивизма» и активизма, существующего в физической реальности. Может, в этом стоит видеть предзнаменование грядущих событий?

11 февраля по всей Европе прошли демонстрации против ACTA (Международного соглашения по борьбе с контрафактной продукцией).

Помимо этого в отчетном квартале мы стали свидетелями десятков различных операций в разных уголках планеты. Ни одна из них не вызвала большого резонанса, поэтому нам было не просто выбрать самые значительные из них:

- Проведенная 31 марта операция #OpGlobalBlackout (операция «Глобальное обесточивание») к глобальному обесточиванию не привела. Специалисты по безопасности были почти единогласны во мнении, что подобная атака технически невозможна. Интересно, однако, отметить, какую огромную волну сообщений и обсуждений вызвала эта операция. Группа Anonymous продолжает демонстрировать, что она разбирается в СМИ и умеет формировать новостную картину.
- Взлом ArcelorMittal: реакция на решение компании закрыть две доменные печи, расположенные в бельгийском городе Льеж.[19]
- DDoS-атака на Ватикан: атака, направленная не против католиков в разных странах мира, а против «коррумпированной» церкви.[20]
- Дистрибутив Anonymous-OS на основе Linux сразу после выхода был объявлен подделкой.[21]

Об авторах отчета

подготовке и написании данного отчета принимали участие сотрудники McAfee Labs Чжэн Бу (Zheng Bu), Адам Восотовски (Adam Wosotowsky), Паула Греве (Paula Greve), Торальв Дирро (Toralv Dirro), Йичонг Линь (Yichong Lin), Дэвид Маркус (David Marcus), Франсуа Паже (François Paget), Питер Сзор (Peter Szor), Дэн Соммер (Dan Sommer), Джимми Ша (Jimmy Shah) и Крейг Шмугар (Craig Schmugar).

О лаборатории McAfee Labs

McAfee Labs — это глобальная исследовательская группа McAfee. Являясь единственной организацией, занимающейся всеми направлениями угроз, включая вредоносные программы, веб-угрозы, угрозы электронной почте, сетевые угрозы и уязвимости, McAfee Labs собирает информацию посредством миллионов датчиков и «облачной» технологии McAfee Global Threat Intelligence™. Группа McAfee Labs, насчитывающая 350 исследователей различных профилей из 30 стран, отслеживает весь спектр угроз в реальном времени, выявляя уязвимости приложений, выполняя анализ и корреляцию рисков, что позволяет выполнять мгновенные исправления с целью защиты корпоративных и частных пользователей.

О компании McAfee

McAfee — стопроцентная дочерняя компания Intel Corporation (NASDAQ: INTC), является крупнейшим в мире предприятием, специализирующейся на технологиях информационной безопасности. Компания McAfee поставляет проверенные упреждающие решения и услуги, которые обеспечивают безопасность систем, сетей и мобильных устройств по всему миру, позволяя пользователям безопасно работать и совершать покупки в Интернете. Наличие непревзойденной технологии Global Threat Intelligence, позволяет компании McAfee создавать инновационные продукты, которые помогают частным пользователям, компаниям, государственным организациям и поставщикам услуг Интернета обеспечивать соответствие нормативно-правовым требованиям, защищать данные, предотвращать нарушения работы, определять уязвимости, а также постоянно следить за уровнем собственной безопасности и повышать его. Компания McAfee непрерывно ведет постоянный поиск новых путей защиты своих клиентов. www.mcafee.com/ru

[1] http://blogs.mcafee.com/mcafee-labs/signed-malware-you-can-runbut-you-cant-hide
[2] http://www.mcafee.com/ru/resources/reports/rp-threat-predictions-2012.pdf
[3] http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html
[4] http://www.kahusecurity.com/
[5] http://krebsonsecurity.com/2012/01/citadel-trojan-touts-trouble-ticket-system/
[6] http://blogs.technet.com/b/microsoft_blog/archive/2012/01/23/microsoft-names-new-defendant-in-kelihos-case.aspx
[7] http://krebsonsecurity.com/2012/01/microsoft-worm-author-worked-at-antivirus-firm/
[8] http://en.gazeta.ru/news/2012/03/07/a_4030561.shtml
[9] http://www.justice.gov/usao/nys/pressreleases/January12/zdoroveninvladimirandzdoroveninkirillindictmentpr.pdf
[10] http://www.secretservice.gov/press/GPA03-12_OpenMarket2.pdf
[11] http://garwarner.blogspot.fr/2012/03/russian-mvd-announces-arrest-of-carberp.html
[12] http://www.huffingtonpost.com/2012/03/05/michael-jackson-hacking-james-marks-james-mccormick_n_1321912.html
[13] http://www.smashtheman.com/2012/03/news/the-legal-attack-against-anonymous-and-lulzsec
[14] http://www.interpol.int/News-and-media/News-media-releases/2012/PR014
[15] http://blogs.mcafee.com/mcafee-labs/hacker-leaves-online-trail-loses-anonymity
[16] http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html
[17] http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html
[18] http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx
[19] http://www.cyberguerrilla.info/?p=3747
[20] http://geeks.thedailywh.at/2012/03/07/geek-news-anonymous-vatican-hack-of-the-day/
[21] http://www.tomshardware.com/news/Anonymous-Anonymous-OS-Viruses-Trojans-Fake,15027.html

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

44605rpt_quarterly-threat-q1_0512_fnl_ETMG