KASPERSKY SECURITY BULLETIN 2013

KASPERSKY LAB
GLOBAL RESEARCH
AND ANALYSIS TEAM
(GREAT)

KASPERSKY lab

СОДЕРЖАНИЕ

РАЗВИТИЕ УГРОЗ В 2013 ГОДУ 4

> 1. Новые старые кампании по кибершпионажу 5
> 2. Кибернаемники: новая тенденция 8
> 3. Хактивизм и утечка данных 9
> 4. Кибервымогательство 10
> 5. Зловреды для мобильных устройств и (без)опасность магазинов приложений . . 12
> 6. Атаки типа watering hole 14
> 7. Самое слабое звено в цепочке безопасности 16
> 8. Нарушение тайны частной жизни и утрата доверия: Lavabit, Silent Circle, NSA 17
> 9. Уязвимости и эксплойты нулевого дня 19
> 10. Взлеты и падения криптовалют: биткойны правят миром 21
> Выводы и прогнозы: 2014 год — «год доверия» 23

КОРПОРАТИВНЫЕ УГРОЗЫ 24

> Зачем атакуют 25
> Организации-мишени 26
> Подготовка атаки 26
> Методы проникновения 27
> Уязвимости и эксплойты 29
> Технологии 30
> Что крадут 32
> Новая тенденция: кибернаемники 32
> Последствия громких разоблачений 33

ОСНОВНАЯ СТАТИСТИКА ЗА 2013 ГОД 34

> Цифры года 34
> Мобильные угрозы 35
> Уязвимые приложения, используемые злоумышленниками 40
> Вредоносные программы в интернете (атаки через Web) 42
> Локальные угрозы 48

ПРОГНОЗЫ 54
> Мобильные угрозы 54
> Защита тайны частной жизни 55
> Атаки на облачные хранилища 56
> Атаки на разработчиков ПО 56
> Кибернаемники 57
> Фрагментация интернета 57
> Пирамида киберугроз 58

РАЗВИТИЕ УГРОЗ В 2013 ГОДУ

Костин Раю, Дэвид Эмм

И снова пришло время для публикации нашего традиционного обзора ключевых событий, ставших определяющими для ситуации в области IT-безопасности в 2013 году. Но давайте сначала вспомним, что, согласно нашему прогнозу, составленному на основе тенденций предыдущего года, должно было определять ситуацию в 2013 году.

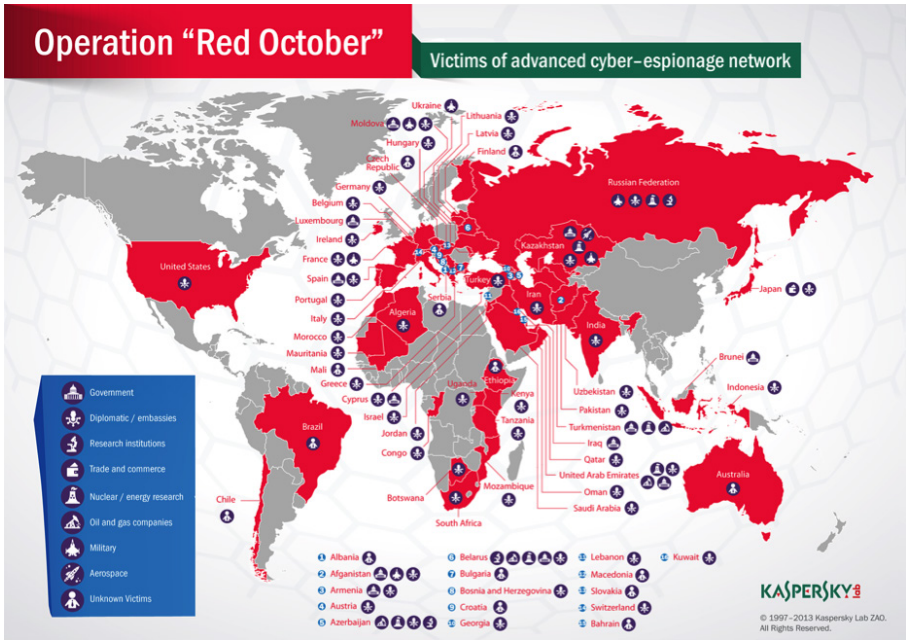
- Целевые атаки и кибершпионаж
- Наступление «хактивистов»
- Кибератаки, финансируемые государствами
- Использование средств слежения правоохранительными органами
- Облачно, вероятны вредоносные атаки
- Уязвимости и эксплойты
- Кибервымогательство
- Кому верить?
- Зловреды для Mac OS
- Мобильные зловреды
- Кто украл мою частную жизнь?!

Теперь перейдем к наиболее заметным событиям и явлениям 2013 года. Вы можете сами решить, насколько точно нам удалось предсказать будущее.

Вот наша десятка важнейших инцидентов IT-безопасности в 2013 году.

1. НОВЫЕ СТАРЫЕ КАМПАНИИ ПО КИБЕРШПИОНАЖУ

Читатель может полагать, что, заглянув в ретроспективный обзор громких инцидентов 2013 года, он прочтет о событиях, которые произошли в этом году. Но с целевыми атаками не все так просто. Часто такие кампании берут свое начало гораздо раньше, чем о них узнают, анализируют и пишут отчеты. Возможно, вы вспомните, что так было со Stuxnet — чем больше мы исследовали его, тем больше назад отодвигалась нами дата его появления. Это верно и для большинства кампаний по кибершпионажу этого года.



Карта жертв Red October

Red October — кампания по кибершпионажу, нанесшая ущерб сотням жертв по всему миру, в том числе дипломатическим организациям и правительственным учреждениям, исследовательским институтам, компаниям, занимающимся энергетикой, в том числе ядерной, а также торговым организациям и организациям авиакосмической промышленности. Вредоносное ПО оказалось невероятно сложным: помимо прочего, зловред оснащен «модулем воскрешения», благодаря которому способен заново заражать компьютеры. Код имеет модульную систему, что позволяет злоумышленникам легко подстроить его под определенную цель.

Интересно, что Red October собирает информацию не только с компьютеров, но и с мобильных устройств, подключенных к сети жертв. Это показывает, что злоумышленники признали мобильные устройства ключевым компонентом современной бизнес-среды и носителем важной информации. Мы опубликовали результаты анализа в январе 2013 года, но совершенно ясно, что кампания началась в 2008-м.

В феврале мы опубликовали анализ вредоносного ПО MiniDuke, разработанного для кражи данных из органов государственной власти и исследовательских институтов. По результатам нашего анализа, жертвами зловреда стали 59 известных организаций в 23 странах, в том числе на Украине, в Бельгии, Португалии, Румынии, Чехии, Ирландии, Венгрии и США. Как многие целевые атаки, MiniDuke сочетал использование социальной инженерии — тактики старой школы, и современных сложных технологий. Например, MiniDuke содержал первый эксплойт, способный обходить песочницу Adobe Acrobat Reader. К тому же, зараженные машины получали команды с командного сервера через аккаунты Twitter, указанные заранее (а в качестве запасного варианта искали эти аккаунты в Google).

В марте мы узнали о серии атак, нацеленных на крупных политиков и правозащитников в странах СНГ и Восточной Европы. Для получения контроля над компьютерами жертв злоумышленники использовали инструмент удаленного администрирования TeamViewer, поэтому операция получила название «TeamSpy». Целью этих атак был сбор информации с взломанных компьютеров. Пусть и не настолько сложная, как Red October, NetTraveler и другие, эта кампания стала не менее успешной, доказав, что не все целевые атаки требуют создания кода с нуля.

О NetTraveler, также известном как NetFile, мы сообщили в июне, и это еще одна угроза, которая уже проявляла активность к моменту обнаружения — в этом случае, с 2004 года.

Эта кампания была разработана для кражи информации, относящейся к исследованию космоса, нанотехнологиям, ядерной энергетике, производству энергии, лазерам, медицине и телекоммуникациям. NetTraveler успешно применили для взлома свыше

650 организаций в 40 странах, в том числе в Монголии, России, Индии, Казахстане, Кыргызстане, Китае, Таджикистане, Южной Корее, Испании и Германии. Жертвами стали государственные и частные организации, в том числе правительственные учреждения, посольства, нефтяные и газовые компании, исследовательские центры, оборонные предприятия и организации Тибетских и Уйгурских активистов.

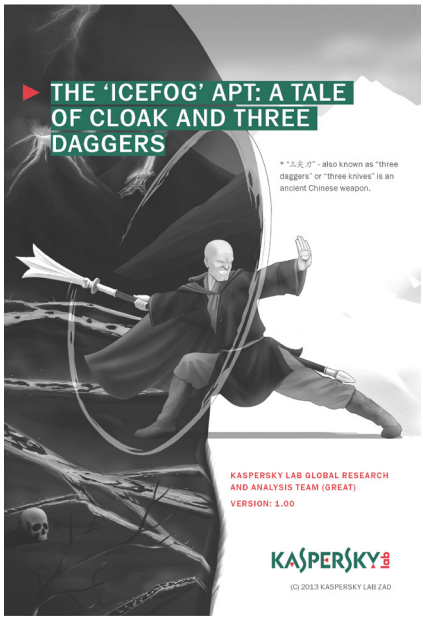
Если ваша компания еще не стала жертвой атаки, очень легко убедить себя в том, что с вами этого не случится, или представить, что большее из того, что мы слышим о вредоносном ПО, - всего лишь рекламный трюк. Прочитав заголовки, легко прийти к выводу, что целевые атаки — это проблема исключительно крупных организаций. Однако не все атаки нацелены на известные имена или на организации, занятые в проектах критически важных отраслей. На самом деле любая организация может стать жертвой злоумышленников. Каждая компания владеет информацией, которая представляет ценность для злоумышленников или может быть использована как мостик на пути к другим жертвам. Это ярко продемонстрировали атаки Winnti и Icefog.

В апреле мы опубликовали отчет о деятельности киберпреступной группировки Winnti, которая с 2009 года специализируется на краже цифровых сертификатов, подписанных легитимными разработчиками ПО, а также занимается кражей интеллектуальной собственности (в том числе кражей исходного кода онлайн-игр). Троянец, который использовала группа, представляет собой DLL-библиотеку для 64-битной среды Windows. Вредоносное ПО использует легитимно подписанный драйвер и работает как полноценный инструмент удаленного администрирования — так злоумышленники получали полный контроль над взломанным компьютером. В общей сложности мы обнаружили свыше 30 компаний, работающих в сфере онлайн-игр и пострадавших от действий группировки — большинство из них находятся в Юго-Восточной Азии, но также встречаются компании из Германии, США, Японии, России, Бразилии, Перу, Белоруссии и Великобритании. В настоящий момент группировка по-прежнему активна.

Атаки Icefog, о которых мы писали в сентябре (подробное описание см. в следующем разделе этого отчета), были нацелены на цепи поставок и, помимо кражи ценной информации из взломанных сетей, служили средством для сбора логинов и паролей к почте и доступа к различным интернет-ресурсам.

2. КИБЕРНАЕМНИКИ: НОВАЯ ТЕНДЕНЦИЯ

На первый взгляд, Icefog — обычная целевая атака, каких много. Это кампания по кибершпионажу, действующая с 2011 года и ориентированная прежде всего на Южную Корею, Тайвань и Японию. Жертвы этой кампании есть также в США, Европе и Китае. Как и в других подобных кампаниях, для заражения жертв злоумышленники применяют целевые фишинговые рассылки (spear-phishing) электронных писем, содержащих вредоносные вложения или ссылки на вредоносные сайты. Как в любой подобной кампании, точно подсчитать количество жертв атак сложно, однако нам известно о нескольких десятках жертв, работающих под Windows, и более 350, использующих Mac OS X (последние большей частью находятся в Китае).



Тем не менее, Icefog имеет несколько ключевых отличий от других атак, о которых мы писали выше. Во-первых, эта кампания — пример нарождающейся тенденции, которую мы наблюдаем последнее время, — атак, проводимых быстро и с хирургической точностью малыми группами кибернаемников. Во-вторых, злоумышленники скрупулезно выбирали потенциальных жертв, среди которых — государственные учреждения, военные подрядчики, судоходные и судостроительные компании, телекоммуникационные компании, операторы спутниковой связи, промышленные и технологические компании и средства массовой информации. В-третьих, в ходе кампании широко применяются средства кибершпионажа собственной разработки для Windows и Mac OSX, причем злоумышленники напрямую управляют взломанными компьютерами. Кроме того, мы обнаружили, что в дополнение к Icefog атакующие применяют бэкдоры и другие вредоносные утилиты для заражения других компьютеров в сети организации-жертвы и для передачи краденных данных на свой сервер.

Китайская группа под названием Hidden Lynx, о чьей деятельности писали эксперты компании Symantec в сентябре, входит в ту же категорию — «наемники», которые осуществляют заказные

атаки с применением технически сложных средств, созданных для выполнения конкретных задач. На счету этой группы, в частности, атака на компанию Bit9 в начале этого года.

Мы прогнозируем появление новых подобных групп в будущем по мере формирования черного рынка «APT-услуг».

3. ХАКТИВИЗМ И УТЕЧКА ДАННЫХ

Кража денег — напрямую с банковских счетов или с помощью тоже краденых личных данных — не единственный мотив, который кроется за взломом систем защиты. Такие атаки также могут быть формой политического или социального протеста или же способом запятнать репутацию компании, на которую нацелена атака. Сегодня интернет участвует практически во всех областях нашей жизни. Для того, кто обладает определенными навыками, гораздо легче атаковать правительственный или коммерческий веб-сайт, чем организовать реальную акцию протеста или демонстрацию.

Для тех, кто преследует такие цели, хорошим оружием стали DDoS-атаки (атаки типа «отказ в обслуживании»). Одна из крупнейших DDoS-атак в истории (а некоторые скажут, что самая крупная) была направлена на организацию Spamhaus в марте этого года. По некоторым расчетам, в пиковый период интенсивность атаки достигала 300 Гбайт/с. Организация, предположительно начавшая атаку, называется Cyberpunker. Конфликт между ней и Spamhaus начался еще в 2011 году, но достиг апогея лишь за пару недель до атаки, когда Spamhaus внесла Cyberpunker в черный список. Владелец Cyberpunker отказался взять на себя ответственность за атаку, однако согласился выступить представителем атакующих. В любом случае атака была запущена кем-то, кто способен генерировать гигантские объемы трафика. Чтобы защитить себя от атаки, организация Spamhaus была вынуждена перенести свой сайт на хостинг провайдера услуг CloudFare, известного своей защитой от DDoS-атак.

Инцидент со Spamhaus, судя по всему, не был связан с другими инцидентами, однако он произошел на фоне продолжавшихся в этом году атак групп хактивистов. В том числе, атак Anonymous. В этом году они взяли на себя ответственность за атаки на министерство юстиции США, Массачусетский технологический институт и веб-сайты разных государств, включая Польшу, Грецию, Сингапур, Индонезию и Австралию (последние два инцидента не обошлись без перепалок между группами Anonymous, которые находятся в этих странах).

Anonymous также взяли на себя ответственность за взлом Wi-Fi сети британского парламента во время протестов на площади Парламента в первых числах ноября.

Активисты, причисляющие себя к «Сирийской электронной армии» (сторонники Сирийского президента Башара Ассада), в течение года также совершили несколько атак. Так, в апреле они взяли на себя ответственность за взлом аккаунта Associated Press в Twitter и размещение фальшивых сообщений о взрывах в Белом Доме — американскому индексу Dow Jones это обошлось в 136 млрд долларов. В июле группировка взломала Gmail-аккаунты трех служащих Белого Дома и аккаунт агентства Thomson Reuters в Twitter.

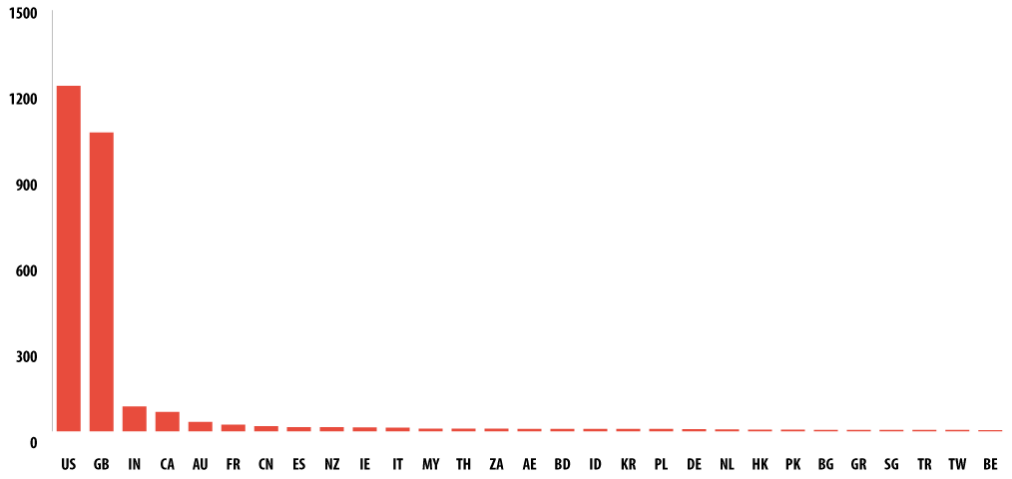
Очевидно, что наша зависимость от технологий, как и огромные вычислительные мощности, которыми обладают современные компьютеры, приводят к тому, что мы становимся потенциально уязвимы к атакам, цели которых весьма разнообразны. Поэтому маловероятно, что действиям хактивистов или кого угодно еще, кто заинтересован в проведении атак на всевозможные организации, когда-нибудь придет конец.

4. КИБЕРВЫМОГАТЕЛЬСТВО

Методы, к которым прибегают киберпреступники, чтобы заработать на своих жертвах, далеко не всегда отличаются утонченностью. Так называемые программы-вымогатели (Ransomware) по сути представляют собой DOS-атаки на отдельно взятый компьютер — они блокируют доступ к его файловой системе или шифруют данные на жестком диске. Особенности поведения таких программ могут различаться. Например, там, где распространено компьютерное пиратство, троянец-вымогатель может выводить на экран сообщение о якобы обнаруженном на машине нелицензионном ПО и требовать плату за возвращение пользователю доступа к компьютеру. В других регионах требования маскируются под всплывающие сообщения полиции об обнаружении на компьютере детской порнографии или иного запрещенного контента, за который пользователь должен заплатить штраф. Но зачастую злоумышленники вовсе не прибегают ни к каким уловкам — они просто зашифровывают данные и сообщают пользователю, что для их восстановления необходимо заплатить. Таков, например, троянец Cryptolocker, который мы проанализировали в октябре.

Cryptolocker устанавливает соединение с командным сервером и загружает с него открытый ключ RSA, с помощью которого шифрует данные. Для каждой новой жертвы создается новый

уникальный ключ, а доступ к закрытым ключам, необходимым для расшифровки файлов, имеют только авторы. Для соединения с командным сервером Cryptolocker использует алгоритм генерации доменных имен, создающий 1000 уникальных имен-кандидатов в сутки. Злоумышленники требуют, чтобы пользователь заплатил им в течение примерно трех дней — устрашающие обои, устанавливаемые на зараженной машине, предупреждают, что в противном случае данные будут безвозвратно утрачены. Предлагаются различные способы оплаты, в том числе с использованием виртуальной валюты Bitcoin. Больше всего жертв в США и Великобритании, за которыми следуют (с большим отставанием) Индия, Канада и Австралия.



Проблема здесь связана не столько с трудностями удаления вредоносного приложения или даже восстановления зараженного компьютера, сколько с возможной утратой данных. В прошлом нам в некоторых случаях удавалось расшифровать «угнанные» данные пользователей. Однако в случае если используется очень мощное шифрование, это не представляется возможным. Такое шифрование применено, например, в некоторых вариантах троянца Gpcode. В Cryptolocker также используется очень мощный шифр. Поэтому как отдельным пользователям, так и организациям любого масштаба просто необходимо регулярно делать резервные копии своих данных, чтобы в случае потери данных — по какой бы то ни было причине — неприятность не стала катастрофой.

Cryptolocker — не единственная программа-вымогатель, попавшая в этом году в заголовки новостей. В июне мы столкнулись с приложением для Android под названием Free Calls Update — фальшивым антивирусом, запугивающим пользователей, чтобы убедить их заплатить за удаление с их устройств несуществующего вредоносного ПО. После установки на устройстве приложение пытается получить права администратора — это дает ему возможность включать и выключать Wi-Fi и 3G, а также не позволяет пользователю легко удалить вредоносное приложение с устройства. Установочный файл вредоносного приложения удаляется с целью предотвратить обнаружение со стороны легитимного антивирусного ПО, если пользователь решит его установить. Приложение выдает ложные сообщения об обнаружении вредоносных программ и предлагает пользователю приобрести лицензию на полную версию, которая якобы их удалит. При посещении пользователем веб-страниц приложение во всплывающем окошке сообщает ему, что вредоносная программа пытается украсть с телефона порнографический контент. Это окошко появляется постоянно и мешает работе с устройством.

5. ВРЕДОНОСНОЕ ПО ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ И (БЕЗ)ОПАСНОСТЬ МАГАЗИНОВ ПРИЛОЖЕНИЙ

Стремительный рост количества вредоносного ПО для мобильных платформ, который начался в 2011-м, продолжился и в этом году. На сегодняшний день существует свыше 148 тысяч модификаций мобильных вредоносных программ, образующих 777 семейств. Как и в прошлые годы, подавляющее большинство из них — 98,05% всех обнаруженных вредоносных приложений — нацелены на устройства на базе Android. И в этом нет ничего удивительного. Эта платформа отвечает всем требованиям злоумышленников: она популярна, для нее легко разработать приложение, а пользователи устройств на базе Android могут скачивать приложения (в том числе и вредоносные) откуда угодно. Последний фактор очень важен: злоумышленники активно используют тот факт, что пользователи загружают приложения из Google Play, а также из других онлайн-магазинов или с веб-сайтов. Это также позволяет злоумышленникам создавать поддельные сайты, замаскированные под легитимные магазины приложений. Поэтому спада в области разработки вредоносного ПО для Android в ближайшее время ожидать не приходится.

Виды вредоносного ПО, нацеленного на мобильные устройства, практически полностью повторяют виды зловредов, которые чаще всего заражают компьютеры и ноутбуки — это бэкдоры, троянцы и троянцы-шпионы. Единственным исключением являются SMS-троянцы, разрабатываемые специально для смартфонов.

При этом растет не только количество зловредов: мы также наблюдаем повышение сложности вредоносного ПО. В июне мы проанализировали Obad — самый сложный мобильный троянец на сегодняшний день. Это многофункциональная угроза: Obad отправляет SMS-сообщения на платные номера, загружает и устанавливает другие вредоносные программы, использует Bluetooth для распространения на другие устройства, а также удаленно выполняет команды с консоли. Кроме того, этот троянец очень сложен, его код сильно обфусцирован и он использует три ранее неизвестные уязвимости, причем одна из них позволяет троянцу получать на устройстве расширенные права администратора, но при этом не попадать в список приложений, имеющих такие привилегии. Это не позволяет пользователю просто удалить программу с устройства. Obad также может заблокировать экран — не больше, чем на 10 секунд, однако этого достаточно, чтобы троянец успел отправить свою копию (и другое вредоносное ПО) на находящиеся поблизости устройства. Этот трюк придуман для того, чтобы владелец смартфона не заметил активность зловреда.

Obad использует различные методы распространения. Мы уже упомянули Bluetooth, но троянец также распространяется через поддельный магазин Google Play, посредством SMS-спама и за счет перенаправления пользователей со взломанных сайтов. Кроме того, Obad может быть установлен в системе другим мобильным троянцем — Opfake.

Киберпреступники, стоящие за Obad, могут управлять троянцем с помощью заранее заданных строк, передаваемых в SMS-сообщениях. Список действий, которые может выполнять зловред, включает отправку SMS-сообщений и ping-запросов на определенные ресурсы, функционирование в качестве прокси-сервера, соединение с определенными адресами, загрузку и установку определенных файлов, отправку списка установленных на устройстве приложений, отправку информации об определенных приложениях, отправку контактов жертвы на сервер и выполнение команд, полученных с сервера.

Троянец собирает данные с устройства и отсылает их на командный сервер — в том числе MAC-адрес устройства, имя устройства, номер IMEI, баланс счета, местное время и

информацию о том, удалось ли зловреду получить права администратора устройства или нет. Все эти данные загружаются на командный сервер: сначала троянец пробует использовать активное интернет-соединение, а если его нет, ищет ближайшую точку доступа Wi-Fi, не требующую авторизации.

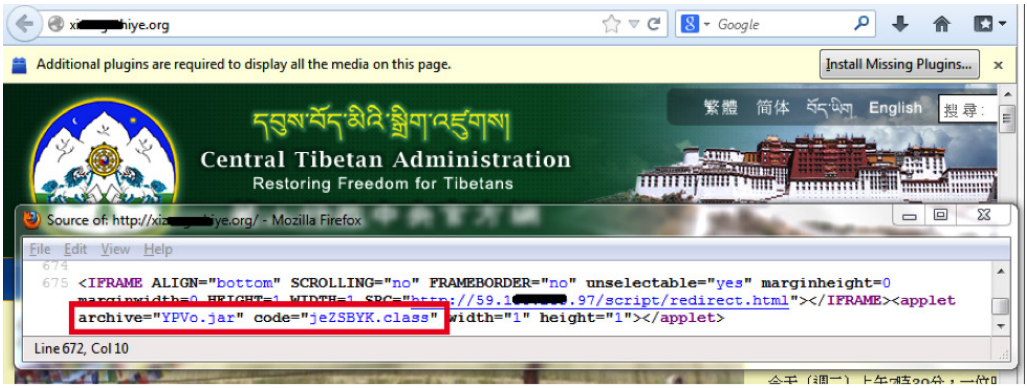
6. АТАКИ ТИПА WATERING HOLE

Возможно, вам знакомы термины «drive-by загрузка» и «целевой фишинг». В первом случае киберпреступники находят незащищенные веб-сайты и внедряют вредоносный скрипт в HTTP- или PHP-код одной из страниц. Этот скрипт может непосредственно устанавливать вредоносные программы на компьютер посетителя сайта или использовать IFRAME, чтобы перенаправлять жертву на вредоносный сайт. Второй вариант представляет собой направленную форму фишинга, часто применяемую в качестве отправной точки для целевой атаки. Определенному человеку в организации-мишени отправляется электронное письмо в расчете на то, что он откроет ссылку или приложение, которые запустят вредоносный код и помогут преступникам проникнуть в корпоративную сеть.

Если объединить эти два подхода (drive-by загрузку и целевой фишинг), то получится так называемая атака типа watering hole. Киберпреступники изучают поведение людей, которые работают в интересующей их организации, чтобы узнать, какие интернет-ресурсы они чаще всего посещают. Затем злоумышленники заражают веб-сайт, пользующийся у сотрудников популярностью — желательно такой, который принадлежит доверенной организации и служит ценным источником информации. В классическом варианте атаки применяется эксплойт нулевого дня. Когда сотрудник открывает страницу этого сайта, его компьютер подвергается заражению: как правило, на него устанавливается троянская программа-бэкдор, позволяющая злоумышленникам получить доступ к внутренней сети компании. Это очень похоже на подкарауливание жертвы у водопоя (watering hole), когда вместо того, чтобы выслеживать добычу, хищник ждет в засаде в таком месте, куда потенциальная жертва наверняка придет сама.

В этом году атаки типа watering hole пользуются у киберпреступников большим успехом. Сразу после нашего сообщения об атаках Winnti мы обнаружили экслойт для Flash Player на сайте попечительского фонда Tibetan Homes Foundation, который поддерживает детей-беженцев из Тибета. Выяснилось, что этот сайт был взломан с целью распространения бэкдоров,

подписанных сертификатами, которые ранее использовались в кампании Winnti. Это классический пример атаки типа watering hole: преступники изучили интернет-предпочтения своих жертв и взломали соответствующие сайты для того, чтобы таким путем заразить их компьютеры. Та же методика была применена в августе, когда вредоносный код на сайте Правительства Тибета в изгнании перенаправлял посетителей, использующих язык CN (упрощенный китайский), на ресурс с Java-эксплойтом, загружавший на их компьютеры бэкдор, предназначенный для проведения целевых атак.



В сентябре нами были зарегистрированы новые атаки типа watering hole, направленные на эти группы в рамках кампании NetTraveler.

Важно отметить, что атаки типа watering hole являются лишь одним из приемов, применяемых преступниками наряду с целевым фишингом и другими видами атак. Описанные выше заражения являются частью кампании, направленной против тибетских и уйгурских сайтов, которая продолжается уже более двух лет.

И наконец, все эти случаи — еще одно доказательство того, что мишенью целевой атаки может стать практически любая организация, а не только международная корпорация или другая солидная структура.

7. САМОЕ СЛАБОЕ ЗВЕНО В ЦЕПОЧКЕ БЕЗОПАСНОСТИ

Многие современные угрозы чрезвычайно сложны. Особенно это касается целевых атак, для осуществления которых преступники создают специальные эксплойты, использующие незакрытые уязвимости в приложениях, или разрабатывают специализированные модули, помогающие им похищать данные своих жертв. Однако часто самой главной уязвимостью, которую эксплуатируют злоумышленники, является человеческий фактор. Злоумышленники применяют методы социальной инженерии, чтобы ввести в заблуждение сотрудников организации и вынудить их совершить действия, ставящие под угрозу корпоративную безопасность. Люди попадаются на эти уловки по разным причинам: иногда они просто не осознают опасность; иногда поддаются на заманчивые предложения получить «бесплатный сыр»; а иногда идут в обход правил, чтобы облегчить себе жизнь — например, используют один пароль на все случаи жизни.

Многие нашумевшие целевые атаки, которые мы анализировали в этом году, начались именно с эксплуатации человеческого фактора. В Red October, серии целевых атак на тибетских и уйгурских активистов, в MiniDuke, NetTraveler и Icefog для получения первоначального доступа к корпоративным сетям организаций-мишеней использовался целевой фишинг. Киберпреступники ищут подход к сотрудникам этих организаций, используя данные, которые удается собрать на официальном сайте компании, на открытых форумах, а также путем тщательного анализа информации, которую люди размещают в социальных сетях. Все это помогает преступникам создавать электронные сообщения, которые не вызывают подозрений и застают людей врасплох.

Этот же подход используют и организаторы массовых атак с применением социальной инженерии, в ходе которых фишинговые сообщения рассылаются большому числу случайных пользователей.

Социальная инженерия применяется и в реальной жизни, причем этот аспект безопасности часто упускают из виду. Он громко напомнил о себе в этом году, когда преступники попытались установить KVM-переключатели в филиалах двух британских банков. В обоих случаях злоумышленники представлялись сотрудниками инженерной службы и пытались получить физический доступ в банк, чтобы установить там оборудование, которое позволило бы им отслеживать сетевую активность организации. Подробнее об этих инцидентах можно прочитать здесь и здесь.

Эта же тема привлекла внимание нашего коллеги Дэвида Джэкоби (David Jacoby): в сентябре он провел небольшой эксперимент в Стокгольме с целью выяснить, насколько легко можно получить доступ к информационным системам компаний, эксплуатируя готовность персонала помочь человеку, попавшему в затруднительное положение. Отчет Дэвида вы можете прочитать здесь.

К сожалению, в компаниях часто недооценивают значение человеческого фактора в вопросах безопасности. Даже в том случае, когда информирование персонала об информационных угрозах признается необходимым, используемые для этого методы часто оказываются неэффективными. Однако те, кто игнорируют данный аспект безопасности, делают это на свой страх и риск, поскольку совершенно очевидно, что технологии сами по себе не могут гарантировать полную защиту корпоративной сети. Поэтому крайне важно, чтобы во всех организациях знание и соблюдение мер безопасности персоналом стало неотъемлемой частью стратегии защиты корпоративной сети.

8. НАРУШЕНИЕ ТАЙНЫ ЧАСТНОЙ ЖИЗНИ И УТРАТА ДОВЕРИЯ: LAVABIT, SILENT CIRCLE, NSA

Обзор информационных угроз 2013 года не может считаться полным без упоминания Эдварда Сноудена и широких последствий для тайны частной жизни, которые повлекла за собой публикация сведений о Prism, XKeyscore, Tempora и других программах слежки за гражданами.

Вероятно, одним из наиболее заметных последствий публикации этой информации стало закрытие сервиса по обмену зашифрованными электронными письмами Lavabit. Мы писали об этом сервисе здесь. Еще один провайдер услуг шифрования почты — Silent Circle — также решил прекратить свою работу, что оставило пользователям весьма ограниченный выбор возможностей для безопасного обмена личными электронными письмами. Причина, по которой эти два сервиса прекратили свое существование, — невозможность предоставлять подобные услуги в условиях давления со стороны правоохранительных органов и других государственных структур.

Еще один сюжет, существенно повлиявший на ситуацию в области тайны частной жизни, – компрометация Агентством национальной безопасности США (National Security Agency, NSA)

алгоритмов эллиптической криптографии, принятых Национальным институтом стандартов и технологий США (National Institute of Standards and Technology, NIST). По-видимому, NSA внедрило своеобразный «бэкдор» в алгоритм, известный под названием Dual Elliptic Curve Deterministic Random Bit Generation (Dual EC DRBG). По некоторым сведениям, «бэкдор» позволяет определенным сторонам с легкостью взламывать данный протокол шифрования, внедряясь таким образом в канал связи, который считается безопасным. Компания RSA, один из крупнейших мировых разработчиков систем шифрования, заявила, что этот алгоритм применяется по умолчанию в одном из предлагаемых ею пакетов средств шифрования, и рекомендовала всем своим клиентам прекратить его использование. Данный алгоритм был одобрен NIST в 2006 году, но был доступен и широко применялся как минимум с 2004 года.

Любопытно, что один из широко обсуждаемых инцидентов имеет непосредственное отношение к антивирусной отрасли. В сентябре бельгийская телекоммуникационная компания Belgacom заявила о взломе ее сети. В ходе плановой проверки сотрудники Belgacom обнаружили на нескольких серверах и компьютерах сотрудников неизвестный вирус. Позднее были озвучены предположения, которые указывали на NSA и его британский аналог GCHQ (Government Communications Headquarters) как на возможный источник заражения и самого вируса. Несмотря на то, что компании антивирусной индустрии не получили образцы данного вредоносного ПО, появились новые сведения, согласно которым атака была осуществлена через модифицированные страницы LinkedIn, в которые при помощи технологии man-in-the-middle (MITM) вставлялись ссылки на сервера с эксплойтами.

Все эти инциденты, связанные со слежкой и шпионажем, породили вопросы о том, насколько активно компании индустрии IT-безопасности сотрудничают с государственными структурами. Фонд EFF (Electronic Frontier Foundation) совместно с другими организациями опубликовал 25 октября 2013 года открытое письмо, в котором антивирусным компаниям был задан ряд вопросов относительно обнаружения и нейтрализации вредоносных программ, создаваемых и распространяемых при участии государственных структур.

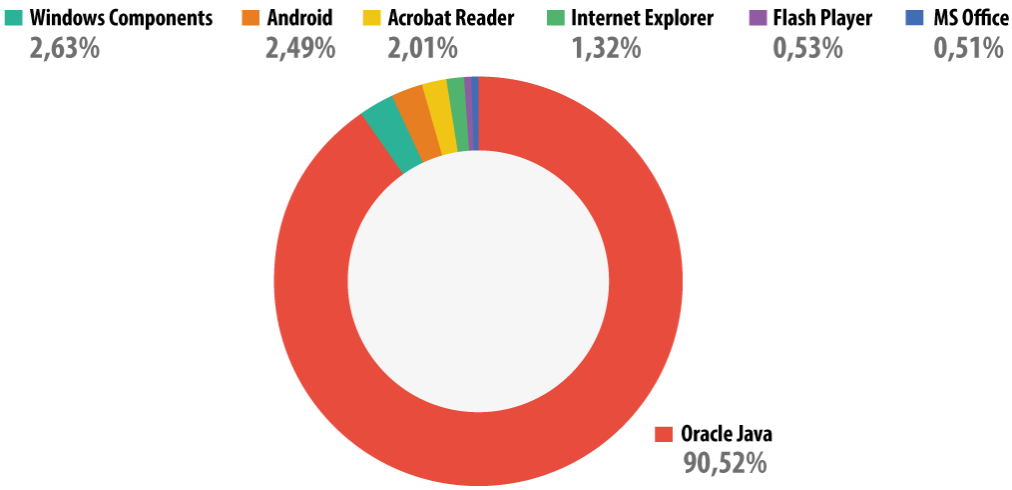
Что касается «Лаборатории Касперского», то у нас очень простая и однозначная позиция относительно обнаружения вредоносного ПО: мы делаем все возможное для обнаружения и нейтрализации любых атак с применением вредоносного ПО, независимо от их источника или целей. Для нас не существует «правильных» или «неправильных» вредоносных программ. Наша команда экспертов активно участвовала в обнаружении и анализе нескольких вредоносных

атак, к которым были причастны государственные структуры и государства. В 2012 году мы опубликовали подробный отчет об анализе вредоносных программ Flame и Gauss, входящих в число крупнейших среди известных на сегодняшний день кампаний кибершпионажа, проводимых на государственном уровне. Мы также публиковали предупреждения об опасности так называемых «легальных» средств слежки, таких как DaVinci (HackingTeam) и FinFisher (Gamma). Крайне важно, чтобы эти инструменты слежения не попали в плохие руки, — именно поэтому индустрия IT-безопасности не может делать исключений в том, что касается обнаружения вредоносного ПО. В действительности, крайне маловероятно, что государственная организация, обладающая серьезным интеллектуальным и человеческим потенциалом, станет обращаться к разработчику (или разработчикам) антивирусов с просьбой воздержаться от обнаружения определенных вредоносных программ, созданных при поддержке государства. Такое «привилегированное» вредоносное ПО вполне может попасть не в те руки и быть применено в том числе и против тех, кто его создал.

9. УЯЗВИМОСТИ И ЭКСПЛОЙТЫ НУЛЕВОГО ДНЯ

Киберпреступники продолжают широко использовать уязвимости в легитимном ПО для проведения вредоносных атак. Они делают это с помощью эксплойтов — фрагментов кода, разработанного специально для эксплуатации уязвимостей в ПО с целью установки вредоносных программ на компьютер без ведома пользователя. Такой вредоносный код может содержаться в специально созданном вложении в электронном письме или эксплуатировать уязвимость в браузере.

Если злоумышленник эксплуатирует уязвимость, известную только ему (так называемая уязвимость нулевого дня), то всякий, кто использует уязвимое приложение, остается беззащитным до тех пор, пока не будет выпущен патч для закрытия бреши в этом приложении. Однако очень часто преступники используют известные уязвимости, для которых «заплатки» уже давно существуют. Эксплойты для давно известных уязвимостей успешно применялись в ходе многих крупных целевых атак 2013 года, включая Red October, MiniDuke, TeamSpy и NetTraveler, а также большого числа атак с применением социальной инженерии, нацеленных на неопределенную аудиторию и составляющих основную массу всех киберпреступлений.



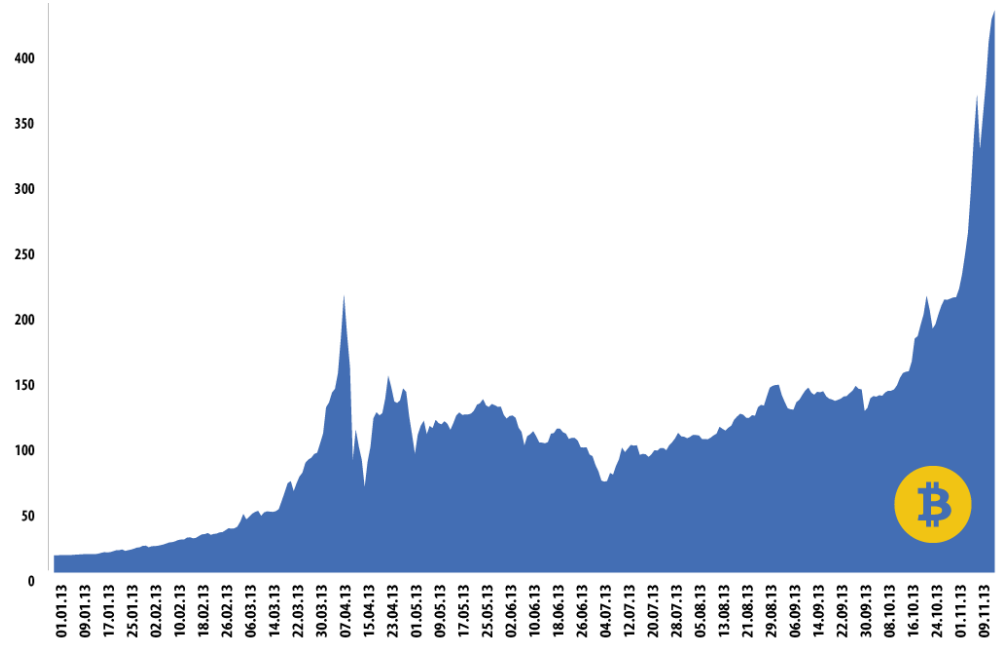
Злоумышленники предпочитают использовать уязвимости в наиболее популярных приложениях, которые пользователи по тем или иным причинам редко обновляют. Это дает преступникам широкие возможности для достижения своих целей. Так, в 2013 году через уязвимости в Java-приложениях было совершено 90,52% всех атак, а через уязвимости в Adobe Acrobat Reader — 2,01%. Это служит продолжением установившейся тенденции и не является сюрпризом. Java присутствует на огромном количестве компьютеров (по данным Oracle, на 3 миллиардах машин), а ее обновления не устанавливаются автоматически. Киберпреступники также продолжают эксплуатировать уязвимости в Adobe Reader, хотя за последние 12 месяцев количество атак существенно сократилось. Это связано с тем, что обновления для Adobe Reader стали выпускаться чаще, а в последней версии они к тому же устанавливаются автоматически.

Для минимизации рисков IT-безопасности компаниям необходимо использовать самые последние версии всего программного обеспечения, имеющегося на компьютерах корпоративной сети, устанавливать обновления безопасности по мере их появления и удалять ПО, которое больше не требуется для работы. Также можно использовать специальный сканер, позволяющий выявлять приложения с незакрытыми уязвимостями, или установить защитное решение, блокирующее попытки эксплуатации этих уязвимостей со стороны вредоносного ПО.

10. ВЗЛЕТЫ И ПАДЕНИЯ КРИПТОВАЛЮТ: БИТКОЙНЫ ПРАВЯТ МИРОМ

В 2009 году некий Сатоси Накамото (Satoshi Nakamoto) опубликовал доклад, которому суждено было произвести революцию в мире электронных валют. Документ под названием “Bitcoin: A Peer-to-Peer Electronic Cash System” (Bitcoin: P2P-система электронных денег) определял основную структуру распределенной децентрализованной системы платежей, не предусматривающей платы за проведение транзакций. Система Bitcoin была реализована, люди начали ею пользоваться. Поначалу это были математики и энтузиасты новой виртуальной платежной системы, но вскоре к ним присоединились обычные пользователи, а также киберпреступники и террористы.

Еще в январе 2013 года стоимость одного биткойна составляла $13. Однако по мере того, как все новые сервисы начинали принимать биткойны в качестве средства платежа, стоимость электронной валюты росла. Наконец, 9 апреля 2013 г. она превысила 260 долларов (средняя стоимость составляла $214), а на следующий день обрушилась, потому что владельцы большого количества биткойнов начали обменивать виртуальные деньги на реальные.



Обменный курс Bitcoin/USD на Mt.Gox, 2013

В ноябре 2013 г. биткойн снова начал набирать силу, достигнув отметки $400 и устремившись к $450, а может быть, и к более высоким значениям.

Почему же биткойны пользуются такой популярностью? Прежде всего, это почти анонимное и при этом безопасное платежное средство. Нет ничего удивительного, что на поднявшейся в 2013 году волне разоблачения государственной слежки пользователи пытаются найти альтернативные способы осуществления платежей. Кроме того, эта виртуальная валюта пользуется большим успехом у киберпреступников, которые ищут возможности скрыться из поля зрения правоохранительных органов.

В мае мы писали о бразильских киберпреступниках, создающих фишинговые сайты, замаскированные под биржи Bitcoin. Кроме того, появились специализированные ботнеты по добыче биткойнов, а также вредоносные программы, предназначенные для кражи кошельков Bitcoin.

25 октября в ходе совместной операции ФБР и Управления США по борьбе с наркотиками был закрыт печально известный сайт Silkroad. Согласно пресс-релизу, распространенному генеральной прокуратурой США, Silk Road («Шелковый путь») — это «скрытый веб-сайт, позволяющий пользователям покупать и продавать запрещенные наркотики и другие незаконные товары и услуги — анонимно и без риска быть пойманным правоохранительными органами». Сайт использовал в качестве средства оплаты биткойны, что позволяло как продавцам, так и покупателям оставаться неизвестными. ФБР и Управление по борьбе с наркотиками изъяли у владельца Silkroad, известного как Dread Pirate Roberts («Страшный пират Робертс»), около 140 тыс. биткойнов (по нынешним ценам порядка 56 млн. долларов). Оборот сайта, который открылся в 2011 году и был доступен только через сеть TOR Onion, достиг 9,5 млн. биткойнов.

Очевидно, что киберпреступники нашли для себя в Bitcoin тихую гавань, однако у этой платежной системы есть множество других пользователей, не преследующих незаконные цели. Сервис становится все более популярным, и было бы любопытно узнать, следует ли ожидать репрессивных мер против бирж Bitcoin со стороны государственных органов в попытке положить конец их использованию в противозаконных целях.

Если у вас в собственности есть биткойны, вас скорее всего волнует, как их сберечь. Несколько советов можно найти в посте наших коллег Стефана Танасе и Сергея Ложкина.

ВЫВОДЫ И ПРОГНОЗЫ: 2014 ГОД — «ГОД ДОВЕРИЯ»

В отчете 2011 года мы назвали год «взрывоопасным». Мы также предсказывали, что 2012-й будет годом разоблачений, а 2013-й — годом сенсаций и переосмысления ситуации.

И действительно, некоторые из открытий 2013 года стали поистине сенсационными. Они заставили нас по-новому посмотреть на то, как мы теперь используем интернет и с какими видами рисков нам приходится сталкиваться. В 2013 году наиболее опасные группы киберпреступников продолжали осуществлять крупномасштабные кампании — например, RedOctober и NetTraveler. Злоумышленники освоили новые приемы, такие как атаки типа watering hole, однако эксплойты нулевого дня остаются популярными среди серьезных киберпреступников. В 2013 году на сцене появились кибернаемники — компактные группы, специализирующиеся на проведении «молниеносных» APT-атак на заказ. В заголовках новостей постоянно мелькали хактивисты, а также утечки данных. Последние способны нагнать страху даже на самых крутых сисадминов. Тем временем киберпреступники активно создавали новые методы кражи пользовательских денег и биткойнов; широчайшее распространение получили программы-вымогатели (Ransomware). И наконец, серьезной проблемой, не имеющей простого решения, остается мобильное вредоносное ПО.

Конечно, все хотели бы знать, как эти тенденции скажутся на ситуации в 2014 году. Мы предполагаем, что через весь 2014 год красной нитью пройдет тема восстановления доверия.

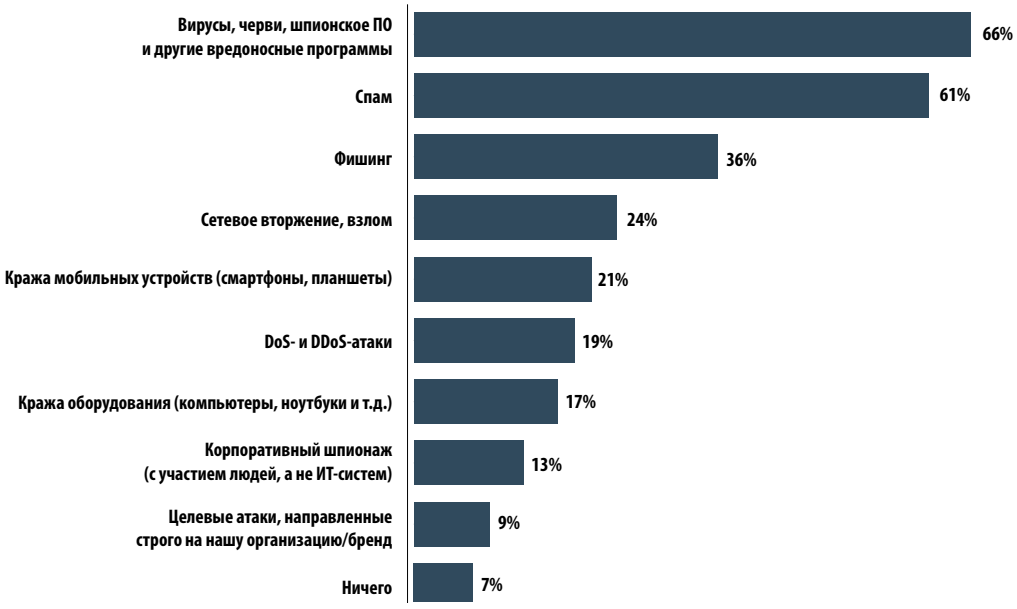
Тайна частной жизни, как и многочисленные факторы, ведущие к ее сохранению или утрате, останется горячей темой. Шифрование снова войдет в моду: мы ожидаем появления многочисленных сервисов, обещающих защитить личную жизнь пользователей от посторонних глаз. Облако — чудо-технология прошлых лет — теперь забыто, поскольку люди потеряли к нему доверие, а государства более серьезно задумались о том, как применение облачных технологий соотносится с тайной частной жизни. В 2014 году финансовые рынки, вероятно, почувствуют на себе влияние виртуальной валюты Bitcoin, в которую будут вкладывать значительные средства инвесторы из Китая и других стран. Не исключено, что стоимость биткойна достигнет $10 000, но нельзя также исключать и краха виртуальной валюты, в результате которого пользователи станут искать более надежные альтернативные варианты.

КОРПОРАТИВНЫЕ УГРОЗЫ

Виталий Камлюк, Сергей Ложкин

За последние два года количество обнаруживаемых серьезных кибератак выросло настолько, что каждая новая атака уже редко вызывает удивление. Отчеты антивирусных компаний об обнаружении очередного ботнета или хитрого образца вредоносного программного обеспечения для сбора данных появляются регулярно.

Все чаще потенциальными жертвами кибератак становятся коммерческие компании. Согласно результатам опроса, проведенного «Лабораторией Касперского» и аналитической компанией «B2B International», 91% опрошенных организаций в мире хотя бы один раз в течение года подверглись кибератаке, 9% компаний стали мишенью целевых атак.



Использование компьютеров и других цифровых устройств во всех бизнес-процессах создало основу для успешного применения вредоносного программного обеспечения для коммерческого шпионажа и кражи корпоративных данных. Это открывает настолько большие

возможности, что в ближайшем будущем вредоносные программы могут полностью заменить инсайдерскую разведку. Но риски для корпоративного сектора этим не ограничиваются. Зависимость успешности бизнеса от надежной работы компьютеров и каналов связи между ними дает злоумышленникам основание для использования различных программ деструктивного действия: от шифровальщиков и «программ-стирателей», распространяющихся, как болезнь, в корпоративной среде, до армии послушных зомби, поглощающих все свободные ресурсы корпоративных интернет-серверов и сетей передачи данных.

ЗАЧЕМ АТАКУЮТ

- **Кража информации.** Хищение ценных корпоративных данных, коммерческой тайны или персональных данных сотрудников и клиентов компании, мониторинг деятельности компании являются целью многих: от бизнесменов, которые обращаются к услугам киберпреступников для проникновения в корпоративные сети конкурентов, до разведывательных служб разных стран.

- **Уничтожение данных или блокирование работы инфраструктуры.** Некоторые вредоносные программы используются для своего рода диверсий: их задача состоит в уничтожении важных данных или нарушении работы инфраструктуры компании. Например, троянские программы Wiper и Shamoon стирают системные данные на рабочих станциях и серверах без возможности их восстановления.

- **Кража денег.** Заражение специализированными троянскими программами, похищающими финансовые средства через системы дистанционного банковского обслуживания (ДБО), а также целевые атаки на внутренние ресурсы процессинговых и финансовых центров приводят к финансовым потерям атакованных компаний.

- **Удар по репутации компании.** Успешность бизнеса и очень высокая посещаемость официальных сайтов компаний, особенно работающих в сфере интернет-услуг, привлекает злоумышленников. Взлом корпоративного сайта с последующим внедрением ссылок, направляющих посетителей на вредоносные ресурсы, вставка вредоносного рекламного баннера или размещение политически ориентированного сообщения на взломанном ресурсе наносит существенный урон отношению клиентов к компании.

  Еще одним критически важным репутационным риском является кража цифровых сертификатов IT-компаний. В отдельных случаях, например для компаний, имеющих свои публичные центры сертификации, потеря сертификатов или проникновение в

инфраструктуру цифровой подписи может привести к полному уничтожению доверия к компании и последующему закрытию бизнеса.

- **Финансовый ущерб.** Одним из популярных способов нанесения прямого вреда компаниям и организациям являются DDoS-атаки. Киберпреступники разрабатывают новые способы проведения таких атак. В результате DDoS-атак порой на несколько дней выводятся из строя внешние веб-ресурсы компаний. В таких случаях клиенты не только не могут воспользоваться услугами атакованной компании, что наносит ей прямой финансовый ущерб, но и нередко совсем отказываются от них в пользу более надежной компании, что ведет к уменьшению базы клиентов и долгосрочным финансовым потерям.

  В 2013 году выросла популярность атак типа DNS Amplification, когда злоумышленники с помощью ботнетов отправляют рекурсивные запросы к DNS-серверам, возвращая ответ на атакуемые системы. Именно так была проведена одна из самых мощных в этом году DDoS-атак — атака на сайт проекта Spamhaus.

ОРГАНИЗАЦИИ-МИШЕНИ

При массовом распространении вредоносных программ жертвой киберпреступников может стать любая компания, компьютеры которой им удастся заразить. Так, даже в небольшую коммерческую компанию может проникнуть популярный банковский троянец (ZeuS, SpyEye и др.), что в результате приведет к потере и денег, и интеллектуальной собственности.

По результатам наших исследований, в 2013 году объектами целевых атак (тщательно спланированных действий по заражению сетевой инфраструктуры определенной организации или частного лица) стали предприятия нефтяной индустрии, телекоммуникационные компании, научно-исследовательские центры и компании, занятые в аэрокосмической, судостроительной и других отраслях промышленности, связанных с разработкой высоких технологий.

ПОДГОТОВКА АТАКИ

Киберпреступники используют большой арсенал сложных инструментов для проникновения в корпоративные компьютерные сети. Планирование целевой атаки на компанию может

занимать несколько месяцев, после чего используются все возможные технологии, начиная социальной инженерией и заканчивая эксплойтами к неизвестным уязвимостям в программном обеспечении.

Атакующие скрупулёзно изучают коммерческий профиль предприятия, публичные ресурсы, в которых можно почерпнуть любую полезную информацию, веб-сайты и веб-порталы компании, профили сотрудников в социальных сетях, анонсы и итоги различных презентаций, выставок и прочее. Преступники могут изучать сетевую инфраструктуру компаний, сетевые ресурсы и коммуникационные узлы для планирования стратегии проникновения и похищения информации.

Злоумышленники при планировании атаки могут создавать поддельные вредоносные веб-сайты, в точности копирующие внешний вид сайтов, принадлежащих компаниям-клиентам или партнерам атакуемой организации, регистрировать похожие по названию доменные имена. В дальнейшем их используют для обмана и заражения жертвы.

МЕТОДЫ ПРОНИКНОВЕНИЯ

В 2013 году одним из самых популярных у злоумышленников методов проникновения вредоносных программ в корпоративную сеть стала рассылка сотрудникам атакуемой компании электронных писем с вредоносными вложениями. Чаще всего в такие письма вложен документ в привычном для офисных работников формате Word, Excel или PDF. При открытии вложенного файла эксплуатируется уязвимость в программном обеспечении и происходит заражение системы вредоносной программой.

СЛАБОЕ ЗВЕНО

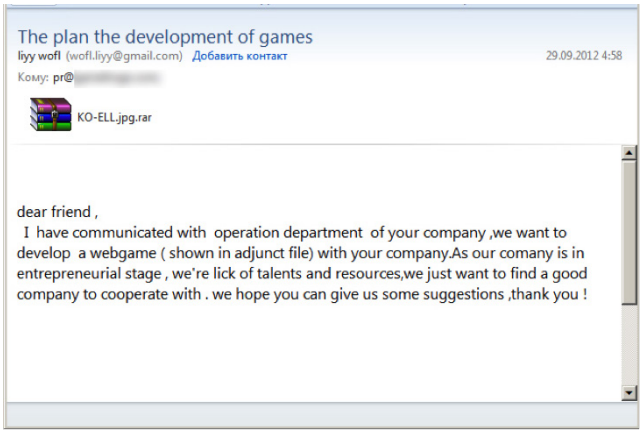
Зачастую получателями вредоносных писем становятся сотрудники, которые по характеру своей деятельности часто общаются с адресатами вне своей корпоративной структуры. Чаще всего вредоносная корреспонденция отправляется сотрудникам PR-отделов.

Подразделения, занимающиеся подбором кадров, также получают много писем от внешних пользователей. Злоумышленник может выступить в роли потенциального кандидата на открытую вакансию, вступить в переписку и прислать зараженный PDF-файл с резюме. Несомненно, такой файл будет открыт сотрудником HR, и при наличии уязвимости его рабочая станция будет заражена.

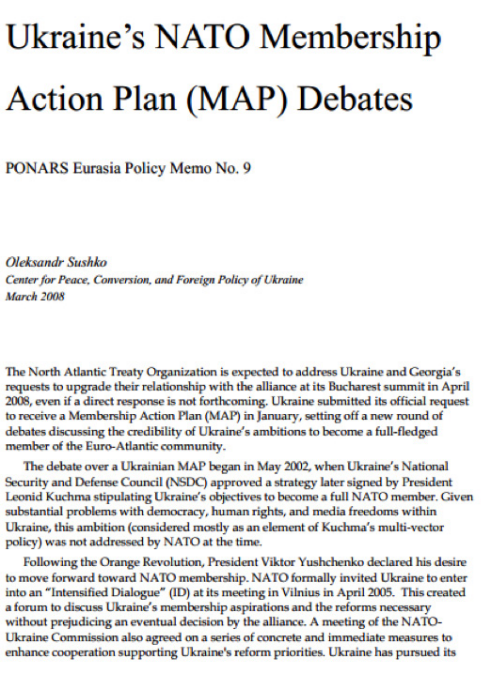
В финансовые подразделения компаний киберпреступники могут рассылать вредоносные письма от имени налоговых органов — под видом разнообразных запросов, требований, заявлений и т.п. Юридические отделы могут получить вредоносные послания якобы от судебных органов, приставов и прочих органов государственной власти.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Содержание письма обычно представляет интерес для сотрудника, которому оно адресовано, — оно связано либо с его обязанностями, либо со сферой деятельности компании. Так, например, в целевой атаке, направленной против частных компаний, занятых в сфере видеоигр, хакерская группа Winnti использовала письма с предложением о сотрудничестве:



А шпион Miniduke рассылался с помощью письма о планах украинской внешней политики, в частности о взаимоотношениях Украины с НАТО:



Ukraine's NATO Membership Action Plan (MAP) Debates

PONARS Eurasia Policy Memo No. 9

Oleksandr Sushko
Center for Peace, Conversion, and Foreign Policy of Ukraine
March 2008

The North Atlantic Treaty Organization is expected to address Ukraine and Georgia's requests to upgrade their relationship with the alliance at its Bucharest summit in April 2008, even if a direct response is not forthcoming. Ukraine submitted its official request to receive a Membership Action Plan (MAP) in January, setting off a new round of debates discussing the credibility of Ukraine's ambitions to become a full-fledged member of the Euro-Atlantic community.

The debate over a Ukrainian MAP began in May 2002, when Ukraine's National Security and Defense Council (NSDC) approved a strategy later signed by President Leonid Kuchma stipulating Ukraine's objectives to become a full NATO member. Given substantial problems with democracy, human rights, and media freedoms within Ukraine, this ambition (considered mostly as an element of Kuchma's multi-vector policy) was not addressed by NATO at the time.

Following the Orange Revolution, President Viktor Yushchenko declared his desire to move forward toward NATO membership. NATO formally invited Ukraine to enter into an "Intensified Dialogue" (ID) at its meeting in Vilnius in April 2005. This created a forum to discuss Ukraine's membership aspirations and the reforms necessary without prejudicing an eventual decision by the alliance. A meeting of the NATO-Ukraine Commission also agreed on a series of concrete and immediate measures to enhance cooperation supporting Ukraine's reform priorities. Ukraine has pursued its

УЯЗВИМОСТИ И ЭКСПЛОЙТЫ

Киберпреступники активно используют эксплойты к известным уязвимостям в программном обеспечении.

Знаменитый Red October, например, использовал как минимум три различных эксплойта для уже известных уязвимостей в Microsoft Office — CVE-2009-3129 (MS Excel), CVE-2010-3333 (MS Word) и CVE-2012-0158 (MS Word), а зловред Nettraveler — эксплойт для CVE-2013-2465, уязвимости в Java версий 5, 6 и 7, которая была устранена Oracle лишь в июне 2013 г.

Но наиболее опасными являются уязвимости, которые еще неизвестны разработчику (0-day уязвимости). Киберпреступники активно ищут в популярных программах еще неизвестные бреши и создают к ним эксплойты. При наличии такой уязвимости в ПО вероятность ее эксплуатации очень высока. Такую уязвимость (CVE-2013-0640) в Adobe Reader версий 9, 10, 11, на время атаки еще неизвестную, использовал Miniduke.

ТЕХНОЛОГИИ

Киберпреступники постоянно совершенствуют вредоносное программное обеспечение, используют необычные подходы и решения для хищения информации.

Red October после проникновения в систему работал как многофункциональная модульная платформа и в зависимости от цели добавлял в зараженную систему различные модули, каждый из которых осуществлял определенный набор действий: первичный сбор информации о зараженной машине и сетевой инфраструктуре, кражу паролей от различных сервисов, клавиатурный шпионаж, самораспространение, передачу похищенной информации и т.д.

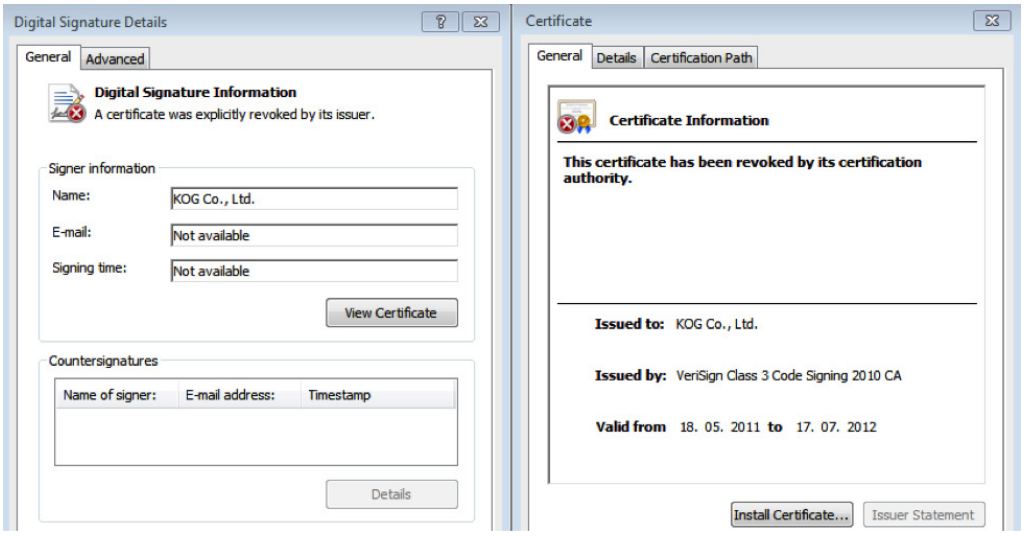
Также стоит отметить, что киберпреступники не могли не обратить внимания на развитие мобильных технологий и распространение мобильных устройств в корпоративной среде. Современный смартфон или планшет является практически полноценной рабочей станцией и хранит множество данных, становясь таким образом целью злоумышленников. Создатели Red October разработали специальные модули, которые определяли, когда к зараженной рабочей станции подключались смартфоны на платформах Apple iOS, Windows Mobile и телефоны производства Nokia, затем копировали с них данные и отсылали на сервер управления.

Создатели Kimsuky внедрили в зловред целый модуль по удаленному управлению зараженными системами, причем сделали это на основе вполне легитимного средства удаленного администрирования TeamViewer, немного модифицировав его программный код. После чего несколько операторов подключались к инфицированным компьютерам вручную, собирая и копируя информацию, представляющую интерес.

Хакерская группа Winnti похищала в корпоративных сетях разработчиков онлайн-игр цифровые сертификаты и подписывала ими свой вредоносный драйвер, заражая в дальнейшем другие

компании. Например, был похищен цифровой сертификат южнокорейской компании KOG. После того как мы уведомили компанию о хищении, сертификат был отозван.

Отозванный сертификат:



Кроме того одним из модулей 64-битного троянца был полнофункциональный бэкдор — это первый известный нам случай использования 64-битных вредоносных программ, имеющих действительную цифровую подпись легальной компании.

Шпионский зловред Miniduke использовал Twitter для получения информации о серверах управления. Операторы Miniduke с помощью специально созданных аккаунтов публиковали определенным образом сформированные твиты с зашифрованным адресом управляющего сервера:

Троянец с зараженной машины читал Twitter и подключался к управляющим системам.

ЧТО КРАДУТ

Злоумышленники заинтересованы в похищении самой разной информации. Это могут быть новейшие технологические разработки компаний и научно-исследовательских институтов, исходные коды программных продуктов, финансовые и юридические документы, персональные данные сотрудников и клиентов, а также любая иная информация, представляющая коммерческую тайну. Часто эта информация хранится в незашифрованном состоянии в сетях предприятий в виде электронных документов, технических заданий, отчетов, чертежей, презентаций, изображений и т.д.

Как говорилось выше, киберпреступники используют различные подходы к сбору данных. Некоторые зловреды собирают практически все виды электронных документов. Например, Red October интересовали документы в форматах **txt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau** и т.д., которые вредоносная программа отсылала на управляющие серверы.

Другой подход, отмеченный нами в Kimsuky и Icefog, — практически сделанный вручную анализ хранящихся данных в корпоративных сетях (с помощью встроенных в зловреды технологий удаленного доступа к зараженным рабочим станциям) и последующее копирование только тех документов, которые представляли интерес для злоумышленников. При этом злоумышленники учитывают все особенности атакуемой компании и четко представляют, какие форматы данных там используют и какую информацию хранят. Так, в случае Kimsuky и Icefog происходила кража весьма специфичных для компаний-жертв документов в формате hwp, популярных в Южной Корее.

НОВАЯ ТЕНДЕНЦИЯ: КИБЕРНАЕМНИКИ

Исследуя последние целевые атаки, мы пришли к выводу, что в мире киберпреступников появилась новая категория атакующих, которую мы назвали «кибернаемники». Это организованные группы хакеров с очень высоким уровнем подготовки, которые могут быть наняты правительствами и частными компаниями для организации и проведения сложных эффективных целевых атак на частные компании с целью кражи информации, уничтожения данных или инфраструктуры.

Кибернаемники получают контракт, в котором указаны цели и характер задания, после чего начинают тщательную подготовку и осуществление атаки. Если раньше при целевых атаках происходило массовое хищение различной информации, то кибернаемники стремятся добыть вполне конкретные документы или контакты людей, которые могут владеть искомой информацией.

В 2013 году мы расследовали деятельность группы кибернаемников IceFog, осуществлявшей одноименные целевые атаки. В ходе расследования нам удалось обнаружить журнал активности операторов Icefog, подробно описывающий все действия атакующих. По этим записям было понятно, что злоумышленники знали, в каких директориях должна находиться интересующая их информация.

ПОСЛЕДСТВИЯ ГРОМКИХ РАЗОБЛАЧЕНИЙ

2013 год принес масштабные разоблачения атак шпионских программ, прямо или косвенно связанных с деятельностью различных государств. Результатом этих разоблачений может стать утрата доверия к глобальным сервисам и корпорациям, а также зарождение идеи создания собственных аналогов глобальных сервисов, но уже в границах отдельных государств. Это, в свою очередь, может привести к своеобразной деглобализации интернета и росту спроса на локальные IT-продукты и сервисы. Уже сегодня во многих странах существуют местные аналоги глобальных служб, таких как национальные поисковые системы, почтовые службы, национальные системы обмена сообщениями и даже местные социальные сети.

При этом рост числа новых программных продуктов и сервисов обеспечивают национальные компании–разработчики. Как правило, это компании, размер и бюджет которых меньше, чем у ведущих мировых разработчиков. Соответственно, и качество продуктов в этих компаниях проверяется не столь тщательно. По нашему опыту расследования кибератак, чем мельче и неопытнее разработчик ПО, тем больше уязвимостей будет найдено в его коде. Это обстоятельство значительно упрощает задачу киберпреступникам, осуществляющим целевые атаки.

Более того, получив преимущество в контексте контроля информации и аппаратных ресурсов, отдельные государства могут обязать локальные компании пользоваться национальными программными продуктами или интернет-службами, что, в конечном итоге, может негативно сказаться на безопасности корпоративного сектора.

ОСНОВНАЯ СТАТИСТИКА ЗА 2013 ГОД

Мария Гарнаева, Кристиан Функ

Эта часть отчета Kaspersky Security Bulletin 2013 сформирована 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.
- Наши 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 нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в США и России.

МОБИЛЬНЫЕ УГРОЗЫ

Мир мобильных устройств относится к той сфере, где IT-безопасность развивается наиболее быстро. В 2013 году проблема безопасности мобильных устройств встала очень остро, и это связано и с количественным, и с качественным ростом мобильных угроз. Если 2011 год был годом становления мобильных зловредов, особенно в секторе Android-устройств, а 2012 — годом развития их многообразия, то 2013 год стал годом наступления их зрелости. Неудивительно, что мир мобильных зловредов становится все более похожим на мир угроз для персональных компьютеров с точки зрения применяемых киберпреступниками методов и технологий; однако скорость развития этой сферы впечатляет.

Obad — пожалуй, наиболее заметное событие в сфере мобильных зловредов. Этот мобильный троянец распространяется разными способами, в том числе через уже существующий мобильный ботнет — смартфоны, зараженные Trojan-SMS.AndroidOS.Opfake.a, используются в качестве дополнительного вектора заражения. С них на все номера из списка контактов рассылаются сообщения, содержащие вредоносные ссылки. Такая практика широко распространена в сфере угроз для персональных компьютеров и популярна как сервис, предоставляемый ботоводами на теневом рынке киберпреступников.

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 малотребовательны по отношению к вычислительной мощности устройств и, соответственно, легко реализуемы на смартфонах. Ботнет MTK, появившийся в начале 2013 года, а также ботнет Opfake, как и многие другие, подтверждают, что мобильные ботнеты для киберпреступников стали большим, чем просто «площадкой для игр», и уже активно используются для основной цели: дать киберпреступникам заработать денег.

ЗНАЧИМЫЕ СОБЫТИЯ

> **Мобильные банковские троянцы.** Сюда относится мобильный фишинг, кража информации о кредитных картах, перевод денег с банковских карт на счёт мобильного телефона и оттуда — в кошелек QIWI. В 2013 году появились также мобильные троянцы, способные проверять баланс счёта жертвы, чтобы «доход» был максимальным.

> **Мобильные ботнеты.** Как сказано выше, ботнеты предоставляют большие возможности и большую гибкость при использовании нелегальных схем получения прибыли. Теперь это явление охватило и мобильные устройства. По нашим оценкам, около 60% мобильных вредоносных программ представляют собой элементы больших и малых мобильных ботнетов.

> **Backdoor.AndroidOS.Obad.** Этот зловред — пожалуй, самый универсальный из всех, зарегистрированных на сегодняшний день. Он включает целых три эксплойта, бэкдор, SMS-троянец, предоставляет функциональные возможности бота и другие. Это, по сути, швейцарский армейский нож, оснащенный разнообразными инструментами.

> **Контроль ботнетов через Google Cloud Messaging.** Киберпреступники обнаружили способ, как использовать сервис Google Cloud Messaging (GCM) для осуществления контроля зомби-устройств в ботнете. Этот метод используется в относительно небольшом количестве вредоносных программ, но некоторые из них при этом широко распространены. Выполнение команд, получаемых через GCM, производится системой GCM, и их невозможно заблокировать непосредственно на зараженном устройстве.

> **APT-атаки против уйгурских активистов.** Мы наблюдали, как в целевых атаках против уйгурских активистов используются зловреды, написанные и под Windows, и под MAC OS X. В прошлом атаки происходили также через PDF, XLS, DOC и ZIP-файлы, рассылаемые по электронной почте. Теперь в арсенал злоумышленников добавлены APK-файлы, отслеживающие личную информацию, хранящуюся на устройстве-жертве, а также передающие данные о его местонахождении.

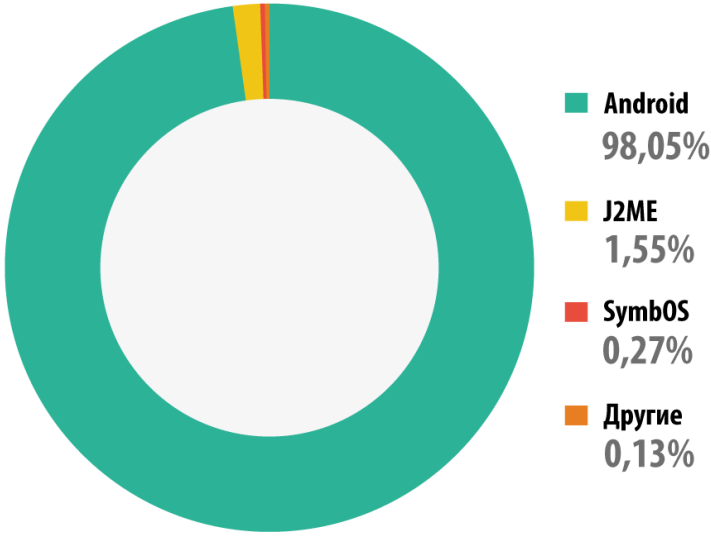
> **Уязвимости в Android.** В 2013 году мы наблюдали эксплойты, направленные на Android и созданные для трех разных целей: для обхода проверки целостности кода приложения при установке (также известную как уязвимость мастер-ключа), для повышения прав и для затруднения анализа приложения. Последние два типа также задействованы в Obad.

> **Атака на ПК при помощи Android-устройства.** Существуют угрозы для персональных компьютеров, которые могут заразить смартфоны, но мы обнаружили и зловред под

Android, который заражает ПК. Когда Android-устройство подсоединяется к компьютеру в режиме эмуляции USB-флешки, запускается вредоносный контент.

СТАТИСТИКА

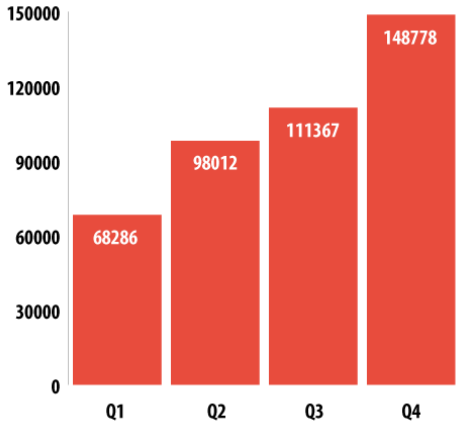
Что касается мобильных ОС, на которые нацелены вредоносные программы, то значимых изменений за 2013 год не произошло. Android по-прежнему остаётся основной целью для вредоносных атак — на эту платформу нацелено уже 98,05% всех известных зловредов. Как видно на диаграмме ниже, никакая другая ОС и рядом не стоит по «популярности». Причиной тому — ведущие позиции Android на рынке, преобладание сторонних магазинов приложений и в значительной степени открытая архитектура этой платформы, благодаря чему под нее легко писать как разработчикам приложений, так и авторам вредоносных программ. Мы не думаем, что эта тенденция в ближайшем будущем изменится.



Распределение мобильных вредоносных программ по платформам

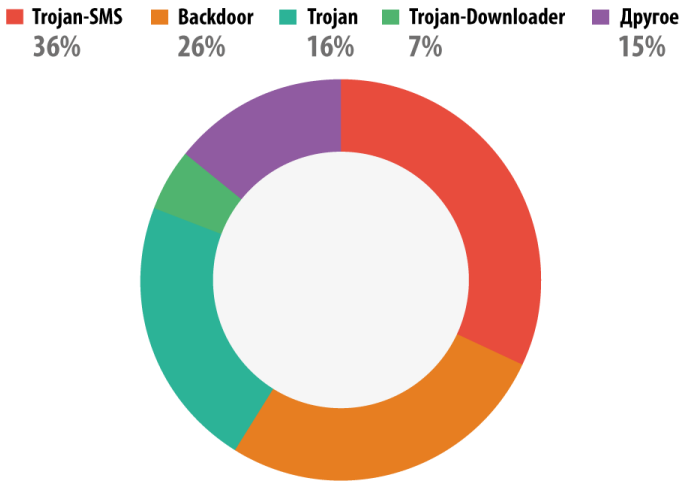
На сегодняшний день нам удалось собрать 8 260 509 уникальных вредоносных установочных пакетов. Стоит учитывать, что разные установочные пакеты могут устанавливать программы с одним и тем же функционалом, разница может заключаться лишь в интерфейсе вредоносного приложения и, например, содержимом отправляемых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

Общее число образцов мобильных зловредов в нашей коллекции составляет 148 778, из которых 104 427 обнаружены в 2013 году. Только в октябре появилось 19 966 модификаций — половина того количества, что «Лаборатория Касперского» обнаружила за весь 2012 год. К счастью, это сильно отличается от ситуации, наблюдаемой в мире зловредов для персональных компьютеров — их мы обрабатываем более 315 000 образцов в сутки. Тем не менее, тенденция к интенсивному росту вполне очевидна:



Количество образцов в нашей коллекции

Среди мобильных зловредов по-прежнему лидируют SMS-троянцы:



Распределение мобильных вредоносных программ по поведениям

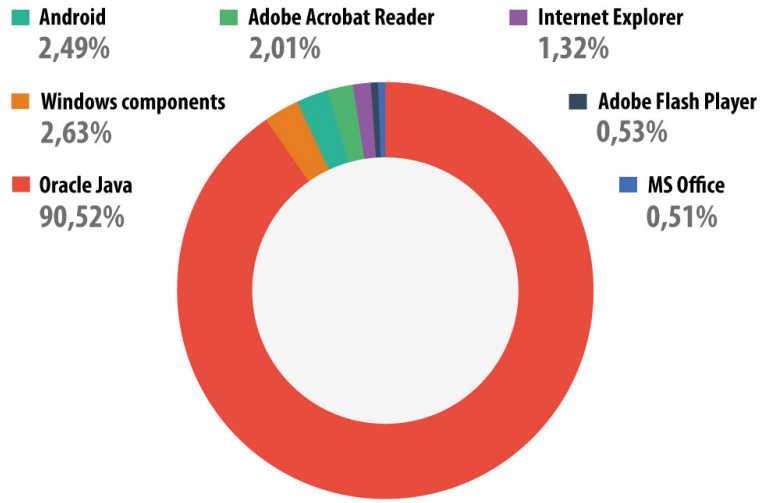
Однако зловреды категории Trojan-SMS за очень малым исключением эволюционировали в ботов, поэтому можно смело объединить двух лидеров диаграммы в одну категорию — Backdoor. Таким образом, 62% вредоносных приложений являются элементами мобильных ботнетов.

ВЫВОДЫ

- Все техники и механизмы инфицирования, сокрытия деятельности вредоносных программ очень быстро перебираются с PC на платформу Android. Этому способствует ее открытость и популярность.
- Большинство мобильных вредоносных приложений ориентировано на кражу денег и только во вторую очередь на кражу личной информации.
- Большинство мобильных вредоносных приложений представляют собой ботов с богатым функционалом. В ближайшее время начнется торговля мобильными ботнетами.
- Явно прослеживается «банковская» направленность развития мобильных зловредов. Вирусописатели следят за развитием сервисов мобильного банкинга. При успешном инфицировании смартфона сразу проверяют, 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.

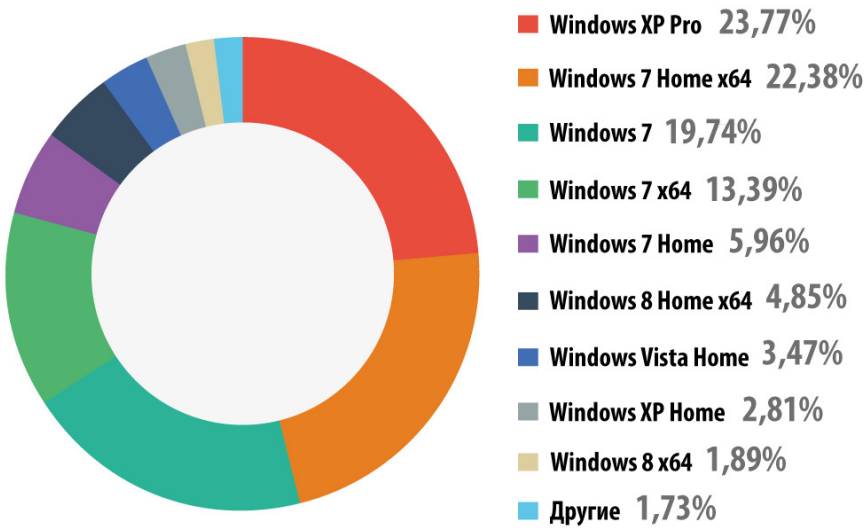


Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений

Из всех зафиксированных нами попыток эксплуатации уязвимостей 90,52% пришлось на уязвимости в Oracle Java. Такие уязвимости эксплуатируются в ходе drive-by атак через интернет, и новые Java-эксплойты входят в состав множества эксплоит-паков. Подробнее о Java-эксплойтах можно прочитать в нашей статье.

На втором месте расположилась категория «Windows компоненты», которая включает уязвимые файлы семейств ОС Windows, не относящиеся к Internet Explorer и программам Microsoft Office — их мы выделили отдельно. В этой категории самое большое количество атак приходится на обнаруженную в win32k.sys уязвимость CVE-2011-3402, которую впервые использовал Duqu.

На третьем месте с показателем 2,5% расположились эксплойты для Android OS. Уязвимости в Android используют злоумышленники (а иногда и сами пользователи), чтобы получить root-привилегии, которые дают практически неограниченные возможности для манипуляций над системой. Данные уязвимости не используются в drive-by атаках и эксплойты к ним детектируются либо веб-антивирусом в случае попытки скачивания пользователем приложения с эксплойтом, либо файловым антивирусом при нахождении эксплойта уже на устройстве. Тут стоит упомянуть, что недавно появилась информация о нахождении в браузере Chrome на Nexus 4 и Samsung Galaxy S4 уязвимости, которая может привести к использованию в будущем Android-уязвимостей в drive-by атаках.



Распределение установленной у пользователей OS Windows по версиям, 2013

Среди пользователей наших продуктов, подтвердивших свое участие в KSN, суммарно 61,5% используют различные версии операционной системы Windows 7 (на 5% больше чем в прошлом году); 6,3% - Windows XP (на 7,75% меньше, чем в 2012 году).

ВРЕДОНОСНЫЕ ПРОГРАММЫ В ИНТЕРНЕТЕ (АТАКИ ЧЕРЕЗ WEB)

Статистические данные в этой главе получены на основе работы веб-антивируса, который защищает пользователей в момент загрузки вредоносных объектов с вредоносной/зараженной веб-страницы. Вредоносные сайты специально создаются злоумышленниками; зараженными могут быть веб-ресурсы, контент которых создается пользователями (например, форумы), а также взломанные легитимные ресурсы.

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.

По сравнению с прошлым годом темпы роста числа атак через браузер снизились. Число отраженных в 2013 году интернет-атак превышает аналогичный показатель 2012 года в 1,07 раз, а в 2012 году мы зафиксировали рост в 1,7 раз. Основной способ атаки — через эксплоит-паки — дает злоумышленникам практически гарантированную возможность заражения компьютеров, если на них не установлена защита и имеется хотя бы одно популярное и уязвимое (не обновленное) приложение.

ВРЕДОНОСНЫЕ ПРОГРАММЫ В ИНТЕРНЕТЕ: TOP 20

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

	НАЗВАНИЕ*	% ОТ ВСЕХ АТАК**
1	**Malicious URL**	93,01%
2	**Trojan.Script.Generic**	3,37%
3	**AdWare.Win32.MegaSearch.am**	0,91%
4	**Trojan.Script.Iframer**	0,88%
5	**Exploit.Script.Blocker**	0,49%
6	**Trojan.Win32.Generic**	0,28%
7	**Trojan-Downloader.Script.Generic**	0,22%
8	**Trojan-Downloader.Win32.Generic**	0,10%

9	**Hoax.SWF.FakeAntivirus.i**	0,09%
10	**Exploit.Java.Generic**	0,08%
11	**Exploit.Script.Blocker.u**	0,08%
12	**Exploit.Script.Generic**	0,07%
13	**Trojan.JS.Iframe.aeq**	0,06%
14	**Packed.Multi.MultiPacked.gen**	0,05%
15	**AdWare.Win32.Agent.aece**	0,04%
16	**WebToolbar.Win32.MyWebSearch.rh**	0,04%
17	**AdWare.Win32.Agent.aeph**	0,03%
18	**Hoax.HTML.FraudLoad.i**	0,02%
19	**AdWare.Win32.IBryte.heur**	0,02%
20	**Trojan-Downloader.HTML.Iframe.ahs**	0,02%

* Детектирующие вердикты модуля веб-антивируса. Информация предоставлена пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.
** Процент от всех веб-атак, которые были зафиксированы на компьютерах уникальных пользователей.

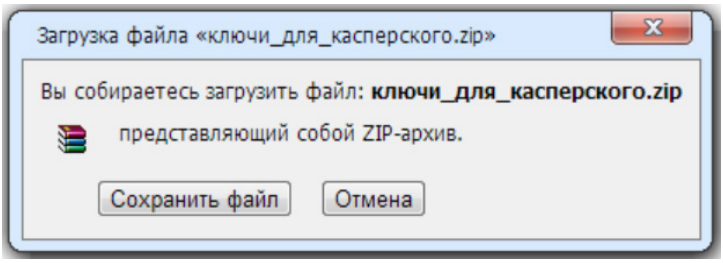
По сравнению с 2012 годом увеличилась доля вердиктов, связанных с блокированием зловредных ссылок, находящихся в черном списке веб-антивируса (1 место — Malicious URL). Развитие новых технологий детектирования, опирающихся на возможности KSN, позволило за год увеличить долю угроз, обнаруживаемых такими методами, с 87% до 93%. Значительная часть детектов Malicious URL приходится на сайты с эксплойтами и на сайты, перенаправляющие на эксплойты.

7 из 20 мест в нашем рейтинге заняли вердикты, которые присваиваются вредоносным объектам, используемым в drive-by атаках — самом популярном способе проникновения вредоносных программ через интернет. Это и эвристические вердикты, такие как Trojan.Script.Generic, Trojan.Script.Iframer, Exploit.Script.Blocker, Trojan-Downloader.Script.Generic, Exploit.Java.Generic, Exploit.Script.Generic, и не-эвристические. Это вердикты, присваиваемые как скриптам, перенаправляющим на эксплойты, так и самим эксплойтам.

Девятое место занимает Hoax.SWF.FakeAntivirus.i. Так детектируются флеш-файлы с анимацией, имитирующей работу антивирусного программного обеспечения. По итогам «проверки» компьютер пользователя оказывается «заражен» огромным количеством вредоносных программ. Для избавления от них злоумышленники тут же предлагают специальное защитное решение, жертве обмана нужно только отправить SMS на короткий номер и получить в ответ

ссылку, по которой они якобы могут скачать антивирусное ПО. Подобные флеш-файлы могут показываться на сайтах, размещающих у себя баннеры рекламной сети, участники которой не гнушаются время от времени «подкладывать» перенаправление на нежелательный контент.

Восемнадцатое место Hoax.HTML.FraudLoad.i — детект HTML-страницы, которая имитирует стандартное окошко для загрузки файла:



На подобную страницу перенаправляют различные русскоязычные сайты, на которых предлагается скачать какой-либо контент: игры, программы, фильмы (чаще всего подобные сайты размещаются на бесплатных хостингах). Если пользователь нажмет кнопку «Сохранить файл», то будет перенаправлен на файловый хостинг, где предлагается скачать файл после оформления платной подписки по SMS. Однако после выполнения всех требований вместо искомого контента он получает либо текстовый файл с инструкцией по использованию поисковиков, либо, что еще хуже, вредоносную программу.

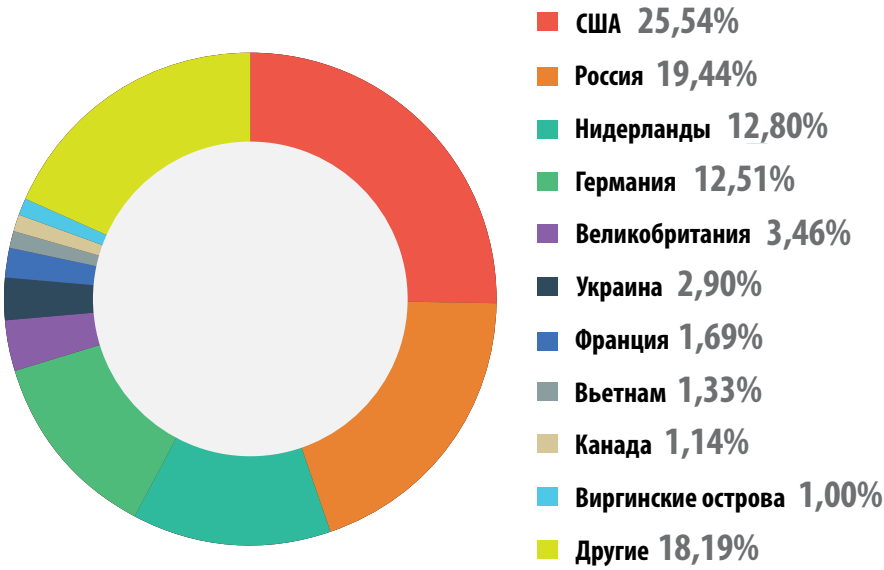
По сравнению с 2012 годом в рейтинге больше вердиктов рекламных программ. суммарная доля детектирований которых в TOP 20 выросла с 0,3% до 1,04%.

СТРАНЫ - ИСТОЧНИКИ ВЕБ-АТАК: TOP 10

Данная статистика показывает распределение по странам источников заблокированных антивирусом веб-атак на компьютеры пользователей (веб-страницы с редиректами на эксплойты, сайты с эксплойтами и другими вредоносными программами, центры управления ботнетами и т.д.). Отметим, что каждый уникальных хост мог быть источником одной и более веб атак.

Для определения географического источника веб-атак использовалась методика сопоставления доменного имени с реальным IP-адресом, на котором размещен данный домен, и установление географического местоположения данного IP-адреса (GEOIP).

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 — это на 14,5% меньше, чем в 2012 году.



Распределение по странам источников веб-атак

TOP 10 стран в 2013 году практически не изменился по сравнению с 2012 годом. Из первой десятки выбыл Китай, занимавший первое место в рейтинге до 2010 года, а на восьмом месте появился Вьетнам. В 2010 году властям Китая удалось убрать из локального киберпространства множество вредоносных хостингов, в то же время были ужесточены правила регистрации доменов в зоне .cn. После этого доля вредоносных хостингов в Китае резко сократилась. В 2010 году Китай занимал 3 место, в 2011 году — 6-е, в 2012 году - 8-е, а по итогам 2013 года эта страна заняла в рейтинге лишь 21-е место.

СТРАНЫ, В КОТОРЫХ ПОЛЬЗОВАТЕЛИ ПОДВЕРГАЛИСЬ НАИБОЛЬШЕМУ РИСКУ ЗАРАЖЕНИЯ ЧЕРЕЗ ИНТЕРНЕТ

Чтобы оценить степень риска заражения через интернет, которому подвергаются компьютеры пользователей в разных странах мира, мы подсчитали, насколько часто в течение года пользователи продуктов «Лаборатории Касперского» в каждой стране сталкивались со срабатыванием веб-антивируса. Полученные данные являются показателем агрессивности среды, в которой работают компьютеры в разных странах.

20 стран, в которых отмечен наибольший риск заражения компьютеров через интернет:

	СТРАНА*	% УНИКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ**
1	**Азербайджан**	56,29%
2	**Казахстан**	55,62%
3	**Армения**	54,92%
4	**Россия**	54,50%
5	**Таджикистан**	53,54%
6	**Вьетнам**	50,34%
7	**Молдова**	47,20%
8	**Беларусь**	47,08%
9	**Украина**	45,66%
10	**Киргизия**	44,04%
11	**Шри-Ланка**	43,66%
12	**Австрия**	42,05%
13	**Германия**	41,95%
14	**Индия**	41,90%
15	**Узбекистан**	41,49%
16	**Грузия**	40,96%
17	**Малайзия**	40,22%
18	**Алжир**	39,98%
19	**Греция**	39,92%
20	**Италия**	39,61%

Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.
*При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (меньше 10 тысяч).
**Процент уникальных пользователей, подвергшихся веб-атакам, от всех уникальных пользователей продуктов ЛК в стране.

В 2013 году в этом рейтинге сменился лидер: первое место занял Азербайджан, где веб-атакам подверглись 56,3% пользователей. Россия, которая лидировала два года подряд, сместилась на 4-ю строчку с показателем 54,5% (на 4,1% меньше, чем в прошлом году).

Покинули TOP 20 США, Испания, Оман, Судан, Бангладеш, Мальдивы, Туркменистан. Среди новичков — Австрия, Германия, Греция, Грузия, Киргизия, Вьетнам, и Алжир.

США опустились с 19-го сразу на 25-е место. Показатель этой страны уменьшился на 7% и составил 38,1%. Напомним, что еще два года назад по уровню веб-угроз эта страна была на 3-м месте. Уменьшение риска заражения компьютеров через интернет в США может быть связано в том числе с ростом популярности у пользователей веб-серфинга через мобильные устройства. Испания, которая в 2012 замыкала TOP 20, в 2013 году оказалась на 31-м месте (36,7%, на 8% меньше, чем в прошлом году).

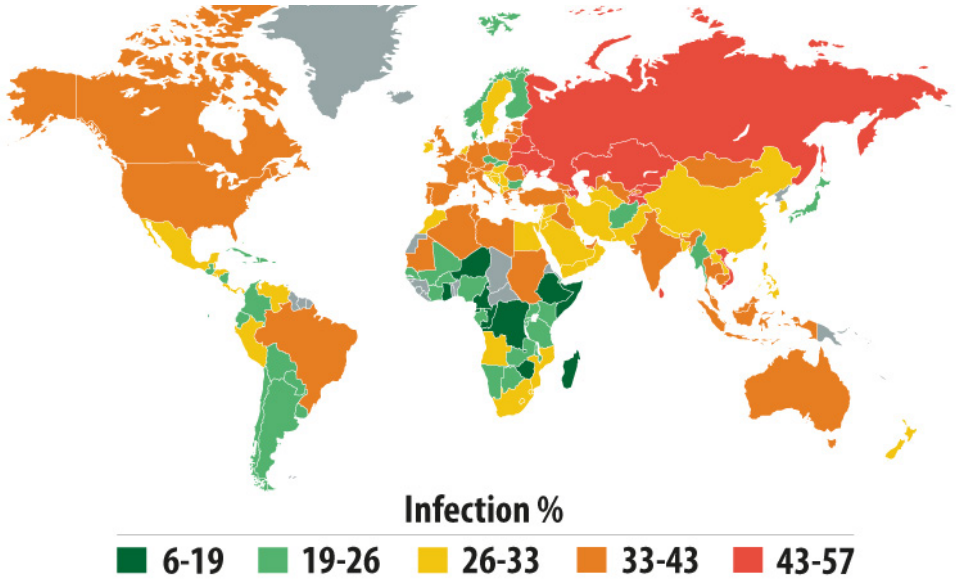
Австрия (+8%), оказалась сразу на 12-м месте, Германия (+9,3%) - на 13-м, а Греция (-1,6%) - на 19-м. Замыкает TOP 20 еще одна западноевропейская страна - Италия (-6%).

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

- **Группа повышенного риска.** В эту группу с результатом 41-60% вошли первые 15 стран из TOP 20. Это Россия, Австрия, Германия, большинство стран постсоветского пространства и страны Азии. Эта группа уменьшилась более чем вдвое: по итогам 2012 года в нее входила 31 страна.
- **Группа риска.** В эту группу с показателями 21-40,99% попали 118 стран, в том числе: Австралия (38,9%), США (38,1%), Канада (36,5%); Италия (39,6%), Франция (38,1%), Испания (36,7%), Великобритания (36,7%), Нидерланды (27,3%), Финляндия (23,6%), Дания (21,8%); Польша (37,6%), Румыния (33,2%), Болгария (24,1%); Бразилия (34,6%), Мексика (29,5%), Аргентина (25%); Китай (32,3%), Япония (25,3%).
- **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.

Африканские страны из группы самых безопасных при веб-серфинге попали в группы с высоким и средним уровнем заражения по уровню локальных угроз (см. ниже). В этих странах интернет пока не очень хорошо развит, и для обмена файлами пользователи активно

используют различные съемные носители информации. Поэтому веб-угрозам в этих странах подвергаются немногие, тогда как вредоносные программы, распространяющиеся на съемных носителях, часто детектируются на компьютерах пользователей.



В среднем уровень опасности интернета за год увеличился на 6,9%: в 2013 году в мире 41,6% компьютеров пользователей интернета хотя бы раз подвергались веб-атаке. Интернет по-прежнему является основным источником вредоносных объектов для пользователей большинства стран мира.

ЛОКАЛЬНЫЕ УГРОЗЫ

Исключительно важным показателем является статистика локальных заражений пользовательских компьютеров. В эти данные попадают объекты, которые проникли на компьютеры не через интернет, почту или сетевые порты.

В этом разделе мы анализируем статистические данные, полученные на основе работы антивируса, сканирующего файлы на жестком диске в момент их создания или обращения к ним, и данные по сканированию различных съемных носителей информации.

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.

ВРЕДОНОСНЫЕ ОБЪЕКТЫ, ОБНАРУЖЕННЫЕ НА КОМПЬЮТЕРАХ ПОЛЬЗОВАТЕЛЕЙ: TOP 20

	НАЗВАНИЕ	% УНИКАЛЬНЫХ АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ*
1	**DangerousObject.Multi.Generic**	39,1%
2	**Trojan.Win32.Generic**	38,0%
3	**Trojan.Win32.AutoRun.gen**	20,1%
4	**Virus.Win32.Sality.gen**	13,4%
5	**Exploit.Win32.CVE-2010-2568.gen**	10,6%
6	**AdWare.Win32.DelBar.a**	8,0%
7	**Trojan.Win32.Starter.lgb**	6,6%
8	**Virus.Win32.Nimnul.a**	5,5%
9	**Worm.Win32.Debris.a**	5,4%
10	**Virus.Win32.Generic**	5,4%
11	**Trojan.Script.Generic**	5,4%
12	**Net-Worm.Win32.Kido.ih**	5,1%
13	**AdWare.Win32.Bromngr.i**	4,6%
14	**Net-Worm.Win32.Kido.ir**	4,4%
15	**Trojan.Win32.Starter.yy**	3,9%
16	**DangerousPattern.Multi.Generic**	3,8%
17	**HiddenObject.Multi.Generic**	3,8%
18	**Trojan.Win32.Hosts2.gen**	3,7%
19	**AdWare.Win32.Agent.aeph**	3,6%
20	**Trojan.WinLNK.Runner.ea**	3,6%

Данная статистика представляет собой детектирующие вердикты модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.
*Процент уникальных пользователей, на компьютерах которых антивирус детектировал данный объект, от всех уникальных пользователей продуктов ЛК, у которых происходило срабатывание антивируса.

Вердикт DangerousObject.Multi.Generic, используемый для вредоносных программ, обнаруженных с помощью облачных технологий, в этом году поднялся со второго места на первое. Облачные 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. При помощи системы мгновенного обнаружения угроз UDS, работающей в составе Kaspersky Security Network, более 11 млн. компьютеров пользователей были защищены в режиме реального времени.

Второе место занимает эвристический вердикт Trojan.Win32.Generic - лидер прошлого года.

Exploit.Win32.CVE-2010-2568.gen (5-е место), Trojan.WinLNK.Runner.ea (20-е место) являются детектами вредоносных lnk-файлов (ярлыков). В lnk-файлах данных семейств осуществляется запуск другого вредоносного исполняемого файла. Они активно используются червями для распространения через USB-накопители.

Восемь программ из TOP 20 либо имеют механизм самораспространения, либо используются как одна из составляющих в схеме распространения червей: Virus.Win32.Sality.gen (4-е место), Trojan.Win32.Starter.lgb (7-е место), Virus.Win32.Nimnul.a (8-е место), Worm.Win32.Debris.a (9-е место), Virus.Win32.Generic (10-е место), Net-Worm.Win32.Kido.ih (12-е место), Net-Worm.Win32.Kido.ir (14-е место), Trojan.Win32.Starter.yy (15-е место).

Доля знаменитых червей Net-Worm.Win32.Kido (12-е и 14-е места), появившихся еще в 2008 году, из года в год уменьшается по мере того, как пользователи обновляют свои системы.

В TOP 20 в этом году не попали вердикты семейства Virus.Win32.Virut, однако доли других представителей вирусов — Sality (4-е место) и Nimnul (8-е место) — увеличились соответственно на 8,5% и на 1,4%.

Новое семейство в рейтинге этого года - Worm.Win32.Debris.a - на 9-м месте. Распространяется червь через съемные носители с помощью lnk-файлов. Полезная нагрузка этого червя представляет собой вредоносную программу Andromeda, которая используется для загрузки посторонних файлов. Эта программа известна на черном рынке вирусописателей еще с 2011 года. Однако новый способ ее инсталляции и распространения был выделен нами в отдельное семейство.

На 18-м месте расположился вердикт Trojan.Win32.Hosts2.gen - он присваивается вредоносным программам, которые пытаются изменить специальный файл hosts, перенаправляя запросы пользователей к определенным доменам на свои подконтрольные хосты.

СТРАНЫ, В КОТОРЫХ КОМПЬЮТЕРЫ ПОЛЬЗОВАТЕЛЕЙ ПОДВЕРГАЛИСЬ НАИБОЛЬШЕМУ РИСКУ ЛОКАЛЬНОГО ЗАРАЖЕНИЯ

Чтобы оценить, в каких странах пользователи чаще всего сталкиваются с киберугрозами, для каждой из стран мы подсчитали, насколько часто в течение года пользователи в ней сталкивались со срабатыванием антивирусной программы. Учитывались вредоносные программы, найденные непосредственно на компьютерах пользователей или же на съемных носителях, подключенных к компьютерам — флешках, картах памяти фотоаппаратов, телефонов, внешних жестких дисках. Эта статистика отражает уровень зараженности персональных компьютеров в различных странах мира.

TOP 20 стран по уровню зараженности компьютеров:

СТРАНА*	%**
Вьетнам	68,14%
Бангладеш	64,93%
Непал	62,39%
Монголия	60,18%
Индия	59,26%
Судан	58,35%
Афганистан	57,46%
Алжир	56,65%
Лаос	56,29%
Камбоджа	55,57%
Ирак	54,91%
Джибути	54,36%
Мальдивы	54,34%
Пакистан	54,12%
Шри-Ланка	53,36%
Мавритания	53,02%
Индонезия	52,03%
Руанда	51,68%

Ангола	50,91%
Египет	50,67%

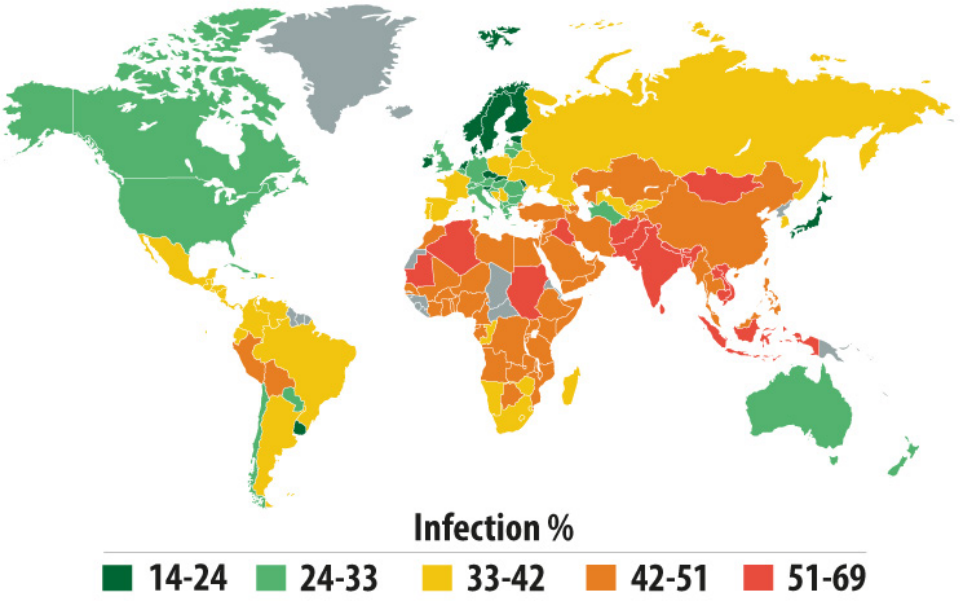
Настоящая статистика основана на детектирующих вердиктах модуля антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.
*При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (меньше 10 тысяч).
**Процент уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы, от всех уникальных пользователей продуктов ЛК в стране.

Уже больше года TOP 20 стран по уровню зараженности компьютеров состоит из стран Африки, Ближнего Востока и Юго-Восточной Азии. Однако за прошедший год ситуация в целом изменилась к лучшему. Если в 2012 году показатели страны - лидера рейтинга превышали 99%, то в 2013 году максимальный показатель в TOP 20 не достигает 70%.

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

В случае локальных угроз мы можем разделить все страны мира на несколько категорий. Учитывая общее уменьшение уровня локальных заражений, связанное, по всей видимости, с падением популярности использования флешек для обмена информацией, мы снизили пороговые значения показателей групп (по сравнению со статистикой за 2012 год).

- **Максимальный уровень заражения (более 60%):** 4 страны, лидирующие в рейтинге — Вьетнам (68,1%), Бангладеш (64,9%), Непал (62,4%) и Монголия (60,2%).
- **Высокий уровень заражения (41-60%):** 67 стран мира, в том числе Индия (59,2%), Китай (46,7%), Казахстан (46%), Азербайджан (44,1%), Россия (41,5%), большинство стран Африки.
- **Средний уровень заражения (21-40,99%):** 78 стран, в том числе Испания (36%), Франция 33,9%, Португалия (33,1%), Италия (32,9%), Германия (30,2%), США (29%), Великобритания (28,5%), Швейцария (24,6%), Швеция (21,4%), Украина (37,3%), Бразилия (40,2%), Аргентина (35,2%), Чили (28,9%), Южная Корея (35,2%), Сингапур (22,8%).
- **Наименьший уровень заражения (0-20,99%):** 9 стран мира.



В десятку самых безопасных по уровню локального заражения стран попали:

МЕСТО	СТРАНА	%
1	**Дания**	14,74%
2	**Чехия**	15,584%
3	**Финляндия**	15,93%
4	**Куба**	17,18%
5	**Япония**	18,93%
6	**Словакия**	19,24%
7	**Словения**	19,32%
8	**Норвегия**	19,36%
9	**Сейшельские острова**	19,90%
10	**Мальта**	21,28%

По сравнению с 2012 годом в списке произошло одно изменение — в нем появились Сейшельские острова, которые вытеснили Нидерланды.

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

ПРОГНОЗЫ

Александр Гостев

МОБИЛЬНЫЕ УГРОЗЫ

Начавшись много лет назад с троянца Gpcode, вредоносные программы-«вымогатели» эволюционировали в двух направлениях: троянцы, которые блокируют работу компьютера и требуют деньги за разблокировку, и троянцы, которые шифруют данные на компьютере и требуют гораздо более существенные суммы за расшифровку.

В 2014 году вирусописатели должны сделать логичный шаг в развитии этих видов троянских программ и обратить внимание на мобильные устройства. В первую очередь, конечно же, на устройства с административными правами на базе ОС Android. Шифрование пользовательских данных на смартфоне: фотографий, контактов, переписки — при наличии у троянца администраторских прав может быть реализовано достаточно просто, а распространение подобных троянских программ, в том числе и через легальный сервис Google Play, не составит большого труда.

Тенденция усложнения мобильных вредоносных программ, которую мы наблюдали в 2013 году, вне всякого сомнения, продолжится в 2014-м. Как и прежде, злоумышленники будут стремиться с помощью мобильных троянцев добраться до денег пользователей. Продолжится развитие средств, с помощью которых можно получить доступ к банковским аккаунтам владельцев мобильных устройств (мобильный фишинг, «банковские» троянцы). Начнется торговля мобильными ботнетами; их станут активно использовать для распространения сторонних вредоносных приложений. Уязвимости в ОС Android по-прежнему будут использоваться при заражении мобильных устройств, не исключено, что и в drive-by атаках на смартфоны.

АТАКИ НА BITCOIN

Атаки на биткойн-пулы, биржи и пользователей Bitcoin станут одной из самых громких тем года.

Атаки на биржи будут пользоваться наибольшей популярностью у киберпреступников, поскольку при таких атаках соотношение затрат и прибыли оптимальное.

Что касается атак на пользователей Bitcoin, то в 2014 году значительно возрастет опасность атак с целью кражи их кошельков. Напомним, что в прошлом злоумышленники заражали компьютеры пользователей и использовали их для майнинга. Однако сейчас эффективность подобного метода снизилась в тысячи раз, тогда как кражи биткойнов сулят атакующим громадную прибыль при полной анонимности.

ЗАЩИТА ТАЙНЫ ЧАСТНОЙ ЖИЗНИ

Во всех странах люди хотят скрыть свою частную жизнь от спецслужб. Обеспечить защиту данных пользователей невозможно без соответствующих мер со стороны интернет-сервисов, используемых пользователями, — социальных сетей, почтовых служб, облачных хранилищ. Однако существующих сейчас способов защиты недостаточно. Несколько подобных сервисов уже заявили о внедрении дополнительных мер по защите данных пользователей — например о шифровании данных, передаваемых между собственными серверами. Внедрение методов защиты продолжится, поскольку они будут востребованы пользователями, и их наличие при выборе может стать существенным аргументом в пользу того или иного интернет-сервиса.

Есть проблемы и на стороне конечного пользователя. Ему нужно обезопасить информацию, которую он хранит на своем компьютере и мобильных устройствах, а также самостоятельно обеспечить конфиденциальность своих действий в Сети. Это значит, что должна вырасти популярность VPN-сервисов и Tor-анонимайзеров, а также спрос на средства для локального шифрования.

АТАКИ НА ОБЛАЧНЫЕ ХРАНИЛИЩА

Для «облаков» наступают трудные времена. С одной стороны, доверие к облачным сервисам хранения информации пошатнулось из-за разоблачений Сноудена и ставших известными фактов сбора данных спецслужбами разных стран мира. С другой стороны, данные, хранящиеся там, их объем и, самое главное, содержание становятся все более и более привлекательной целью для хакеров. Мы еще три года назад говорили о том, что со временем хакеру может быть гораздо проще взломать облачного провайдера и украсть оттуда данные какой-либо компании, чем взломать саму компанию. Похоже, что это время наступает. Хакеры будут целенаправленно атаковать самое слабое звено — сотрудников облачных сервисов. Атака против них может дать ключи для доступа к гигантским объемам данных. Помимо кражи информации, атакующих могут интересовать возможности по ее удалению или модификации, что в ряде случаев может быть гораздо выгоднее заказчикам атаки.

АТАКИ НА РАЗРАБОТЧИКОВ ПО

Перекликается с описанной выше проблемой вероятный рост атак на разработчиков программных продуктов. В 2013 году мы раскрыли серию атак киберкриминальной группы Winnti. Жертвами этих атак стали игровые компании, у которых были украдены исходники серверной части онлайн-игр. Жертвой другой атаки стала компания Adobe — у нее, в частности, были украдены исходники Adobe Acrobat и ColdFusion. Из более ранних примеров подобных инцидентов выделяется атака на RSA в 2011 году, когда атакующие раздобыли исходные коды SecureID, а затем эти данные были использованы в атаке на Lockheed Martin.

Кража исходных кодов популярных продуктов дает атакующим прекрасную возможность для поиска в них уязвимостей — для последующего использования. Кроме того, при наличии доступа к репозиториям жертвы атакующие могут и модифицировать исходный код программ, добавив в них «бэкдоры».

И опять же, здесь в зоне особого риска находятся разработчики мобильных приложений (а таких разработчиков насчитываются тысячи), и тысячи приложений создаются ими и устанавливаются на сотни миллионов устройств.

КИБЕРНАЕМНИКИ

Разоблачения Сноудена показали, что государства ведут кибершпионаж в том числе с целью экономической помощи «своим» компаниям. Этот факт устранил своего рода моральный барьер, который до этого удерживал бизнес от использования столь радикальных методов конкурентной борьбы.

Компании нередко будут вынуждены вести экономический кибершпонаж, чтобы не потерять конкурентоспособность — ведь другие уже шпионят в целях получения конкурентного преимущества. Не исключено, что в некоторых странах компании будут вести кибершпионаж и за правительственными структурами. А также за своими сотрудниками, партнерами и поставщиками.

Осуществлять такие действия бизнес может только с помощью кибернаемников — организованных групп квалифицированных хакеров, которые будут оказывать компаниям коммерческие услуги по ведению кибершпионской деятельности. Скорее всего, эти хакеры будут называться «кибердетективами».

Одним из примеров использования наемных хакеров для осуществления коммерческого кибершпионажа стала атака Icefog, которую мы раскрыли летом 2013 года.

ФРАГМЕНТАЦИЯ ИНТЕРНЕТА

Поразительные вещи произошли с Сетью. Многие эксперты, и в частности Евгений Касперский, говорили о необходимости создания некого параллельного «безопасного интернета» без возможности анонимного совершения преступных действий в нем. А киберпреступники создали свой собственный отдельный Darknet, основанный на технологиях Tor и I2P, которые позволяют им анонимно заниматься криминалом, торговать и коммуницировать.

Одновременно с этим начался процесс дробления интернета на национальные сегменты. До недавнего времени этим отличался только Китай со своим Великим китайским файерволом. Однако в стремлении отделить значительную часть своих ресурсов и самостоятельно их

контролировать Китай оказался не одинок. Ряд стран, включая Россию, приняли или собираются принять законы, запрещающие использование иностранных сервисов. Особенно эти тенденции усилились после публикаций Сноудена. Так, в ноябре Германия заявила, что собирается полностью замкнуть все коммуникации между германскими ведомствами внутри страны. Бразилия сообщила о намерении проложить альтернативный магистральный интернет-канал, чтобы не использовать тот канал, который идет через американскую Флориду.

Всемирная Сеть стала распадаться на куски. Страны не желают выпускать хотя бы один байт информации за пределы своих сетей. Эти тенденции будут нарастать все сильней, и от законодательных запретов неизбежен переход к техническим ограничениям. После этого вероятным шагом станут и попытки ограничения иностранного доступа к данным внутри страны.

При дальнейшем развитии подобных тенденций мы очень скоро можем оказаться без единого интернета — но с десятками национальных сетей. Не исключено, что некоторые из них даже не будут иметь возможности взаимодействовать друг с другом. При этом теневой Darknet будет единственной наднациональной сетью.

ПИРАМИДА КИБЕРУГРОЗ

Все ожидаемые нами события и тенденции 2014 года проще всего представить графически, взяв за основу пирамиду киберугроз, нарисованную нами год назад.

Эта пирамида состоит из трех элементов. В основании находятся угрозы, используемые в атаках на рядовых пользователей со стороны традиционных киберпреступников, движимых исключительно соображениями собственной финансовой выгоды. На среднем уровне — угрозы, используемые в целевых атаках корпоративного кибершпионажа, а также так называемые полицейские программы-шпионы, применяемые государствами для шпионажа за своими гражданами и компаниями. Верхушка пирамиды — киберугрозы, создаваемые государствами для проведения кибератак на другие государства.

Большинство описанных выше сценариев развития киберугроз относятся к среднему уровню пирамиды. Поэтому в 2014 году мы ожидаем наиболее значительное увеличение количества угроз, связанных с экономическим и внутригосударственным кибершпионажем.

Обеспечит увеличение числа подобных атак перепрофилирование части киберпреступников, которые сейчас заняты атаками на пользователей, в кибернаемников-кибердетективов. Кроме того, весьма возможно, что услуги кибернаемников станут оказывать и те IT-специалисты, которые ранее никогда не занимались криминальной деятельностью. Этому будет способствовать ореол легитимности, который создадут работе «кибердетективов» заказы со стороны солидных компаний.