KASPERSKY lab

KASPERSKY SECURITY BULLETIN 2015

GREAT

#KLReport

ОГЛАВЛЕНИЕ

РАЗВИТИЕ УГРОЗ В 2015 ГОДУ

Традиционно конец года – это время для размышлений, время для переосмысления жизни и мыслей о будущем. Мы бы хотели предложить наш обычный обзор основных событий, которые формировали ландшафт информационных угроз в 2015 г.

ЦЕЛЕВЫЕ АТАКИ И ВРЕДОНОСНЫЕ КАМПАНИИ

Целевые атаки в наши дни – это уже характерная часть ландшафта информационных угроз; вполне ожидаемо, им посвящается целый раздел нашего годового отчёта. в прошлом году, в наших прогнозах на 2015 год, мы обозначили некоторые контуры будущего APT-угроз, каким оно нам тогда представлялось.

- Слияние киберпреступности и APT-угроз
- Фрагментация крупных APT-группировок
- Развитие вредоносных технологий
- Новые методы передачи краденых данных
- «Гонка кибервооружений», появление новых APT-агентов

Вот главные APT-кампании, о которых мы рассказывали в течение года.

Carbanak совместил киберпреступную деятельность – в данном случае кражу денег из финансовых учреждений – с методами проникновения в сеть жертвы, которые характерны для целевых атак. Кампания была раскрыта весной 2015 г.: «Лабораторию Касперского» пригласили провести расследование, связанное с работой системы одного банка, чьи банкоматы начали выдавать деньги «случайным образом». Оказалось, что компьютерная сеть банка заражена. Carbanak – это бэкдор, предназначенный для шпионских действий, кражи данных и удаленного управления зараженной системой. Злоумышленники использовали методы APT-атак для проникновения на компьютеры своих жертв – рассылали сотрудникам банка адресные фишинговые сообщения. Внедрившись на один банковский компьютер, злоумышленники провели разведку, определив системы, связанные с обработкой данных, ведением учёта и банкоматами, и просто имитировали деятельность сотрудников банка. Carbanak использовал три способа кражи денег: 1) выдачу наличных средств в банкоматах, 2) перевод денег киберпреступникам через сеть SWIFT и 3) создание фальшивых счетов и вывод денег через «финансовых мулов».

Группировка Equation, занимающаяся кибершпионажем, стала одной из самых нашумевших новостей I квартала 2015 г. Члены группировки успешно заразили компьютеры тысяч жертв в Иране, России, Сирии, Афганистане, США и в других странах. Среди жертв оказались государственные и дипломатические учреждения, телекоммуникационные и энергетические компании. Это одна из самых сложных APT-кампаний, которые нам приходилось видеть: один из многих модулей, разработанных группировкой, вносит изменения в прошивку жестких дисков, что позволяет, по сравнению с другими целевыми атаками, более надежно скрывать вредоносную программу, обеспечивая ей более долгое пребывание в системе. Очевидно, что разработка данного вредоносного кода началась не позже 2001 г. Видна связь с другими известными атаками – Stuxnet и Flame; в частности, набор вредоносных инструментов включал две уязвимости нулевого дня, которые позже использовались в Stuxnet.

Во время проведения расследования инцидента на Ближнем Востоке экспертами «Лаборатории Касперского» была обнаружена активность ранее неизвестной группировки, проводящей целевые атаки. Группа под названием Desert Falcons («Соколы пустыни») является первой арабской группировкой, проводящей полноценные операции по кибершпионажу, которые, по всей видимости, продиктованы политической ситуацией в регионе. Первые признаки деятельности Desert Falcons относятся к 2011 году, первые заражения произошли в 2013 году, а пик активности группы пришелся на конец

2014 – начало 2015 года. Злоумышленники украли более миллиона файлов более чем у 3000 жертв, в числе которых политические активисты и лидеры, военные и государственные организации, СМИ и финансовые учреждения, расположенные в основном в Палестине, Египте, Израиле и Иордании. Члены Desert Falcons – явно не новички: они с нуля создали вредоносные программы под Windows и Android, искусно организовали атаки, в которых использовались фишинговые электронные сообщения, поддельные вебсайты и поддельные аккаунты в социальных сетях.

В марте 2015 г. вышел наш отчёт об APT-кампании Animal Farm, хотя информация о задействованных в ней инструментах, начала появляться еще в прошлом году. в марте 2014 французская газета Le Monde опубликовала статью о наборе инструментов кибершпионажа, выявленных Центром безопасности коммуникации Канады (CSEC). Описанный инструментарий использовался в операции Snowglobe, нацеленной на франкоговорящие канадские СМИ, Грецию, Францию, Норвегию и некоторые африканские страны. По мнению CSEC, данная операция могла быть инициирована французскими разведывательными службами. Годом позже исследователи опубликовали анализ (1, 2, 3) некоторых вредоносных программ, имеющих много общего с программами операции Snowglobe. в частности, были идентифицированы самплы, содержащие внутреннее имя Babar, которое совпадало с именем программы, упомянутой CSEC. Эксперты «Лаборатории Касперского», проанализировав вредоносные программы данной кампании и выявив связь между ними, назвали стоящую за ними группировку «Animal Farm». Было обнаружено, что данная группа использовала две из трех zero-day уязвимостей, найденных «Лабораторией Касперского» в 2014 году и используемых киберпреступниками. Например, атака со взломанного сайта министерства юстиции Сирии с использованием эксплойтов к уязвимости CVE-2014-0515 приводила к загрузке одного из инструментов Animal Farm под названием Casper. Из особенностей данной кампании интересно отметить, что одна из программ в арсенале группировки, NBOT, разработана для проведения DDoS-атак, а это нехарактерно для APT-групп. Также одно из зловредных «животных» имеет странное название Tafacalou – возможно, это слово из окситанского языка, на котором говорят во Франции и некоторых других странах.

В апреле 2015 г. мы сообщили о появлении нового члена вредоносного семейства Duke, в которое уже входят MiniDuke, CosmicDuke и OnionDuke. CozyDuke APT (также известный как CozyBear, CozyCar и Office Monkeys) атакует правительственные организации и коммерческие компании в США, Германии, Южной Корее и Узбекистане. Атака проводится с использованием сложных технологий, таких как шифрование, защита от обнаружения антивирусными программами и тщательно разработанного набора компонентов, которые сходны по своей структуре с более

ранними угрозами семейства Duke. При этом одной из отличительных особенностей CozyDuke является использование методов социальной инженерии. Некоторые электронные письма, в которых используются приемы целевого фишинга, содержат ссылку на взломанные сайты (в том числе на популярные легитимные сайты), на которых размещен ZIP-архив. Этот архив содержит самораспаковывающийся RAR-архив, который устанавливает вредоносное ПО, показывая пустой PDF-файл в качестве подсадной утки. Другой вариант – отправка в качестве вложений к письмам мошеннических флеш-видео. Интересным примером такого видео (по имени которого названо и вредоносное ПО) является OfficeMonkeys LOL Video.zip. Пока воспроизводится приманка-видеоролик с забавным сюжетом об обезьянах, работающих в офисе, зловред загружает на компьютер исполняемый файл CozyDuke. Забавное видео провоцирует сотрудников разослать его коллегам в офисе, что способствует увеличению числа зараженных компьютеров. Успешное использование методов социальной инженерии, чтобы ввести сотрудников в заблуждение и заставить делать то, что поставит под угрозу безопасность компании, – с помощью CozyDuke и других целевых вредоносных программ, – подтверждает необходимость обучения персонала основам корпоративной безопасности.

Атаки APT-группировки Naikon были в основном направлены на важные цели в Юго-Восточной Азии и регионе Южно-Китайского моря. Родным языком злоумышленников, по-видимому, являлся китайский, а действовала группировка уже не менее 5 лет. Их атаки были нацелены в основном на государственные учреждения высокого уровня, гражданские и военные организации таких стран, как Филиппины, Малайзия, Камбоджа, Индонезия, Вьетнам, Мьянма, Сингапур, Непал, Таиланд, Лаос и Китай. Как и во многих других целевых атаках, злоумышленники широко используют приёмы социальной инженерии, чтобы хитростью заставить сотрудников организаций-жертв установить вредоносное ПО на своих компьютерах. Главный модуль Naikon представляет собой утилиту удаленного администрирования, которая поддерживает 48 команд, с помощью которых злоумышленники могут управлять зараженными компьютерами. Среди них – возможность получить полную информацию об аппаратном и программном обеспечении компьютера, загрузить и отправить данные, установить модули расширения, а также использовать программы-кейлоггеры для получения регистрационных данных сотрудников. Каждой стране, на которую нацелены атаки, назначается свой оператор, который использует ее культурные особенности, например привычку использовать свой личный аккаунт в электронной почте для работы. Используется также специальный прокси-сервер внутри страны, который управляет соединениями с зараженными компьютерами и перенаправляет данные на командные серверы злоумышленников. Наш основной отчет и следующий за ним можно прочитать на нашем сайте.

Исследуя операции Naikon, мы также раскрыли деятельность APT-группировки APT-группировки Hellsing. Эта группа нацелена в основном на правительственные и дипломатические организации в Азии: большинство жертв располагалось в Малайзии и на Филиппинах, хотя мы также фиксировали пострадавших в Индии, Индонезии и США. Сама по себе Hellsing – небольшая и технически непримечательная кибершпионская группировка, атаковавшая на данный момент около 20 организаций. Интересно то, что эта группировка стала объектом целевого фишинга со стороны APT-группировки Naikon – и решила нанести ответный удар! Получив электронное сообщение, адресаты просили отправителя подтвердить авторство адресной рассылки. Они получили ответ атакующего, но вложение открывать не стали. Вместо этого через некоторое время они отправляли письмо обратно атакующим, и оно содержало уже другую вредоносную программу. Очевидно, что группировка Hellsing, поняв, что подверглась целевой атаке, решила установить, кто ее организовал и собрать информацию о его деятельности. Мы и раньше сталкивались с тем, что APT-группировки могли случайно наступить на ногу конкуренту, например украсть у жертв электронную адресную книгу и затем делать рассылки по всем адресам списка. но взаимные APT-атаки – вещь необычная.

Многие целевые атаки направлены на крупные предприятия, правительственные структуры и другие известные учреждения. Поэтому читая заголовки, легко представить себе, что для злоумышленников интерес представляют именно такие организации. Однако одна из кампаний, о которой мы рассказывали в прошлом квартале, ясно показала, что злоумышленников интересует не только крупная рыба. Кибершпионская кампания Grabit разработана для кражи данных компаний малого и среднего бизнеса, расположенных в основном в Таиланде, Вьетнаме и Индии, хотя нам встречались ее жертвы и в США, ОАЕ, Турции, России, Китае, Германии и других странах. Мишенями злоумышленников были такие секторы экономики, как химическая промышленность, нанотехнологии, образование, сельское хозяйство, средства массовой информации и строительство. По нашей оценке, группой, стоящей за проведением этих атак, на данный момент украдено около 10 000 файлов. Очевидно, что потенциальной целью для Grabit является любая компания – либо благодаря своим активам, либо как способ проникнуть в другую организацию.

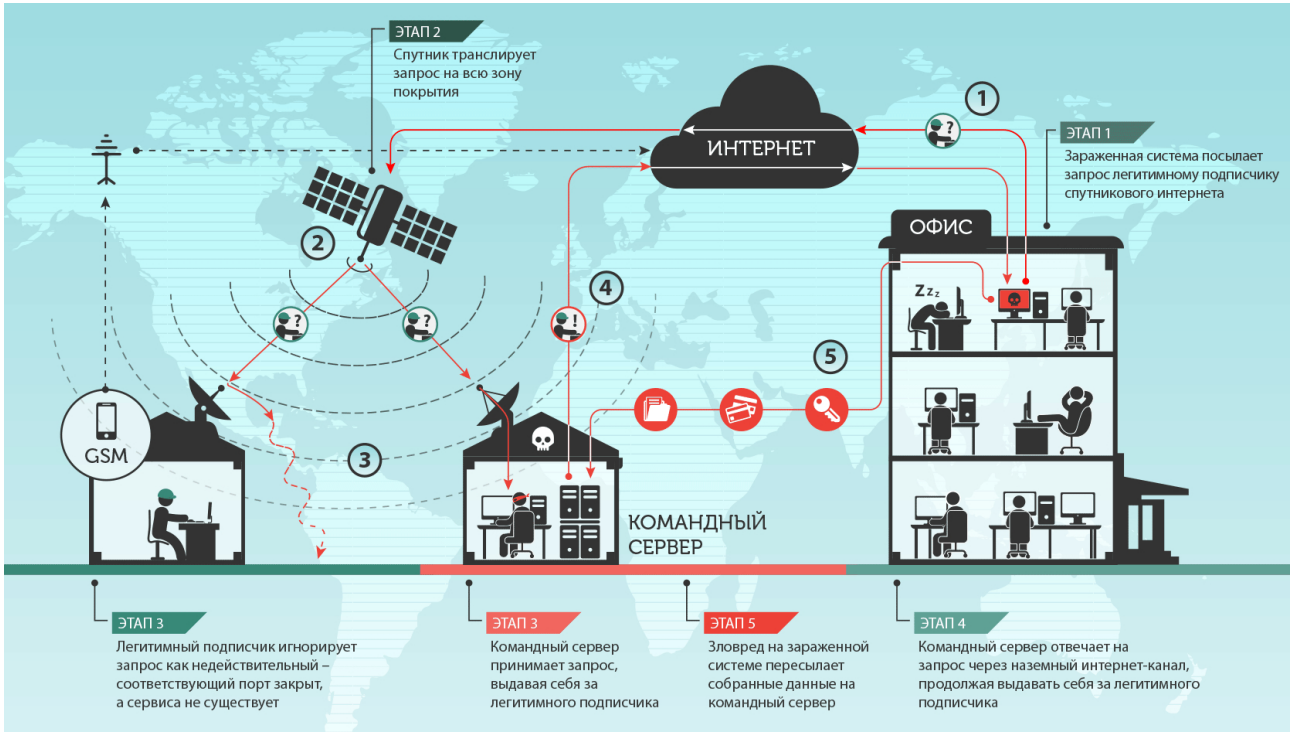
Весной 2015 года в ходе своей плановой проверки безопасности «Лаборатория Касперского» обнаружила попытку вторжения, затрагивающую несколько внутренних систем компании. Было проведено широкомасштабное расследование, в результате которого мы обнаружили новую вредоносную платформу, разработанную одной из наиболее профессионально подготовленных, загадочных и мощных APT-группировок – Duqu, которую еще иногда называют «сводным братом» Stuxnet. Мы дали этой новой вредоносной платформе имя «Duqu 2.0». в атаке на «Лабораторию Касперского» использовалась уязвимость нулевого дня в ядре Windows (закрыта Microsoft 9 июня 2015 года) и, вероятно, еще одна-две уязвимости нулевого дня (на данный момент уже закрытые). Основной задачей злоумышленников был шпионаж: их интересовали технологии, исследования и внутренние процессы «Лаборатории Касперского». При этом «Лаборатория Касперского» была не единственной целью. Некоторые из новых случаев заражения Duqu 2.0 связаны с работой «иранской шестерки» и проведением переговоров с Ираном по ядерной программе. По всей видимости, атаки начались в тех местах, где проходили некоторые из встреч на высоком уровне. Аналогичную атаку группировка предприняла и в связи с мероприятиями, посвященными 70-й годовщиной освобождения Освенцима. Одной из наиболее примечательных особенностей Duqu 2.0 явилось то, что зловред практически не оставляет следов своего присутствия в системе. Эта вредоносная программа не меняет настроек диска или системы, поскольку ее платформа разработана таким образом, что она сохраняется практически исключительно в памяти зараженных систем. Это наводит на мысль о том, что злоумышленники были абсолютно уверены, что они могут сохранить свое присутствие в системе, даже если компьютер конкретной

жертвы будет перезагружен и вредоносные программы будут удалены из памяти. Техническое описание Duqu 2.0 и анализ модуля Duqu 2.0, сохраняющего присутствие в сети можно найти на нашем веб-сайте.

В августе мы писали об APT-группировке Blue Termite, целевые атаки которой были направлены на кражу информации у организаций в Японии. в число жертв группировки вошли правительственные ведомства, местные органы управления, группы общественных активистов, университеты, банки, провайдеры финансовых сервисов, а также компании, работающие в таких отраслях, как энергетика, связь, тяжелая, химическая и автомобильная промышленность, производство электрооборудования, новостные СМИ, информационные услуги, здравоохранение, недвижимость, пищевая промышленность, полупроводники, робототехника, строительство, страхование, транспорт и др. Одной из наиболее заметных жертв группировки стала пенсионная служба Японии. Вредоносное ПО модифицируется с учетом особенностей каждой конкретной жертвы. в коде бэкдора Blue Termite прописаны данные о нем, включая командные серверы, имена API функций, строки для защиты от анализа вредоносного кода, значения мьютексов, а также контрольные суммы (MD5) команд бэкдора и информация о внутреннем прокси-сервере. Данные хранятся в зашифрованном виде, что усложняет анализ вредоносного ПО – для расшифровки каждого образца требуется уникальный ключ. Основной метод заражения, как и во многих других кампаниях, построенных на целевых атаках, – адресная рассылка фишинговых электронных писем. Однако мы обнаружили и другие методы заражения. в их числе drive-by загрузки с применением эксплойта для Flash (CVE-2015-5119) – одного из украденных при взломе Hacking Team, – таким образом были взломаны несколько японских сайтов. Мы также обнаружили атаки типа watering hole, в том числе с использованием сайта, принадлежащего известному члену правительства Японии.

Группировка, стоящая за кибершпионской кампанией Turla, активна уже больше восьми лет (см. наш первый отчет, последующий анализ и обзор вредоносной кампании на сайте Securelist); за это время были заражены сотни компьютеров более чем в 45 странах. Группировка отбирает жертв определенного «профиля», применяя на начальном этапе атаки типа watering hole. При этом, как описано в нашем последнем отчете, в своих дальнейших действиях группа использует спутниковую связь для управления трафиком своих командных серверов. Способ, используемый группировкой Turla для взлома нисходящих спутниковых каналов, не требует подписки на спутниковый интернет. Ключевое преимущество этого метода для киберпреступников состоит в его анонимности – атакующих очень сложно вычислить. Спутниковый приемник может находиться в любом месте зоны покрытия спутника, которая обычно довольно велика, и выявить фактическое местонахождение командного сервера

и физически захватить оборудование сложно. Кроме того, этот метод дешевле, чем покупка подписки на спутниковый интернет, и проще, чем перехват сетевого трафика между жертвой и оператором спутниковой связи и внедрение своих пакетов. Группировка Turla, как правило, выбирает провайдеров спутникового интернета, расположенных на Ближнем Востоке и в Африке, в том числе в Конго, Ливане, Ливии, Нигере, Нигерии, Сомали и ОАЭ. Спутниковый сигнал, передаваемый на эти страны обычно не покрывает страны Европы и Северной Америки, что значительно усложняет для экспертов по безопасности анализ подобных атак. Использование спутникового интернета киберпреступниками – интересный новый ход. Взлом полосы частот нисходящих спутниковых каналов обходится недорого (около 1000 долларов первоначальных инвестиций и примерно такая же сумма в год на текущее обслуживание), прост в реализации и обеспечивает высокий уровень анонимности. с другой стороны, данный метод не всегда так же надежен, как более традиционные методы (абузоустойчивый хостинг, несколько уровней прокси и взломанные веб-сайты) – и все эти методы Turla тоже использует. Это делает менее вероятным его применение для организации крупных ботнетов. Тем не менее, если этот метод получит распространение среди APT-группировок или киберпреступников, это поставит серьезную задачу для перед индустрией IT-безопасности и правоохранительными органами.



В августе 2015 года мы опубликовали обновленный отчет об APT-кампании Darkhotel. Для этих атак изначально было характерно использование краденых сертификатов, внедрение HTA-файлов различными способами и проникновение в гостиничные Wi-Fi сети с целью загрузки бэкдоров на компьютеры жертв.

Продолжая применять упомянутые выше методы, злоумышленники, стоящие за этой APT-кампанией, расширили свой арсенал. в частности, они в большей степени стали концентрировать внимание на адресных фишинговых атаках на выбранных ими жертв. в дополнение к использованию HTA-файлов они также распространяют зараженные RAR-файлы, применяя RTLO-механизм (right to left override) для маскировки настоящих расширений файлов. Злоумышленники также используют Flash-эксплойты, в том числе эксплойт нулевого дня, украденный при взломе Hacking Team. География действий группировки также расширилась – теперь в число её жертв входят пользователи из Северной и Южной Кореи, России, Японии, Бангладеш, Таиланда, Индии, Мозамбика и Германии.

ВЗЛОМЫ И УТЕЧКИ ДАННЫХ

В этом году наблюдался непрерывный поток инцидентов, связанных с нарушением систем безопасности. не приходится удивляться тому, что взломы и утечка данных стали повседневностью: частная информация – это ценная вещь, причем не только для легитимных компаний, но и для киберпреступников. в числе крупнейших инцидентов 2015 года – атаки на Anthem, LastPass, Hacking Team, Управление кадрами США (Us Office of Personnel Management), Ashley Madison, Carphone Warehouse, Experian и TalkTalk. в результате некоторых из них оказались украдены огромные объёмы данных; очевидным стал тот факт, что многие компании не предпринимают соответствующих действий для своей защиты. Дело заключается не только в защите периметра корпоративной сети. Стопроцентной безопасности не существует, и не может быть полной гарантии того, что система защищена от взлома, особенно если кого-либо внутри компании обманом заставят совершить действия, которые поставят под угрозу корпоративную безопасность. с другой стороны, любая организация, которая хранит данные личного характера, обязана обеспечивать их эффективную защиту. Методы такой защиты включают хранение пользовательских паролей в хэшированном и подсоленном виде и шифрование прочих конфиденциальных данных.

С другой стороны, пользователь может минимизировать возможный ущерб в случае взлома на уровне провайдера, выбирая уникальные сложные пароли: идеальный пароль должен быть не короче 15 символов и состоять из комбинации букв, цифр и символов всей клавиатуры. в качестве альтернативы можно пользоваться менеджером паролей, который возьмёт на себя все задачи по созданию надежных паролей и их хранения.

Вообще, тема паролей встаёт вновь и вновь. Если выбрать слишком простой пароль, который легко угадать, то пользователь по сути оказывается незащищенным от возможной кражи идентификационных данных. Проблема усугубляется, если один и то же пароль используется в разных онлайн-аккаунтах – в этом случае взлом одного из них ставит под угрозу безопасность всех учетных записей пользователя. По этой причине в наши дни многие провайдеры, в т.ч. Apple, Google и Microsoft, предлагают двухфакторную аутентификацию, при которой пользователю нужно ввести код, который генерирует аппаратный ключ или который посылается на мобильное устройство пользователя, когда пользователю нужно зайти на сайт или внести изменения в настройки учетной записи. Безусловно, двухфакторная аутентификация повышает уровень безопасности, но только в том случае, когда она обязательно требуется, а не предлагается как вариант.

Кража личных данных может иметь серьезные последствия для тех, кто стал её жертвой. В некоторых случаях, такая кража может вызвать цепную реакцию. Взлом Hacking Team привёл к утечке и публикации 400 ГБ данных, включая информацию об эксплойтах, которые эта итальянская компания использовала в своих программах, предназначенных для слежки. Некоторые из этих эксплойтов использовались в APT-атаках Darkhotel и Blue Termite. Вполне ожидаемо, вскоре после публикации были выпущены патчи к вскрытым уязвимостям.

УМНЫЕ (ЧТО НЕ ЗНАЧИТ «БЕЗОПАСНЫЕ») УСТРОЙСТВА

Интернет стал неотъемлемой частью нашей жизни; к нему каждый день подключается всё большее число бытовых приборов и устройств, используемых в современном доме: «умные» телевизоры, счётчики, видеоняни, чайники и т.д. Читатель, возможно, помнит, как один из наших экспертов изучил свой собственный дом на предмет кибербезопасности. Продолжение истории доступно здесь. Впрочем, «интернет вещей» включает в себя не только устройства, используемые дома.

На протяжении нескольких лет специалисты исследуют потенциальные риски, которые несут в себе автомобили с сетевыми возможностями. в июле 2014 г. «Лаборатория Касперского» и IAB опубликовали обзор потенциальных проблем, связанных с безопасностью «подключенных автомобилей». До этого года исследователи занимались только доступом к системам автомобиля при физическом подключении к нему. Этот подход подвергся пересмотрю, когда исследователи Чарли Миллер и Крис Валашек нашли способ подключиться к критически важным системам автомобиля Jeep Cherokee через беспроводное соединение – они смогли перехватить управление машиной и заставили ее съехать в кювет! (Историю можно прочитать здесь.)

Эта история вскрывает некоторые проблемы, касающиеся всех устройств с возможностью подключения к сети, и эти проблемы выходят далеко за пределы сферы автомобильной промышленности. К сожалению, функции безопасности сложно продать потребителю; на конкурентном рынке важнее оказываются, как правило, те функции, которые облегчают жизнь потребителя. Кроме того, сетевое подключение обычно просто накладывается на уже существующую коммуникационную сеть, при создании которой о безопасности не думали. и наконец, из истории видно, что изменения в исторически сложившуюся систему обычно вносятся только после того, как её слабость с позиции безопасности становится очевидной после какого-либо неприятного события. Подробнее об этой проблематике можно почитать в блогпосте Евгения Касперского, поводом для которого послужило вышеуказанное исследование.

Проблемы такого рода также актуальны и для «умных городов». Например, за последние годы резко выросло использование государственными и правоохранительными структурами систем видеонаблюдения в общественных местах. Многие камеры видеонаблюдения подключаются к интернету по беспроводным каналам, благодаря чему полиция может следить за ними удалённо. Однако такая практика не всегда является безопасной: киберпреступники могут незаметно отслеживать потоки данных с камер, внедрять код в сеть, заменяя данные с камеры поддельными, а также отключать системы. Два эксперта по системам безопасности (Василиос Хиуреас (Vasilios Hioureas) из «Лаборатории Касперского» и Томас Кинзи (Tomas Kinsey) из компании Exigent Systems) недавно провели исследование потенциальных слабых мест в системах видеонаблюдения в одном городе. Отчет Василиоса доступен на нашем сайте.

К сожалению, камеры никак не были скрыты или замаскированы, так что можно было легко увидеть их названия и модели, изучить технические параметры и создать в лаборатории собственную модель. Используемое оборудование было оснащено эффективными средствами безопасности, но они не использовались. Передаваемые по ячеистой сети пакеты данных не шифровались, так что атакующая сторона могла создать свою собственную версию используемого ПО и получить возможность вмешиваться в пересылаемые данные. Злоумышленники могут, в частности, подменять видеопотоки, передаваемые на полицейские участки, и таким образом заставить полицию поверить, что в каком-либо месте произошёл инцидент, и отвлечь ее силы от реального происшествия в другом месте.

Исследователи сообщили о выявленных проблемах соответствующим органам, отвечающим за системы видеобезопасности; проблемы устраняются. Важно, чтобы в этих сетях было внедрено WPA-шифрование, защищенное надежными паролями; с оборудования следует удалять всю маркировку моделей и производителей, чтобы потенциальным злоумышленникам было не так просто выяснить, как работает оборудование; наконец, следует применять шифрование видеоданных, пересылаемых по сети.

Если же посмотреть шире, то проблема заключается в том, что всё больше аспектов нашей каждодневной жизни приобретают «цифровое значение». Если меры безопасности не планируются на этапе разработки, то это может привести к серьезным последствиям, а исправлять задним числом проблемы безопасности может оказаться не таким простым делом. Инициатива Securing Smart Cities, поддерживаемая «Лабораторией Касперского», направлена на то, чтобы помочь ответственным за разработку «умных» городов делать свою работу, не забывая о кибербезопасности.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ ПРОТИВ КИБЕРПРЕСТУПНИКОВ

Киберпреступность стала одной из характерных черт нашего существования – как следствие постоянно растущей активности пользователей онлайн. Теперь этот факт отражается в официальной статистике. Например, Национальная статистическая служба Великобритании теперь включает информацию о киберпреступлениях в свои отчёты по статистике преступности, признавая тем самым, что меняется сама природа преступности в обществе. Без сомнения, киберпреступления могут приносить неплохой доход, но при этом киберпреступники не всегда могут проворачивать свои тёмные дела и оставаться безнаказанными; и здесь многое зависит от действий правоохранительных органов всего мира. в борьбе с киберпреступностью, учитывая его глобальную природу, очень важно международное сотрудничество. в этом году прошли несколько показательных операций правоохранительных органов.

В апреле «Лаборатория Касперского» приняла участие в операции по уничтожению ботнета Simda, координируемой Глобальным инновационным комплексом Интерпола. Это расследование было начато компанией Microsoft, затем круг участников расширился, и к расследованию подключились компания TrendMicro, японский Cyber Defense Institute, сотрудники голландского Национального центра по борьбе с преступлениями в сфере высоких технологий (NHTCU), ФБР, полиция Люксембурга, а также сотрудники Управления «К» МВД России и Национального центрального бюро Интерпола в Москве. в результате совместных действий была остановлена работа 14 командных серверов в Нидерландах, США, Люксембурге, Польше и России. Предварительный анализ некоторых логов sinkhole-серверов, подменивших командные серверы, показал, что от ботнета Simda пострадали 190 стран.

В сентябре полиция Нидерландов арестовала двух человек по подозрению в причастности к атакам с использованием программы-вымогателя CoinVault. Это стало результатом совместных усилий «Лаборатории Касперского», компании Panda Security и голландского Национального центра по борьбе с преступлениями в сфере высоких технологий (NHTCU). Данная вредоносная кампания началась в мае 2014 года и захватила часть текущего года; её жертвы находились более чем в 20 странах, причем большинство – в Нидерландах, Германии, США, Франции и Великобритании. Злоумышленникам удалось зашифровать файлы более чем на 1500 компьютерах

под управлением Windows, а плату за расшифровку данных от жертв требовали в биткойнах. Преступники, стоящие за этой кампанией кибервымогательства, изменяли свои творения несколько раз, чтобы они могли поражать все новые жертвы. в ноябре 2014 года «Лаборатория Касперского» и голландский Национальный центр по борьбе с преступлениями в сфере высоких технологий запустили веб-сайт, действующий как репозиторий для ключей расшифровки, а также разместили в интернете инструмент для расшифровки файлов, чтобы помочь жертвам вернуть свои файлы, не выплачивая выкуп кибервымогателям. Наш анализ разнообразных ухищрений, которые использовали авторы CoinVault, можно найти здесь. Программы-вымогатели стали заметной частью ландшафта угроз. Данный случай показывает, что сотрудничество между экспертами и правоохранительными органами может привести к положительным результатам, и поэтому чрезвычайно важно, чтобы и индивидуальные, и корпоративные пользователи принимали меры для нейтрализации риска, связанного с данным типом вредоносного ПО. Применение программ-вымогателей имеет смысл, только если жертвы готовы платить за расшифровку своих данных. в сентябре агент ФБР внес предложение о том, что пострадавшие должны заплатить требуемую сумму, чтобы восстановить свои данные, – и это вызвало серьезные разногласия. на первый взгляд, это прагматичный подход (хотя бы потому, что бывают случаи, когда восстановить данные по-другому просто невозможно), но он опасен. Во-первых, нет гарантии, что в обмен на деньги киберпреступники предоставят программу, необходимую для расшифровки данных. Во-вторых, получение денег подкрепляет эту преступную бизнес-модель и повышает вероятность того, что в будущем будут создаваться новые программы-вымогатели. Мы бы рекомендовали и компаниям, и индивидуальным пользователям регулярно создавать резервные копии данных – таким образом вы не окажетесь в этой незавидной ситуации.

АТАКИ НА ИНДУСТРИАЛЬНЫЕ ОБЪЕКТЫ

Инциденты, произошедшие из-за проблем с кибербезопасностью, на индустриальных объектах происходят довольно регулярно. Например, по данным US ICS CERT в 2014 финансовом году в США было зафиксировано 245 таких инцидентов, а в июле и в августе 2015 – 22. Однако, по нашему мнению, эти числа не отражают действительной ситуации – киберинцидентов гораздо больше. и если о части инцидентов операторы и владельцы предприятий просто предпочитают молчать, то о другой части они просто не знают.

Давайте посмотрим на два случая, которые привлекли наше внимание в 2015 году.

Во-первых, это инцидент, произошедший в Германии на сталелитейном заводе. в самом конце 2014 года федеральный офис по информационной безопасности Германии (Bundesamt für Sicherheit in der Informations technik, BSI) выпустил отчет (документ на немецком, см. приложение на английском), описывающий киберинцидент, произошедший на одном из сталелитейных предприятий Германии. Результатом этого происшествия стало физическое повреждение доменной печи.

На сегодня это второй после Stuxnet случай кибератаки, повлекшей за собой физическое повреждение промышленного оборудования. По заявлению представителей BSI, изначально посредством фишинговой рассылки была заражена офисная сеть предприятия, а затем хакеры смогли заразить SCADA-компьютер и произвести атаку на оборудование. К сожалению, BSI не предоставил никакой дополнительной информации, и мы не можем сказать, какое именно вредоносное программное обеспечение использовалось и как оно работало.

Такая секретность не полезна всем – операторы аналогичных предприятий (пожалуй, кроме немецких) не могут изучить атаку и внедрить методы противодействия, эксперты по кибербезопасности также пребывают в неведении и тоже не могу предложить клиентам защитные методы.

Другим интересным случаем является атака на аэропорт Фредерика Шопена в Варшаве в июне 2015 года. в один из воскресных дней электронная система подготовки полетных планов польской авиакомпании LOT была выведена из строя приблизительно на 5 часов. По данным Reuters, это вызвало задержку дюжины вылетов.

Деталей менеджмент аэропорта так и не предоставил, и эксперты выражали свое мнение, основываясь на своем опыте. Рубен Сантамарта (Ruben Santamarta), главный консультант по безопасности в компании IOActive, ранее уже обращал внимание на проблемы информационной безопасности в авиации. Основываясь на утверждениях представителей LOT, он предположил, что компания стала жертвой целевой атаки: система не смогла сформировать планы полета из-за того, что были скомпрометированы ключевые узлы бэк-офиса, либо атака была нацелена на устройства наземной связи и привела к неспособности осуществить и валидировать загрузку данных в бортовые компьютеры (в том числе планы полетов).

Наши эксперты тоже отреагировали на инцидент: мы предположили, что есть два возможных сценария этой атаки. Инцидент мог произойти из-за человеческого фактора или сбоя в оборудовании. Либо эта атака на сравнительно небольшой аэропорт Варшавы была лишь предвестником более масштабных действий злоумышленников в других крупных аэропортах мира.

Позже официально было объявлено, что это была DDoS-атака, и на самом деле никакого проникновения не было. но опять же – детальная информация об этом инциденте не раскрывается, и нам остается либо верить официальной информации, либо гадать об истинных причинах и целях атаки.

Кто бы ни стоял за атаками, о которых мы рассказали, и каковы бы ни были их цели, на примере этих атак мы имеем прекрасную возможность убедиться, насколько прочно вошли в нашу жизнь компьютеры и какими уязвимыми стали с годами инфраструктурные объекты.

К сожалению, политика закрытости используется сейчас многими государствами и регуляторами. По нашему мнению, прозрачность и обмен информацией о кибератаках – важная составляющая построения адекватной защиты индустриальных объектов, без этих знаний очень сложно защитить их от будущих угроз.

В заключение хотелось бы отметить еще одну тенденцию, которая уже начала влиять и будет влиять в ближайшие годы на всех нас: оборудование, используемое на промышленных предприятиях, активно подключается к Сети. Конечно же, интернет изобрели достаточно давно, а вот в производственные процессы он приходит на наших глазах. Без преуменьшения эту тенденцию можно назвать индустриальной революцией – рождается «Промышленный интернет вещей» или Предприятие 4.0. в итоге предприятия получают много дополнительных преимуществ и повышают эффективность производства.

Чтобы успеть за этим трендом, производители оборудования просто оснащают необходимыми датчиками и контроллерами проверенное и надежное оборудование, разработанное для мира «без интернета», подключают устройство к Сети и получают «новое оборудование». но они забывают, что с оснащением любого устройства функциями работы с Сетью появляются новые риски и угрозы, связанные с кибербезопасностью, это уже не «физические» устройства, а «киберфизические».

В мире физических устройств все промышленные устройства, приборы, протоколы связи и т.д., проектировались с оглядкой на функциональную безопасность или другими словами – с «защитой от дурака». Это означало, что если устройство спроектировано в соответствии с требованиями функциональной безопасности, то при его эксплуатации без нарушения техники безопасности не должно случиться никаких отказов, не пострадают ни люди, ни экология.

«Предприятие 4.0» получило новое измерение безопасности – безопасность информационную или защиту от намеренного внешнего воздействия. Нельзя просто подключить к интернету объект или устройство родом из «до-интернет эры», последствия такого подключения могут быть, да и бывают, самыми плачевными.

Инженеры, исповедующие старые, «дореволюционные» принципы проектирования, зачастую не учитывают, что теперь с их устройством возможно будет «работать» не только инженер, который знает, что можно делать, а чего нельзя, но и хакер, для которого нет понятия «неразрешенные действия с удаленным объектом». в этом кроется одна из основных причин того, почему сейчас компании с опытом и традициями выпускают хорошее и надежное с точки зрения функциональной безопасности оборудование, которое не обеспечивает достаточный уровень кибербезопасности предприятий.

В мире киберфизических устройств кибер- и физическая составляющие тесно связаны. Кибератака может вывести из строя технологический процесс, повредить оборудование или вызвать техногенную катастрофу. Хакеры – это реальная угроза, а все, что подключено к Сети, может быть атаковано. Поэтому производителям во время разработки нового подключенного индустриального оборудования необходимо прорабатывать меры защиты от киберугроз так же тщательно, как и меры, обеспечивающие функциональную безопасность.

ЗАКЛЮЧЕНИЕ

В 2015 году, пожалуй впервые за историю существования интернета, проблемы защиты сетей и защиты в Сети обсуждались применительно к каждому сектору экономики и повседневной жизни. Выберите любую отрасль современной цивилизации: финансы, промышленное производство, автомобили, самолеты, мобильные устройства, здравоохранение и многое другое, – и вы гарантированно найдете публикации этого года об инцидентах или проблемах кибербезопасности, касающиеся ее.

К сожалению, кибербезопасность теперь неразрывно связана и с проявлениями терроризма в Сети. Методы защиты и нападения в Сети являются объектом значительного интереса различных нелегальных структур и группировок.

Вопросы кибербезопасности вышли на уровень дипломатических ведомств и высших руководителей государств. в этом году были подписаны договоры о кибербезопасности между Россией и Китаем, Китаем и США, Китаем и Великобританией. в рамках этих документов государства обязуются не только сотрудничать, но и не допускать атаки друг на друга. Одновременно активно обсуждались недавние поправки к Вассенаарским соглашениям по ограничению экспорта шпионского программного обеспечения. Одной из главных тем года стало использование незащищенных почтовых сервисов различными политиками по всему миру, включая бывшего (на время событий – действующего) госсекретаря США Хиллари Клинтон.

Все это привело к значительному росту интереса к проблеме кибербезопасности не только со стороны масс-медиа, но и со стороны индустрии развлечений: снимались полнометражные фильмы, сериалы, некоторые эксперты в области кибербезопасности приглашались для участия в фильмах, иногда они играли самих себя.

В 2015 году слово «кибербезопасность» стало модным, но это не значит, что проблема решена. Мы наблюдаем практически экспоненциальный рост во всем, что связано с кибербезопасностью: рост числа атак и атакующих, жертв, расходов на оборону и защиту, законов и договоров, регламентирующих существующие и устанавливающих новые нормы. Мы, со своей стороны, сталкиваемся с заметным увеличением сложности обнаруживаемых атак. Противостояние перешло в активную фазу и до завершающей стадии еще очень и очень далеко.

О том, что нас ждет в ближайшем будущем, читайте в наших прогнозах на 2016 год.

ЭВОЛЮЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИЗНЕС-СРЕДЕ

В конце 2014 года мы опубликовали наше видение того, как будут развиваться события в мире кибер(без)опасности в 2015 году. Четыре из девяти наших прогнозов напрямую были связаны с угрозами для бизнеса, и три пункта из четырех уже сбылись:

- Киберпреступники осваивают целевые атаки APT-класса – да.
- Фрагментация и диверсификация атак APT-групп – да.
- Эскалация атак на банкоматы и PoS-терминалы – да.
- Атаки на виртуальные платежные системы – нет.

Давайте посмотрим, какими в 2015 году были наиболее значительные инциденты и какие новые тренды, связанные с информационной безопасностью в бизнес-среде, мы увидели.

ЦИФРЫ ГОДА

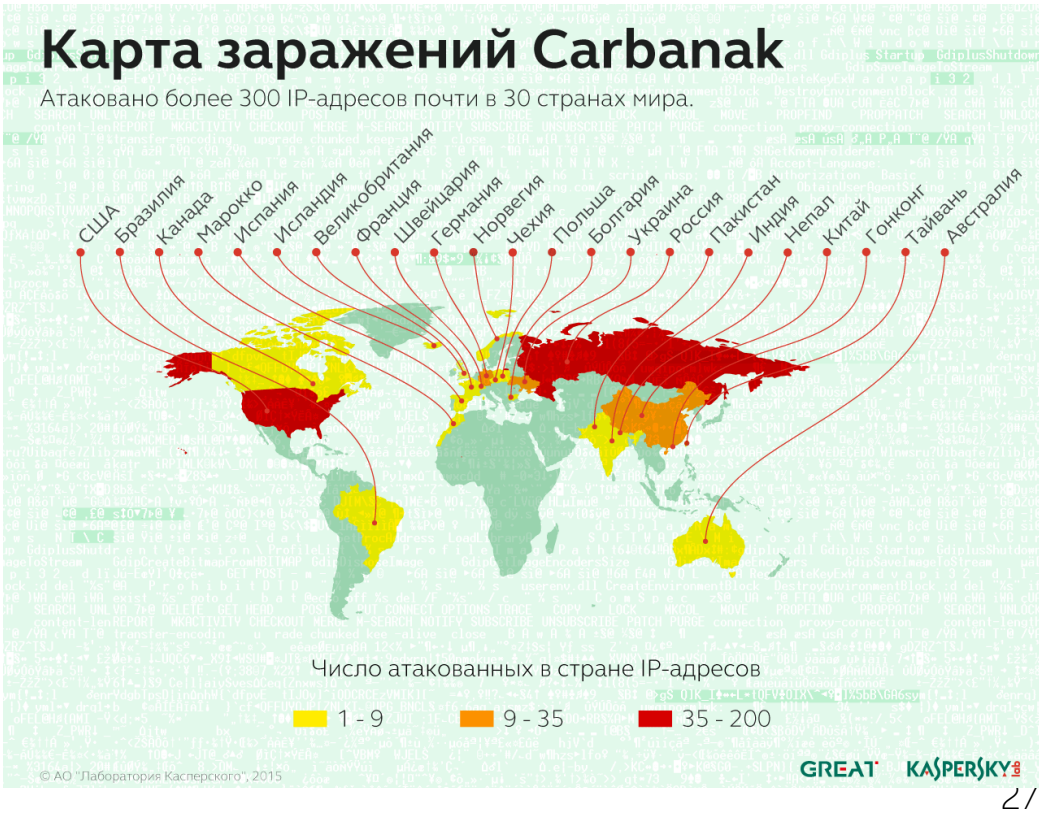
- В 2015 году на 58% корпоративных компьютеров была отражена хотя бы одна атака вредоносного ПО, что на 3 п.п. больше, чем в прошлом году.
- 29% компьютеров, т.е. почти каждый третий компьютер в бизнес-среде, подверглись хотя бы одной атаке через интернет.
- При атаках на бизнес эксплойты к офисным приложениям используются в три раза чаще, чем в атаках на домашних пользователей.
- Файловый антивирус сработал на 41% компьютеров корпоративных пользователей (детектировались объекты, обнаруженные на компьютерах или на съемных носителях, подключенных к компьютерам, — флешках, картах памяти, телефонах, внешних жестких дисках, сетевых дисках).

ЦЕЛЕВЫЕ АТАКИ НА БИЗНЕС: APT И ПРЕСТУПНИКИ

2015 год запомнится рядом атак APT-класса на бизнес. Арсенал и методы, использованные злоумышленниками, были очень похожи на то, с чем мы встречались при разборе APT-атак, но за атаками стояли не государственный структуры, а киберкриминал. Хотя киберпреступники и использовали не характерные для них методы, основная цель атак осталась неизменной — получение финансовой выгоды.

Ярким примером смещения фокуса целевых атак APT-класса на финансовые организации стала операция Carbanak. Это было настоящее ограбление банка в цифровую эру: злоумышленники проникали в сеть банка-жертвы и искали критически важную систему, с помощью которой из атакованной финансовой организации выводили денежные средства. Украв у банка значительную сумму (от 2,5 до 10 млн долларов), преступники искали следующую жертву.

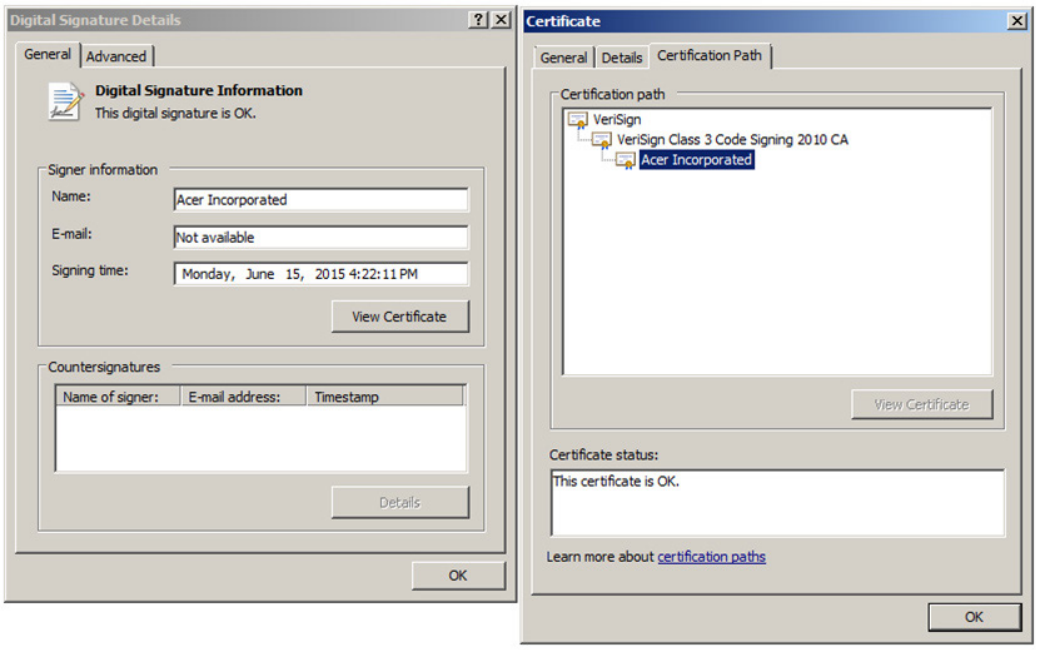
Большинство жертв вредоносной кампании располагалось в Восточной Европе. При этом кампания Carbanak нацелена также и на организации в США, Германии и Китае. Всего же по миру насчитывается более 100 жертв этой атаки, а суммарные убытки пострадавших организаций (в основном это были банки) могут достигать миллиарда долларов.



Не стоит забывать, что информация также может представлять большую ценность, особенно если ее можно использовать при заключении сделок или для игры на различных биржах товаров, ценных бумаг или валют, в том числе криптовалют. Примером целевой атаки, которая могла быть нацелена на получение подобной информации, является Wild Neutron (известна также как Jripbot и Morpho). Впервые эта кампания кибершпионажа получила широкую огласку в 2013 году — тогда от нее пострадало несколько известных компаний, включая Apple, Facebook, Twitter и Microsoft. После того, как эти инциденты получили огласку, организаторы кибершпионской операции свернули свою деятельность. Однако примерно через год «Лаборатория Касперского» зафиксировала возобновление активности Wild Neutron.

Наши исследования показали, что в ходе кампании кибершпионажа были заражены компьютеры пользователей в 11 странах и территориях, а именно в России, Франции, Швейцарии, Германии, Австрии, Словении, Палестине, ОАЭ, Казахстане, Алжире и США. Среди пострадавших — юридические фирмы, инвестиционные компании, организации, работающие с криптовалютой Bitcoin, группы компаний и предприятия, вовлеченные в сделки слияния и поглощения, IT-компании, учреждения здравоохранения, риэлтерские компании, а также индивидуальные пользователи.

Отметим, что в ходе кампании Wild Neutron использовался сертификат подписи кода, украденный у компании Acer.



Подпись компании Acer в установщике Wild Neutron

Тренд на диверсификацию APT-атак хорошо иллюстрирует изменение мишеней атак группировки Winnti. Долгое время считалось, что китайская киберпреступная группировка Winnti атакует только

компании, занимающиеся компьютерными играми. Однако начиная с весны 2015 года стала поступать информация, свидетельствующая о том, что злоумышленники, обкатавшие свои инструменты и методы, стараются получить выгоду от атак на новые мишени. Их интересы больше не ограничивается индустрией развлечений: группировка нацелилась на фармацевтические и телекоммуникационные компании. При анализе новой волны атак Winnti, как и в случае с Wild Neutron, было выявлено, что руткит Winnti подписан украденным сертификатом, принадлежащим одному из подразделений огромного японского конгломерата.

2015 год также отметился расширением географии – как атак, так и атакующих. Например, во время проведения расследования инцидента на Ближнем Востоке экспертами «Лаборатории Касперского» была обнаружена активность неизвестной ранее группировки, проводящей таргетированные атаки. Группа была названа «Соколы Пустыни» (Desert Falcons), она является первой арабской группировкой, проводящей полноценные операции по кибершпионажу. К моменту обнаружения насчитывалось около 300 жертв, среди которых были и финансовые организации.

А группировка Blue Termite атаковала организации и компании в Японии:

Информацию о целевых атаках на бизнес можно узнать в опубликованных «Лабораторией Касперского» отчетах: Carbanak, Wild Neutron, Winnti, DarkHotel 2015, Desert Falcons, Blue Termit, Grabit, более подробные результаты исследования предоставляется подписчикам Kaspersky Intelligence Service.

Анализ данных атак позволяет выделить несколько тенденций развития целевых атак на бизнес:

- Под прицел злоумышленников попали организации, выполняющие различные операции с деньгами: банки, фонды и компании, связанные с биржами, в том числе с биржами криптовалют.
- Атаки тщательно готовятся, злоумышленники исследуют интересы потенциальных жертв (сотрудников атакуемой компании) и выявляют сайты, которые они часто посещают, исследуют контакты жертвы, собирают информацию о поставщиках оборудования и услуг.
- Собранные при подготовке атаки данные активно используются. Атакующие взламывают выявленные легитимные сайты, аккаунты пользователей из бизнес-контактов сотрудников атакуемой компании. Такие сайты/аккаунты используются в течение нескольких часов — с них распространяется вредоносный код, после чего заражение прекращается. Такая схема дает злоумышленникам возможность повторно использовать взломанный ресурс через несколько месяцев.
- Активное использование подписанных файлов и легального ПО для сбора информации из атакованной сети.
- Диверсификация атак, атаки на малый и средний бизнес.
- Расширение географии атак, нацеленных на бизнес: крупная атака в Японии, APT группы из арабского мира.

Хотя атак класса APT, за которыми стоит киберкриминал, относительно немного, тенденции их развития несомненно влияют на подходы и методы, используемые в атаках на бизнес «рядовыми» киберпреступниками.

СТАТИСТИКА

Отметим, что общая статистика по корпоративным пользователям (география атак, рейтинг детектируемых объектов) в принципе совпадает со статистикой по домашним пользователям. Это неудивительно – бизнес-пользователи не существуют в изолированной среде, их компьютеры становятся объектами атак злоумышленников, которые распространяют вредоносные программы без учета специфики атакуемого. Таких атак/зловредов большинство, и данные по атакам, нацеленным именно на бизнес-пользователей, мало влияют на общую статистику.

В 2015 году хотя бы одна атака вредоносного ПО была отражена на 58% корпоративных компьютеров, что на 3 п.п. больше, чем в прошлом году.

Веб-угрозы (атаки через интернет)

В 2015 году 29%, т.е. практически каждый третий компьютер в бизнес-среде, подвергся хотя бы одной атаке через интернет.

TOP 10 вредоносных программ, атаки через интернет

Отметим, что в данном рейтинге представлены только вредоносные программы, мы исключили из него рекламные программы, которые действуют весьма назойливо и доставляют неприятности пользователю, но не наносят вреда компьютеру.

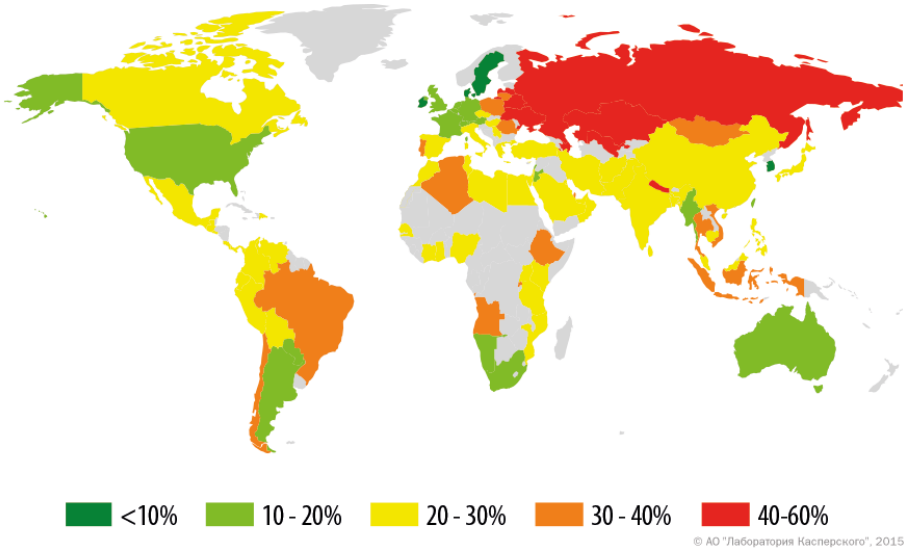
	Название*	% атакованных пользователей**
1	Malicious URL	57,0
2	Trojan.Script.Generic	24,7
3	Trojan.Script.Iframer	16,0
4	Exploit.Script.Blocker	4,1
5	Trojan-Downloader.Win32.Generic	2,5
6	Trojan.Win32.Generic	2,3
7	Trojan-Downloader.JS.Iframe.diq	2,0
8	Exploit.Script.Generic	1,2
9	Packed.Multi.MultiPacked.gen	1,0
10	Trojan-Downloader.Script.Generic	0,9

** Детектирующие вердикты модуля веб-антивируса. Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных*

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

Практически весь TOP 10 состоит из вердиктов, которые присваиваются объектам, использующимся в drive-by атаках, – это различные троянцы-загрузчики и эксплойты.

География веб-атак



География атак через веб-ресурсы, 2015 год (процент атакованных корпоративных пользователей в стране)

Локальные угрозы

Файловый антивирус сработал на 41% компьютеров корпоративных пользователей (детектировались объекты, обнаруженные на компьютерах или на съемных носителях, подключенных к компьютерам, — флешках, картах памяти, телефонах, внешних жестких дисках, сетевых дисках).

TOP 10 вредоносных программ, локальные угрозы

Отметим, что в данном рейтинге представлены только вредоносные программы, мы исключили из него рекламные программы, которые действуют весьма назойливо и доставляют неприятности пользователю, но не наносят вреда компьютеру.

	Название*	% атакованных пользователей**
1	DangerousObject.Multi.Generic	23.1%
2	Trojan.Win32.Generic	18.8%
3	Trojan.WinLNK.StartPage.gena	7.2%
4	Trojan.Win32.AutoRun.gen	4.8%
5	Worm.VBS.Dinihou.r	4.6%
6	Net-Worm.Win32.Kido.ih	4.0%
7	Virus.Win32.Sality.gen	4.0%
8	Trojan.Script.Generic	2.9%
9	DangerousPattern.Multi.Generic	2.7%
10	Worm.Win32.Debris.a	2.6%

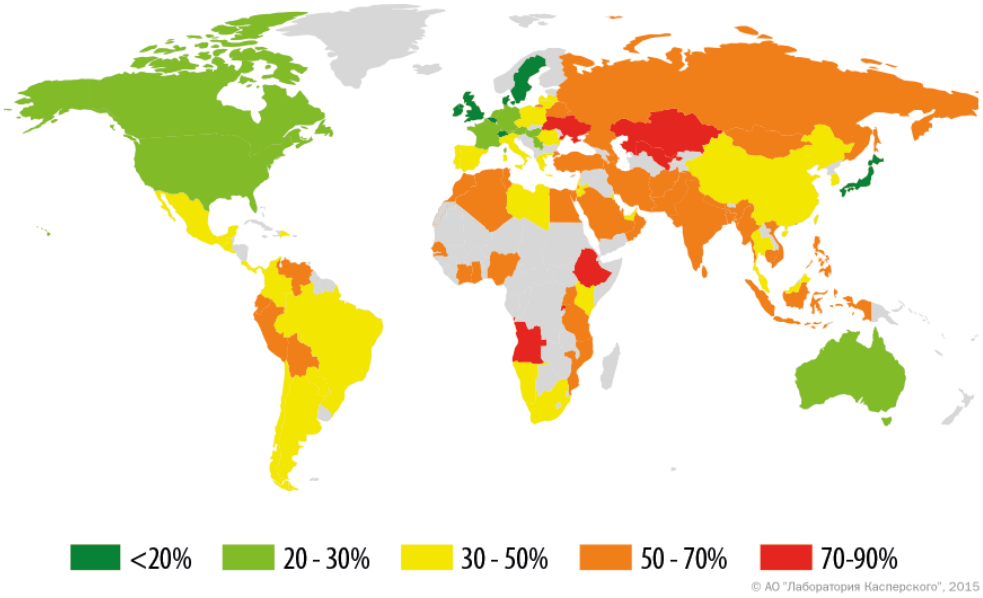
** Детектирующие вердикты модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.*

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

На первом месте различные вредоносные программы, обнаруженные с помощью облачных технологий и детектируемые как DangerousObject.Multi.Generic. Облачные технологии работают, когда в антивирусных базах еще нет ни сигнатуры, ни эвристики для детектирования вредоносной программы, зато у антивирусной компании «в облаке» уже есть информация об объекте. В случае компаний, не желающих отсылать какую-либо статистику в облако, вместо отключения облачных технологий используют Kaspersky Private Security Network, таким образом компьютеры в сети получают защиту из облака.

Остальные представители рейтинга – это, в основном, само-распространяющиеся программы и их компоненты.

География локальных угроз



География обнаружения локальных угроз, 2015 год
(процент атакованных корпоративных пользователей в стране)

ОСОБЕННОСТИ АТАК НА БИЗНЕС

Общая статистика по корпоративным пользователям не отражает специфики атак на бизнес, на нее больше влияет вероятность заражения компьютера в стране или популярность того или иного зловреда у злоумышленников.

Однако более детальный анализ выявляет особенности атак на корпоративных пользователей:

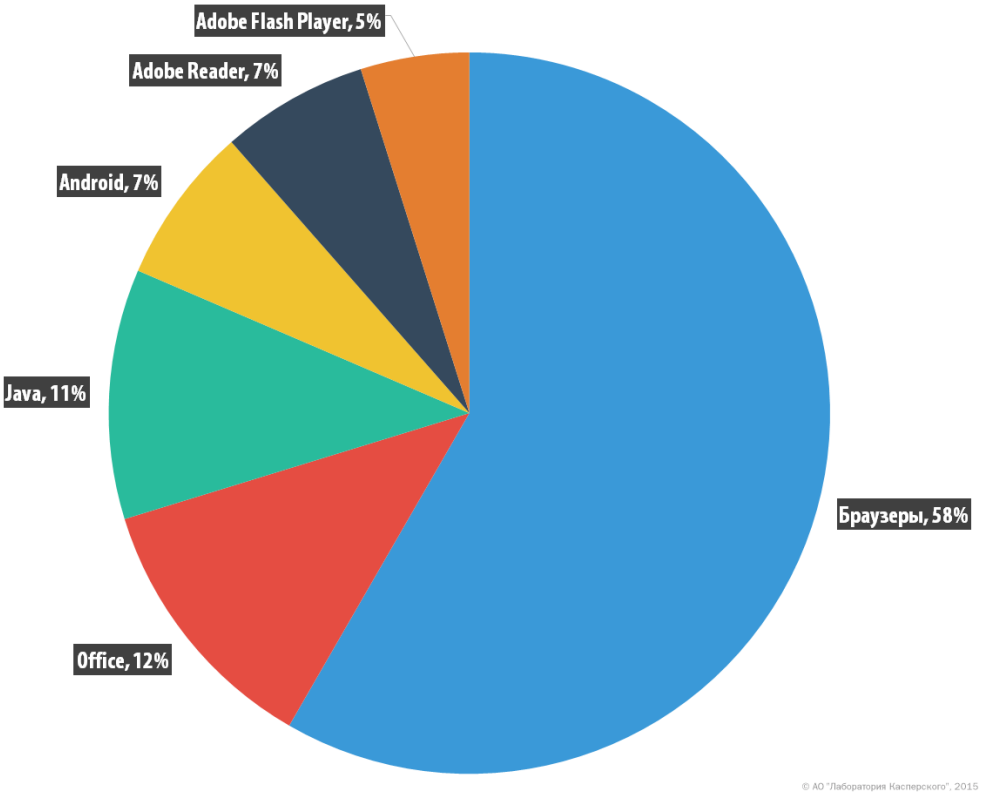
- в 3 раза чаще, чем в атаках на домашних пользователей, используются эксплойты к офисным приложениям,
- используются вредоносные файлы, подписанные валидными цифровыми сертификатами,
- в ходе атак используются доступные легальные программы, что позволяет атакующим дольше оставаться незамеченными.

Кроме того, мы отметили активный рост числа компьютеров корпоративных пользователей, атакованных программами-шифровальщиками.

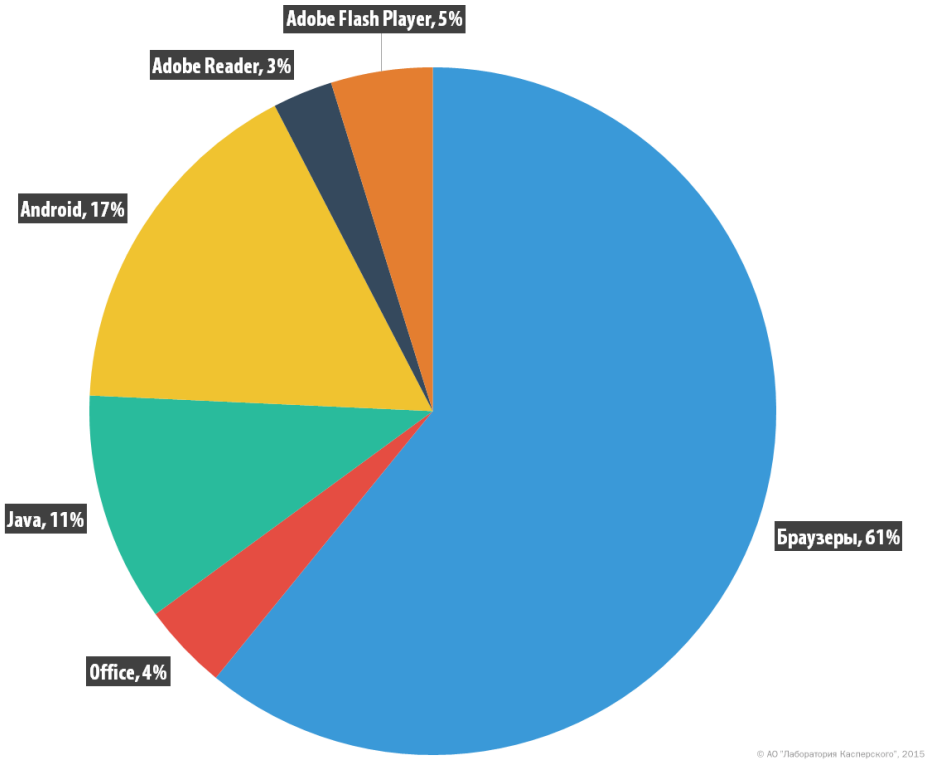
Речь в данном случае далеко не всегда идет об атаках класса APT: «рядовые» злоумышленники фокусируются на корпоративных пользователях — а иногда и на отдельно взятой компании.

Эксплойты в атаках на бизнес

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



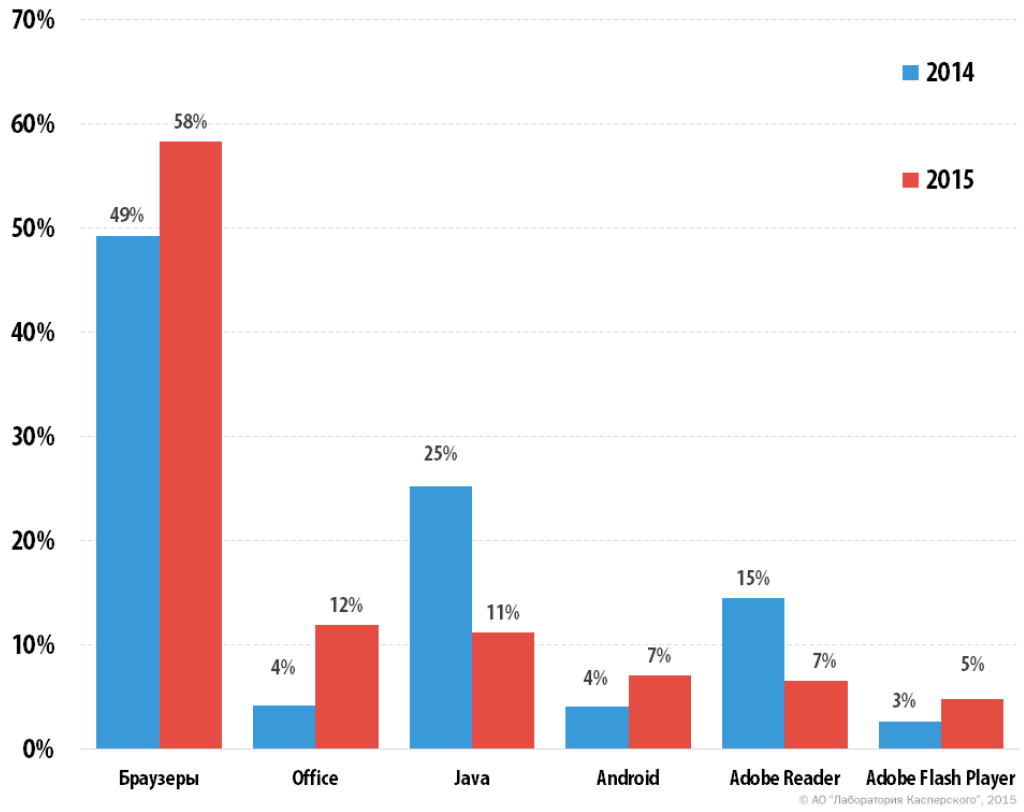
Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений (корпоративные пользователи, 2015 год)



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений (домашние пользователи, 2015 год)

При сравнении эксплойтов, использованных злоумышленниками для атак на домашних и корпоративных пользователей, в первую очередь бросается в глаза значительно более активное использование эксплойтов к офисным программам в атаках на бизнес. Если в атаках на домашних пользователей мы встречали их лишь в 4% случаев, то в атаках на корпоративных пользователей эксплойты для уязвимостей в офисных приложениях составляют 12% от всех обнаруженных за год эксплойтов.

Как и в атаках на домашних пользователей, в атаках на корпоративных пользователей среди атакуемых эксплойтами приложений на первом месте остается категория браузеры. При рассмотрении данной статистики необходимо учитывать, что технологии «Лаборатории Касперского» детектируют эксплойты на различных этапах. В категорию «браузеры» попадают также детектирования лэндинг-страниц, которые «раздают» эксплойты. По нашим наблюдениям, чаще всего это эксплойты к Adobe Flash Player.



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, в 2014 и в 2015 году

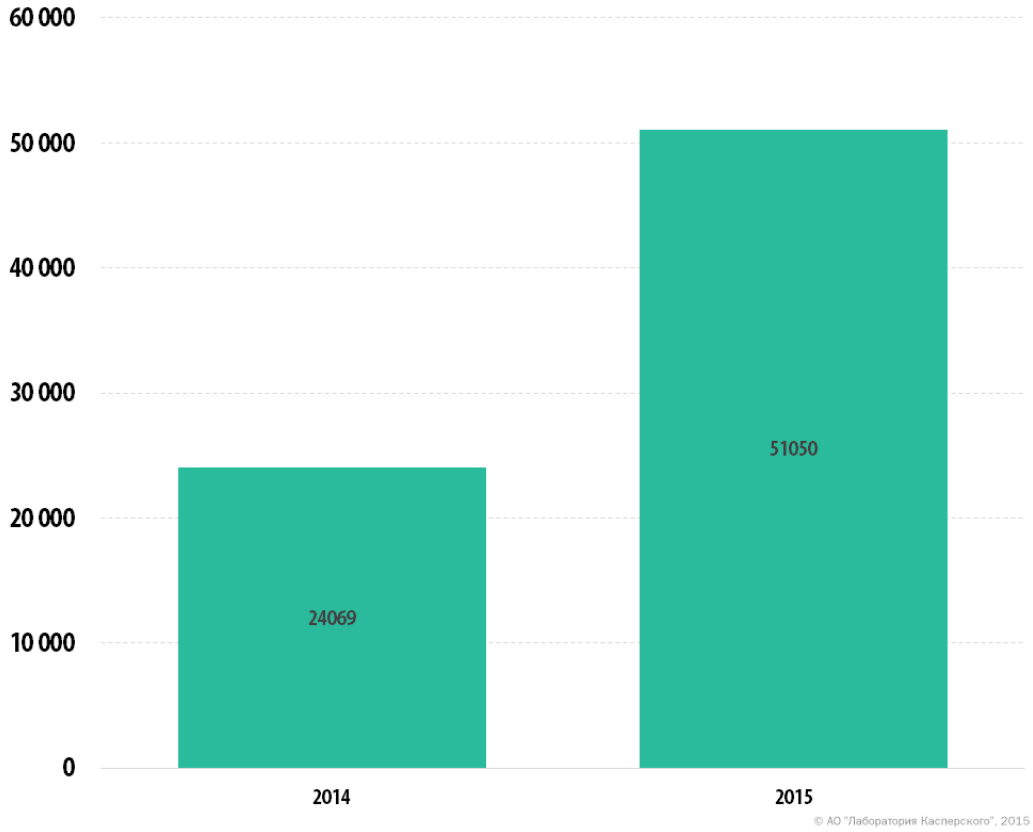
По сравнению с 2014 годом значительно снизилась доля Java- и PDF-эксплойтов — на 14 п.п. и 8 п.п. соответственно. Java-эксплойты стали пользоваться меньшей популярностью, несмотря на то, что в течение года было найдено несколько zero-day уязвимостей. При этом выросла доля атак с использованием уязвимостей в офисных программах (+8 п.п.), браузеров (+9 п.п.), Adobe Flash Player (+9 п.п.), а также Android (+3 п.п.).

Как показывает практика разбора инцидентов безопасности, даже в целевых атаках на корпорации злоумышленники чаще используют эксплойты к уже известным уязвимостям, что обусловлено медленной установкой патчей в корпоративной среде. Рост доли эксплойтов, нацеленных на уязвимые Android-приложения до 7% говорит об увеличивающемся интересе злоумышленников к корпоративным данным на мобильных устройствах сотрудников.

Шифровальщики

Троянцы-шифровальщики долгое время считались угрозой только для домашних пользователей. Теперь же, по нашим данным, злоумышленники, наживающиеся на шифровальщиках, все чаще стали обращать свое внимание на организации.

В 2015 году нашими решениями были обнаружены шифровальщики на более чем **50 тысячах машин** в корпоративных сетях, **что в 2 раза больше, чем годом ранее**. Важно также учитывать, что реальное количество инцидентов в разы больше: данная статистика учитывает только результаты сигнатурного и эвристического детектирования, а продукты «Лаборатории Касперского» в большинстве случаев детектируют троянцы-шифровальщики с помощью поведенческих методов.



Количество уникальных корпоративных пользователей, атакованных троянцами-шифровальщиками в 2014 и 2015 годах

Столь быстро растущий интерес злоумышленников к атакам на бизнес объясняется двумя причинами. Во-первых, сумма, полученная в качестве выкупа от организаций, может быть куда более значительной, чем от пользователей. А во-вторых, шанс, что выкуп будет заплачен, в случае пострадавшей организации выше – компании подчас просто не могут функционировать, если информация на нескольких критичных компьютерах или серверах зашифрована и недоступна.

Одним из самых интересных случаев на этом фронте в 2015 году стало появление первого Linux-шифровальщика (продукты «Лаборатории Касперского» детектируют его как «Trojan-Ransom.Linux.Cryptor»), нацеленного на веб-сайты, в том числе сайты интернет магазинов. Используя уязвимости в веб-приложениях, злоумышленники получали доступ к веб-сайтам и загружали на них вредоносную программу, зашифровывающую данные сервера. В большинстве случаев это приводило к выведению сайта из строя. За расшифровку преступники требовали выкуп в 1 биткойн. Количество зараженных веб-сайтов оценивается в 2 тысячи. Учитывая распространённость *nix-серверов в бизнес-среде, логично предположить, что атаки шифровальщиков, нацеленных на не-Windows платформы, могут получить продолжение в следующем году.

TOP 10 семейств троянцев-шифровальщиков

	Семейство	% атакованных пользователей*
1	Scatter	21
2	Onion	16
3	Cryakl	15
4	Snocry	11
5	Cryptodef	8
6	Rakhni	7
7	Crypmod	6
8	Shade	5
9	Mor	3
10	Crypren	2

** Процент пользователей, атакованных зловредами данного семейства, от всех атакованных пользователей.*

Практически все семейства криптолокеров, вошедшие в TOP 10, требуют в качестве выкупа биткойны.

На первом месте расположились троянцы семейства Scatter, шифрующие файлы на диске и оставляющие зашифрованные файлы с расширением .vault. Семейство Scatter – это многомодульные скриптовые многофункциональные зловреды. За короткое время оно успело значительно эволюционировать, обзаведясь помимо возможности шифрования файлов функциональностью Email-Worm и Trojan-PSW. На втором месте по распространенности

шифровальщики семейства Onion, известные тем, что их командные серверы находятся в сети Tor. На третьем месте – появившиеся еще в апреле 2014 года и написанные на Delphi шифровальщики семейства Cryakl.

В некоторых случаях есть возможность расшифровать данные, зашифрованные этими зловредами – в основном, когда в алгоритме есть какие-либо ошибки. Однако расшифровать данные, которые были зашифрованы последними версиями вредоносных программ, представленных в топе, на сегодняшний день невозможно.

Важно понимать, что для компании заражение подобной программой может обернуться остановкой бизнеса, в случае если будут зашифрованы критически важные данные или в результате шифрования данных будет заблокирована работа критически важного сервера. Следствием подобных атак могут стать огромные убытки, сравнимые с атаками вредоносных программ Wiper, нацеленных на уничтожение данных в компьютерных сетях компаний.

Для борьбы с этой угрозой необходимо применять ряд мер:

- использовать защиту от эксплойтов;
- обязательно включить поведенческие методы детектирования в защитном продукте (в продуктах «Лаборатории Касперского» за это отвечает компонент System watcher);
- настроить процесс резервного копирования данных.

АТАКИ НА POS-ТЕРМИНАЛЫ

Отдельной темой для бизнеса, особенно ведущего торговую деятельность, в 2015 году оказалась безопасность PoS-терминалов (Point Of Sale — точка продажи). По сути сейчас в качестве PoS-терминала может быть использован любой компьютер с подключенным специальным устройством для считывания карт и установленным специальным ПО. Злоумышленники ищут подобные компьютеры и заражают их зловредами, которые позволяют похищать данные карт, проведенных через терминал оплаты.

По всему миру продукты «Лаборатории Касперского» отразили более 11,5 тысяч попыток подобных атак. Сейчас в нашей коллекции 10 семейств программ, нацеленных на кражу данных с PoS-терминалов. 7 из них появились в этом году. Несмотря на небольшое количество попыток атак, не стоит недооценивать опасность, ведь одна успешная атака может скомпрометировать данные десятков тысяч кредитных карт. Столь большое число возможных жертв обусловлено тем, что PoS-терминалы не воспринимаются владельцами и администраторами как объекты, нуждающиеся в защите, поэтому зараженным терминал может оставаться очень долго, и все это время вредоносная программа будет отсылать злоумышленникам считанные терминалом данные кредитных карт.

Эта проблема особенно актуальна в странах, где не используются карты с EMV-чипом. Переход на карты с EMV-чипом должен значительно усложнить задачу получения данных для клонирования карт, но это вопрос достаточно длительного времени. Поэтому требуется принимать хотя бы минимальные меры по защите POS-устройств, благо для них достаточно легко реализуется политика безопасности «запрет запуска неизвестных программ по умолчанию».

Мы ожидаем, что в будущем киберпреступники начнут атаковать мобильные PoS-устройства под управлением Android.

ЗАКЛЮЧЕНИЕ

Наши данные показывают, что инструментарий атак на бизнес отличается от того, что применяют в атаках на домашних пользователей. В атаках на корпоративных пользователей значительно чаще используются эксплойты к офисным приложениям, вредоносные файлы часто оказываются подписанными валидными цифровыми сертификатами, плюс к этому злоумышленники стараются использовать в своих целях доступные легальные программы, чтобы дольше оставаться незамеченными. Кроме того, мы отметили активный рост числа компьютеров корпоративных пользователей, атакованных программами-шифровальщиками. Это касается не только атак класса APT: «рядовые» злоумышленники целенаправленно атакуют корпоративных пользователей, а иногда – сотрудников конкретных компаний.

Использование киберкриминальными группировками, атакующими бизнес, методов и программ из мира APT переводит эти атаки на другой уровень и делает их значительно более опасными. В первую очередь киберпреступники стали применять эти методы для проведения атак на банки с целью вывода крупных сумм денег. Этими же методами они могут выводить со счетов в банках и деньги компаний, получив доступ к сети организации.

В своих атаках криминал полагается на использование уже известных уязвимостей, что связанно с медленной установкой обновлений для ПО в организациях. Кроме того, злоумышленники активно используют подписанные вредоносные файлы и легальные инструменты для создания канала вывода информации: в ход идут известные программы для удаленного администрирования, SSH-клиенты, программы для восстановления паролей и т.д.

Все чаще объектами атак злоумышленников становятся серверы организаций. Помимо кражи данных, известны случаи, когда атакованные серверы использовались в качестве инструмента DDoS атак, или данные просто шифровались, и злоумышленники требовали выкуп. Последние события показали, что это утверждение справедливо как для Windows-, так и для Linux-серверов.

Многие организации, которые стали жертвами атак, столкнулись с требованиями злоумышленников заплатить выкуп за остановку DDoS-атаки, расшифровку данных или за неразглашение украденной информации. Когда организация сталкивается с этим, в первую очередь нужно обращаться в правоохранительные органы и к специалистам по компьютерной безопасности. Потому что, получив выкуп, преступники могут не сдержать слово, как в случае с DDoS-атакой на компанию ProtonMail, которая не остановилась после получения денег.

ПРОГНОЗЫ

Увеличение количества атак на финансовые организации, совершение финансовых махинаций на биржах

В будущем году мы ожидаем как увеличения количества атак на финансовые организации, так и изменения качества таких атак. Помимо перевода денег на свои счета с последующим обналичиванием, злоумышленники могут применять новые техники, в том числе связанные с манипуляцией данными на торговых площадках, где работают как с традиционными, так и с новыми финансовыми инструментами, такими как криптовалюты.

Атаки на инфраструктуру

Практически все ценные данные организаций подчас расположены не в самой организации, а на серверах в датацентрах. Получение доступа к этим элементам инфраструктуры и будет одним из важных векторов атак на компании в 2016 году.

Использование уязвимостей в IoT для проникновения в сети организаций

Практически во всех современных корпоративных сетях сегодня есть IoT устройства. Исследования, проведенные в 2015 году, показали, что существует ряд проблем с безопасностью этих устройств, чем очевидно попробуют воспользоваться злоумышленники, используя их в качестве первой ступени проникновения в сеть организации.

Более жесткие стандарты безопасности, кооперация с правоохранительными органами

Ответом регуляторов на увеличивающееся количество компьютерных инцидентов в бизнес-среде и в целом на изменение ландшафта киберугроз будет разработка новых и обновление уже принятых стандартов безопасности. Организации, заинтересованные в сохранности своих цифровых ценностей, будут активнее сотрудничать с правоохранительными органами, либо упомянутые выше стандарты их к этому обяжут. Это может привести к более эффективной работе по поимке киберпреступников, и в 2016 году мы узнаем о новых арестах.

ЧТО ДЕЛАТЬ?

2015 год показал, что киберпреступники активно стали использовать методы APT-атак для проникновения в сети компаний. Здесь мы говорим и о предварительной разведке с целью выявления слабых звеньев в инфраструктуре и получении информации о сотрудниках, и об использовании spearphishing и waterhole-атак, активном использовании эксплойтов для выполнения кода и получения прав администратора, а также об использовании в атаках помимо троянских программ легального ПО для удаленного администрирования, изучения сети и «восстановления» паролей. Все это требует развития методов и технологий защиты сетей предприятий.

Переходя к конкретным рекомендациям, первым делом, стоит обратить внимание на ТОР 35 стратегий по нейтрализации атак на предприятия, составленный управлением радиотехнической обороны Австралии. Проведя всесторонний детальный анализ локальных атак и угроз, ASD пришло к выводу, что не менее 85% целевых кибервторжений можно нейтрализовать применением четырех базовых стратегий. Три из этих стратегий связаны с использованием специализированных защитных решений (в состав продуктов «Лаборатории Касперского» входят технологические решения, охватывающие эти три важнейшие стратегии).

Четыре основные стратегии, снижающие вероятность успешной целевой атаки:

- Применение белых списков приложений позволяет заблокировать выполнение вредоносного ПО и неутвержденных программ.
- Установка исправлений для Java, Flash, программ просмотра PDF-файлов, веб-браузеров и пакета Microsoft Office.
- Исправление уязвимостей в операционной системе при помощи патчей.
- Ограничение прав административного доступа к операционной системе и приложениям, исходя из служебных обязанностей каждого пользователя.

Более подробную информацию о стратегиях ASD можно найти в документе о стратегиях нейтрализации угроз в энциклопедии Securelist.

Вторым важным фактором является использование данных об актуальных угрозах, т.е. сервисов Threat Intelligence (например, «Лаборатория Касперского» предоставляет услуги Kaspersky Intelligence Service). Своевременная настройка и проверка сети на основе этих данных позволяет защититься от атаки либо выявить атаку на ранних стадиях.

Основные же принципы обеспечения безопасности в корпоративных сетях остаются прежними:

- Обучение персонала, ведь информационная безопасность — это не только забота службы безопасности, но и обязанность каждого отдельно взятого сотрудника.
- Налаживание процессов безопасности: система безопасности должна адекватно отвечать на эволюционирующие угрозы.
- Использование новых технологий и методов: каждый дополнительный слой защиты позволяет снизить риск проникновения в сеть.

ОСНОВНАЯ СТАТИСТИКА ЗА 2015 ГОД

ЦИФРЫ ГОДА

- В 2015 году решения «Лаборатории Касперского» отразили попытки атак вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам на **1 966 324** компьютерах пользователей.
- Программы-вымогатели обнаружены на **753 684** компьютерах уникальных пользователей, при этом программами-шифровальщиками было атаковано **179 209** компьютеров.
- В течение года нашим веб-антивирусом было задетектировано **121 262 075** уникальных вредоносных объектов (скрипты, эксплойты, исполняемые файлы и т.д.).
- Решения «Лаборатории Касперского» отразили **798 113 087** атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира.
- **34,2%** компьютеров пользователей интернета в течение года хотя бы раз подвергались веб-атаке.
- Для проведения атак через интернет злоумышленники воспользовались **6 563 145** уникальными хостами.
- **24%** веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в США.
- Нашим файловым антивирусом на компьютерах пользователей задетектировано **4 миллиона** вредоносных и потенциально нежелательных программ.

УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ

В 2015 году мы наблюдали использование новых техник маскировки эксплойтов, шеллкодов и полезной нагрузки с целью затруднить обнаружение заражения и анализ вредоносного кода. В частности, злоумышленники:

- Использовали криптографический протокол Диффи-Хеллмана
- Прятали эксплойт-пак во Flash-объекте

Одним из знаменательных событий года стало обнаружение двух семейств критических уязвимостей под Android. Эксплуатация уязвимостей Stagefright позволяла атакующему, отправившему специально подготовленную MMS на номер жертвы, удаленно выполнить произвольный код на ее устройстве. Эксплуатация Stagefright 2 производилась с той же целью, но уже с помощью специально подготовленного медиафайла.

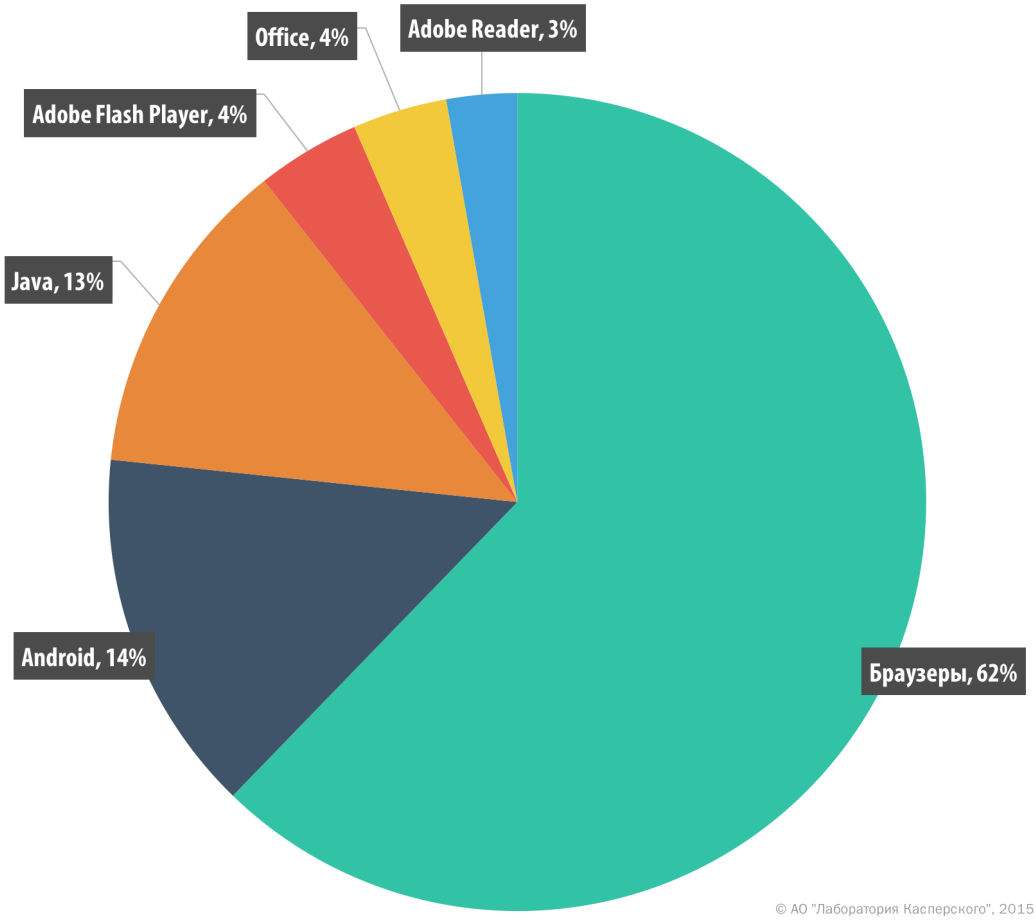
В 2015 году у вирусописателей пользовались популярностью эксплойты для Adobe Flash Player. Это можно объяснить тем, что в течение года было найдено большое количество уязвимостей в данном продукте. Кроме того, в результате утечки данных от Hacking Team в публичном доступе оказалась информация о неизвестных уязвимостях во Flash Player, чем и воспользовались злоумышленники.

Разработчики различных эксплойт-паков оперативно реагировали на обнаружение новых уязвимостей в Adobe Flash Player и добавляли новые эксплойты в свои продукты. Вот «чертова дюжина» востребованных злоумышленниками уязвимостей в Adobe Flash Player, поддержка которых была добавлена в распространенные эксплойт-паки:

1. CVE-2015-0310
2. CVE-2015-0311
3. CVE-2015-0313
4. CVE-2015-0336
5. CVE-2015-0359
6. CVE-2015-3090
7. CVE-2015-3104
8. CVE-2015-3105
9. CVE-2015-3113
10. CVE-2015-5119

11. CVE-2015-5122
12. CVE-2015-5560
13. CVE-2015-7645

Традиционно в некоторые известные эксплойт-паки входил эксплойт для уязвимости в Internet Explorer (CVE-2015-2419). Также в 2015 году было зафиксировано использование уязвимости в Microsoft Silverlight (CVE-2015-1671) для заражения пользователей. Впрочем, данный эксплойт не пользуется популярностью среди основных «игроков» на рынке эксплойтов.



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, 2015 год

Рейтинг уязвимых приложений 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.

Хотя доля эксплойтов для Adobe Flash Player в нашем рейтинге составляет всего 4%, «в дикой природе» они встречаются довольно часто. При рассмотрении данной статистики необходимо учитывать, что технологии «Лаборатории Касперского» детектируют эксплойты

на различных этапах. В результате в категорию «Браузеры» (62%) попадают также детектирования лэндинг-страниц, которые «раздают» эксплойты. И по нашим наблюдениям, такие страницы чаще всего загружают именно эксплойты к Adobe Flash Player.

В течение года мы наблюдали снижение количества случаев использования Java-эксплойтов. Если в конце 2014 года их доля среди всех заблокированных эксплойтов составляла 45%, то за этот год она постепенно уменьшилась на 32 п.п. – до 13%. Более того, на данный момент Java-эксплойты полностью исключены из всех известных эксплойт-паков.

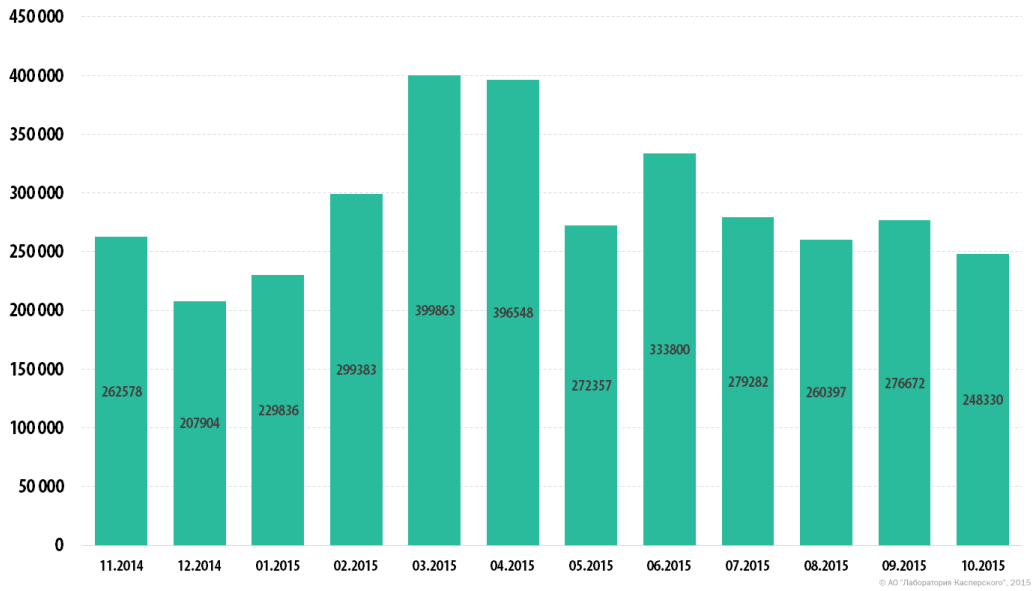
В то же время мы отметили рост использования эксплойтов для Microsoft Office – с 1 до 4%. Согласно нашим наблюдениям, в 2015 году эти эксплойты распространялись посредством массовых почтовых рассылок.

ФИНАНСОВОЕ ВРЕДОНОСНОЕ ПО

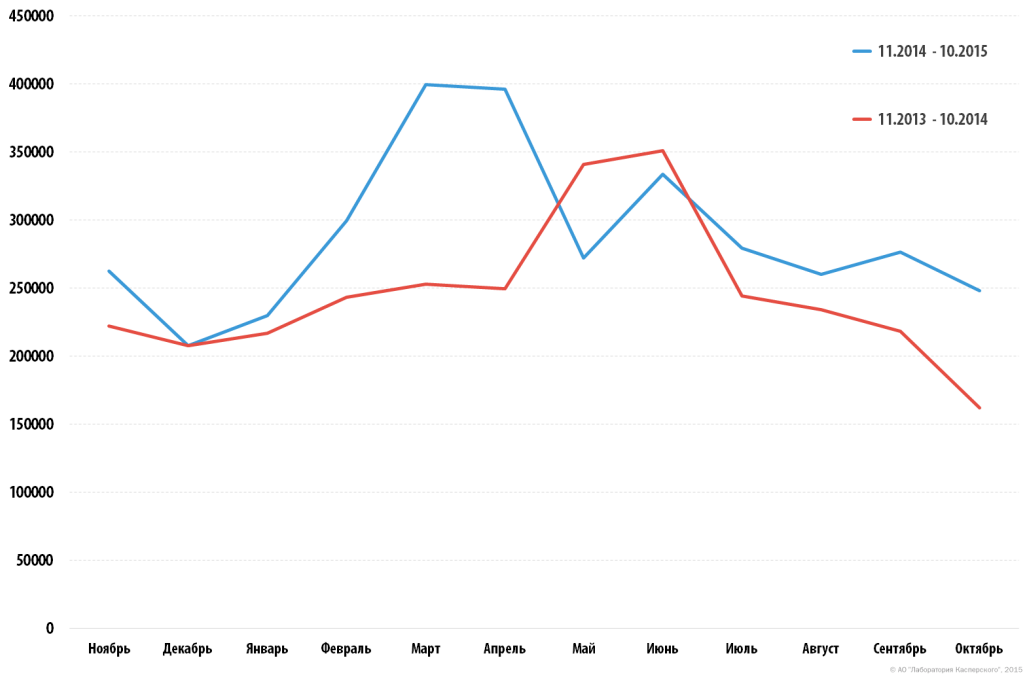
Настоящая статистика основана на детектирующих вердиктах продуктов «Лаборатории Касперского», которые были предоставлены пользователями, подтвердившими свое согласие на передачу статистических данных.

Годовая статистика за 2015 год составлена на основе данных следующего отчетного периода: ноябрь 2014 – октябрь 2015.

В 2015 году решения «Лаборатории Касперского» отразили попытки атак вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам на **1 966 324** компьютерах пользователей. По сравнению с 2014 годом (**1 910 520**) данный показатель увеличился на 2,8%.



Число пользователей, атакованных финансовым вредоносным ПО, ноябрь 2014 – октябрь 2015 года

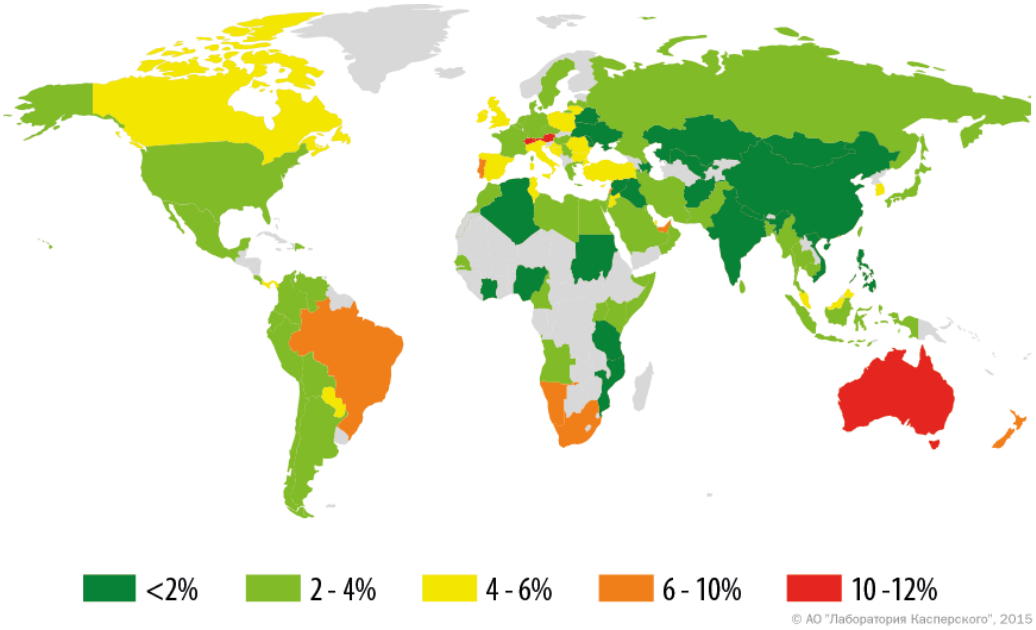


Число пользователей, атакованных финансовым вредоносным ПО в 2014 и 2015 годах

В 2015 году активность финансового вредоносного ПО росла в период с февраля по апрель с максимальными показателями в марте-апреле. Еще один всплеск был зафиксирован в июне. В 2014 году больше всего пользователей было атаковано финансовыми зловредами в мае-июне. С июня по октябрь в 2014 и 2015 годах количество атакованных пользователей постепенно уменьшалось.

География атак

Чтобы оценить популярность финансового вредоносного ПО у злоумышленников и риск, которому подвергаются компьютеры пользователей в разных странах мира, мы подсчитали в каждой стране процент пользователей продуктов «Лаборатории Касперского», которые столкнулись с этой угрозой в отчетный период, от всех атакованных уникальных пользователей наших продуктов в стране.



География атак банковского вредоносного ПО в 2015 году (процент пользователей, атакованных банковскими троянцами, от всех атакованных зловредами пользователей)

TOP-10 стран по проценту атакованных пользователей в 2015 году

	Страна*	% атакованных пользователей**
1	Сингапур	23,1
2	Австрия	18,8
3	Швейцария	7,2
4	Австралия	4,8
5	Новая Зеландия	4,6
6	Бразилия	4,0
7	Намибия	4,0
8	Гонконг	2,9
9	ЮАР	2,7
10	Ливан	2,6

** При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского», относительно мало (меньше 10 тысяч).*

*** Процент уникальных пользователей «Лаборатории Касперского», подвергшихся атакам финансовых зловредов, от всех атакованных уникальных пользователей продуктов «Лаборатории Касперского» в стране.*

Лидером этого рейтинга стал Сингапур. В этой стране из всех атакованных зловредами пользователей «Лаборатории Касперского» хотя бы раз в течение года с банковскими троянцами столкнулись 11,6% пользователей. Этот факт иллюстрирует популярность финансовых угроз по отношению ко всем угрозам в данной стране.

В Испании с банковскими троянцами хотя бы раз в течение года столкнулись 5,4% атакованных пользователей, в Италии — 5,0%, в Британии – 5,1%, в Германии - 3,8%, во Франции – 2,9%, в США данный показатель составил 3,2%, в Японии – 2,5%.

В России с банковскими троянцами столкнулись 2,0% атакованных пользователей.

TOP 10 семейств банковского вредоносного ПО

TOP 10 семейств вредоносных программ, использованных для атак на пользователей онлайн-банкинга в 2015 году (по доле атакованных пользователей):

	Название*	% атакованных пользователей**
1	Trojan-Downloader.Win32.Upatre	42,36
2	Trojan-Spy.Win32.Zbot	26,38
3	Trojan-Banker.Win32.ChePro	9,22
4	Trojan-Banker.Win32.Shiotob	5.10
5	Trojan-Banker.Win32.Banbra	3,51
6	Trojan-Banker.Win32.Caphaw	3,14
7	Trojan-Banker.AndroidOS.Faketoken	2,76
8	Trojan-Banker.AndroidOS.Marcher	2,41
9	Trojan-Banker.Win32.Tinba	2,05
10	Trojan-Banker.JS.Agent	1,88

** Детектирующие вердикты продуктов «Лаборатории Касперского». Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.*

*** Процент уникальных пользователей, атакованных данным зловредом, от всех пользователей, атакованных финансовым вредоносным ПО.*

Подавляющее большинство семейств зловредов, попавших в TOP 10, используют классическую для банковских троянцев технику внедрения произвольного HTML-кода в отображаемую браузером веб-страницу и последующего перехвата платежных данных, вводимых пользователем в оригинальные и добавленные троянцем веб-формы.

Зловреды семейства Trojan-Downloader.Win32.Upatre на протяжении всего года лидируют в данном рейтинге. Размер троянцев не превышает 3,5 Кб, а их функции ограничиваются загрузкой «полезной нагрузки» на зараженный компьютер – чаще всего это троянцы-банкеры семейства, известного как Dyre/Dyzap/Dyreza. Основной задачей банковских троянцев этого семейства является кража платежных данных пользователя. Для этого Dyre использует перехват данных банковской сессии между браузером жертвы и веб-приложением онлайн-банкинга – другими словами, реализует технику «Man-in-the-Browser» (MITB). Отметим, что данный зловред активно

распространяется и посредством специально сформированных электронных писем, в которых содержится вложение – документ с загрузчиком. Кроме того, летом 2015 года загрузчик Trojan-Downloader.Win32.Upatre был замечен на скомпрометированных домашних роутерах, что говорит о многоцелевом использовании этого троянца злоумышленниками.

Другой бессменный резидент данного рейтинга — Trojan-Spy.Win32.Zbot (второе место), также уверенно держит свои позиции. Его постоянное присутствие на верхних строчках рейтинга неслучайно. Троянцы семейства Zbot одними из первых стали использовать веб-инжекты для компрометации платежных данных пользователей систем онлайн-банкинга и модификации содержимого банковских веб-страниц. Они использовали несколько уровней шифрования своих конфигурационных файлов и при этом сам расшифрованный файл конфигурации не хранится в памяти целиком, а загружается по частям.

Представители семейства троянцев Trojan-Banker.Win32.ChePro были впервые обнаружены в октябре 2012 г. Тогда троянцы атаковали преимущественно пользователей из Бразилии, Португалии и России, в настоящее время его используют для атак на пользователей многих стран. Большинство образцов ChePro – загрузчики, которым для успешной атаки необходимы другие файлы. Как правило, это банковские вредоносные программы, позволяющие делать снимки экрана, регистрировать клавиатурные нажатия и читать содержимое буфера копирования, т.е. имеющие функционал, дающий возможность использовать вредоносную программу для атаки практически на любые системы онлайн-банкинга.

Отметим, что в этом рейтинге присутствуют два семейства мобильных банковских троянцев: Faketoken и Marcher. Зловреды этих семейств воруют платежные данные с мобильных устройств под управлением операционной системы Android.

Представители семейства Trojan-Banker.AndroidOS.Faketoken работают в паре с компьютерными банковскими троянцами. Для их распространения киберпреступники используют технологии социальной инженерии: когда клиент банка с зараженного компьютера посещает страницу онлайн-банкинга, троянец модифицирует эту страницу, предлагая загрузить Android-приложение, которое якобы будет защищать транзакции. На самом деле ссылка ведет на вредоносное приложение Faketoken. После того как зловред оказывается на смартфоне жертвы, преступники через зараженный банковским троянцем компьютер пользователя получают доступ к банковскому счету, а зараженное мобильное устройство позволяет им перехватывать одноразовый пароль двухфакторной аутентификации (mTAN).

Второе семейство мобильных банковских троянцев – Trojan-Banker.AndroidOS.Marcher. Заразив мобильное устройство, зловреды отслеживают запуск всего двух приложений: клиента мобильного банкинга одного из европейских банков и Google Play. В случае если пользователь входит в магазин Google Play, Marcher демонстрирует пользователю фальшивое окно для ввода данных о платежной карте, которые затем попадают к злоумышленникам. Аналогичным образом троянец действует и в случае открытия пользователем банковского приложения.

На десятом месте рейтинга находится семейство Trojan-Banker.JS.Agent – вредоносный JS-код, который является результатом процедуры инжекта в страницу онлайн-банкинга. Задача данного кода – перехватить платежные данные, которые пользователь вводит в формы на странице онлайн-банкинга.

2015 – ИНТЕРЕСНЫЙ ГОД ДЛЯ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Троянцы-вымогатели – это класс вредоносного ПО, которое вносит несанкционированные изменения в пользовательские данные (это, например, программы-шифровальщики) или блокирует нормальную работу компьютера. Для расшифровки данных и разблокировки компьютера владельцы вредоносных программ обычно требуют от жертв выплаты определенной суммы денег («выкупа»).

С момента появления CryptoLocker в 2013 году, программы-вымогатели прошли длинный путь развития. Например, в 2014 году был обнаружен первый вымогатель для ОС Android. Всего через год уже 17% всех случаев заражения вымогателями приходилось на программы-вымогатели, созданные для ОС Android.

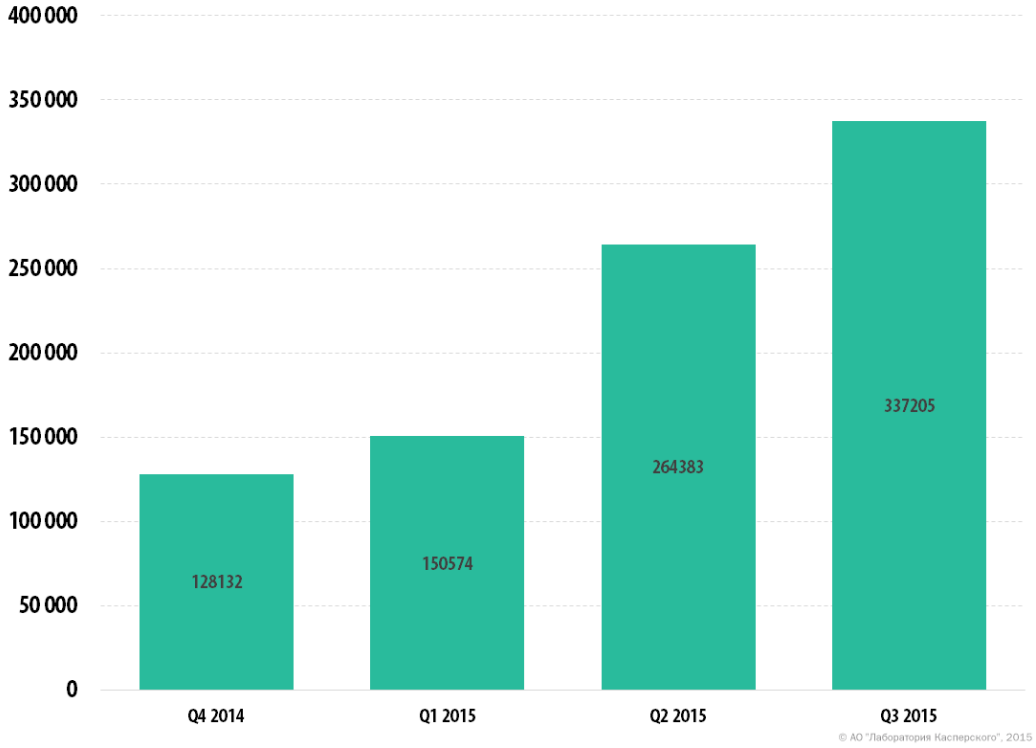
В 2015 году появилась первая программа-вымогатель для Linux – она относится к классу Trojan-Ransom.Linux. К счастью, создатели зловреда допустили небольшую ошибку при реализации программы, что позволяет расшифровать данные без выплаты выкупа.

К сожалению, такие ошибки при реализации допускаются все реже и реже. ФБР заявило по этому поводу следующее: «Программы-вымогатели сделаны настолько хорошо... Скажем прямо: мы часто рекомендуем просто заплатить требуемую сумму». То, что такой план не всегда разумен, стало понятно в этом году, когда голландская полиция смогла задержать двоих подозреваемых, связанных с вредоносной программой CoinVault. Чуть позже они выдали все 14 000 ключей шифрования, которые «Лаборатория Касперского» внесла в свой новый инструмент дешифровки. В результате все жертвы CoinVault смогли расшифровать свои файлы бесплатно.

Кроме всего прочего, 2015 год ознаменовался появлением зловреда TeslaCrypt. Он известен в том числе благодаря использованию графических интерфейсов других семейств программ-вымогателей: сначала авторы зловреда позаимствовали интерфейс CryptoLocker, затем CryptoWall. В последнем случае они полностью скопировали HTML-страницу из CryptoWall 3.0, изменив только ссылки.

Число пользователей, подвергшихся атакам

На следующем графике представлен рост числа пользователей, ставших жертвами программ-вымогателей в прошедшем году:



Число пользователей, атакованных троянцами-вымогателями (Q4 2014 г. – Q3 2015 г.)

За весь 2015 год программы-вымогатели обнаружены на **753 684** компьютерах. Таким образом вымогатели становятся все большей проблемой.

TOP 10 наиболее распространенных семейств троянцев-вымогателей

Ниже представлен список десяти наиболее широко распространенных семейств троянцев-вымогателей. В список вошли семейства браузерных вымогателей, блокировщиков и некоторых хорошо известных шифровальщиков. Несколько лет назад были очень популярны так называемые блокировщики Windows, которые ограничивают доступ к системе (например, семейство Trojan-Ransom.Win32.Blocker) и требуют выкупа – начали они распространяться в России, а затем переместились на Запад. Но в наши дни они уже не так широко распространены и не попали в TOP 10.

	Название*	Процент пользователей**
1	Trojan-Ransom.HTML.Agent	38,0
2	Trojan-Ransom.JS.Blocker	20,7
3	Trojan-Ransom.JS.InstallExtension	8,0
4	Trojan-Ransom.NSIS.Onion	5,8
5	Trojan-Ransom.Win32.Cryakl	4,3
6	Trojan-Ransom.Win32.Cryptodef	3,1
7	Trojan-Ransom.Win32.Snocry	3,0
8	Trojan-Ransom.BAT.Scatter	3,0
9	Trojan-Ransom.Win32.Crypmod	1,8
10	Trojan-Ransom.Win32.Shade	1,8

** Статистика основана на детектирующих вердиктах продуктов «Лаборатории Касперского». Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.*

*** Процент уникальных пользователей «Лаборатории Касперского», подвергшихся атакам конкретного семейства троянцев-вымогателей, от всех пользователей, подвергшихся атакам троянцев-вымогателей.*

На первом месте находится семейство Trojan-Ransom.HTML.Agent (38%), на втором – Trojan-Ransom.JS.Blocker (20,7%). Оба семейства блокируют браузер, демонстрируя веб-страницы с различным нежелательным контентом, который обычно включает сообщение с требованием выплаты денег (например, «предупреждение от правоохранительных органов») или содержит код JavaScript, блокирующий браузер вместе с сообщением.

На третьем месте находится Trojan-Ransom.JS.InstallExtension (8%) – это блокирующая браузер веб-страница, которая навязывает пользователю установку расширения Chrome. При попытке закрыть страницу часто проигрывается файл voice.mp3: *«Чтобы закрыть страницу, нажмите кнопку «Добавить»*. Предлагаемые расширения не являются вредоносными, но сама страница так назойлива, что пользователю сложно отказаться. Такой вид продвижения расширений используется партнерской программой.

Эти три вредоносных семейства особенно широко распространены в России и почти также широко представлены в некоторых странах постсоветского пространства.

Если посмотреть, где класс троянцев-вымогателей наиболее широко распространен (весь класс, не только три семейства, указанные выше), то окажется, что в тройке лидеров – Казахстан, Россия и Украина.

В третьем квартале 2015 года активизировался Cryakl – за день мы фиксировали до 2300 попыток заражения. Интересна схема шифрования Cryakl: вместо всего файла он шифрует первые 29 байт плюс три других блока, расположенных в файле случайным образом. Это делается, чтобы избежать распознавания поведенческими методами, тогда как шифрование первых 29 байт уничтожает заголовок.

Cryptodef – это пресловутый троянец-вымогатель Cryptowall. В отличие от других семейств вымогателей, о которых здесь идет речь, Cryptowall чаще всего обнаруживается в США – частота заражений в этой стране в три раза выше, чем в России. Cryptowall распространяется через спам-сообщения, содержащие заархивированный код JavaScript. При исполнении JavaScript загружает на компьютер Cryptowall, который начинает шифровать файлы. В сообщение с требованием выкупа злоумышленники внесли изменения: теперь жертв поздравляют с тем, что они «стали частью огромного сообщества Cryptowall».

Шифровальщики могут быть реализованы не только в виде исполняемых файлов, но и в виде скриптов, написанных с использованием простых скриптовых языков, как в случае семейства Trojan-Ransom.BAT.Scatter. Это семейство появилось в 2014 г. и стало быстро развиваться, совмещая функции почтового червя и троянца, крадущего учетные данные с пораженного компьютера. При шифровании используются две пары асимметричных ключей, что позволяет шифровать пользовательские файлы без раскрытия секретного ключа. Для шифрования файлов используются легитимные утилиты под другими именами.

Шифровальщик Trojan-Ransom.Win32.Shade, который тоже широко распространен в России, умеет запрашивать с командного сервера список, содержащий ссылки на дополнительные вредоносные программы. Далее он загружает эти зловреды и устанавливает их в систему. Все командные серверы шифровальщика расположены в сети Tor. Предположительно, данный троянец распространяется и через партнерскую программу.

TOP 10 стран, подвергшихся атакам троянцев-вымогателей

	Страна*	% пользователей, атакованных троянцем-вымогателем**
1	Казахстан	5,47
2	Украина	3,75
3	Российская Федерация	3,72
4	Нидерланды	1,26
5	Бельгия	1,08
6	Беларусь	0,94
7	Кыргызстан	0,76
8	Узбекистан	0,69
9	Таджикистан	0,69
10	Италия	0,57

** При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (менее 10 000).*

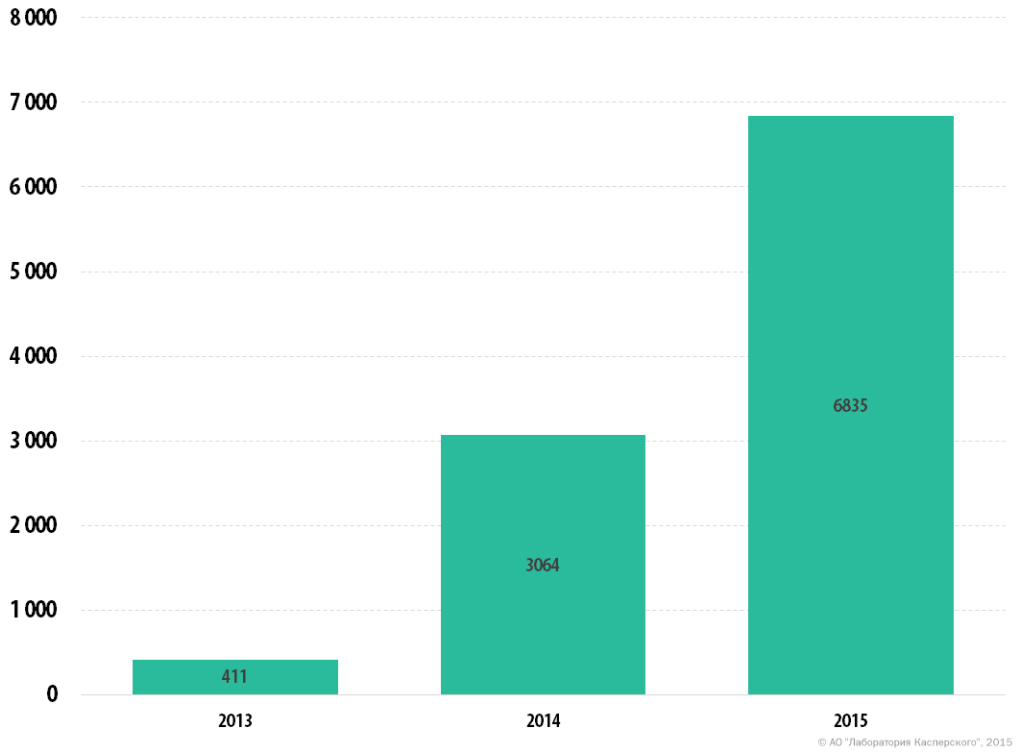
*** Процент уникальных пользователей, компьютеры которых были атакованы троянцами-вымогателями, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.*

Шифровальщики

Хотя сегодня шифровальщики не настолько популярны среди киберпреступников, насколько были популярны блокировщики, они причиняют пользователям больше вреда. И их стоит рассмотреть отдельно.

Число новых троянцев-шифровальщиков

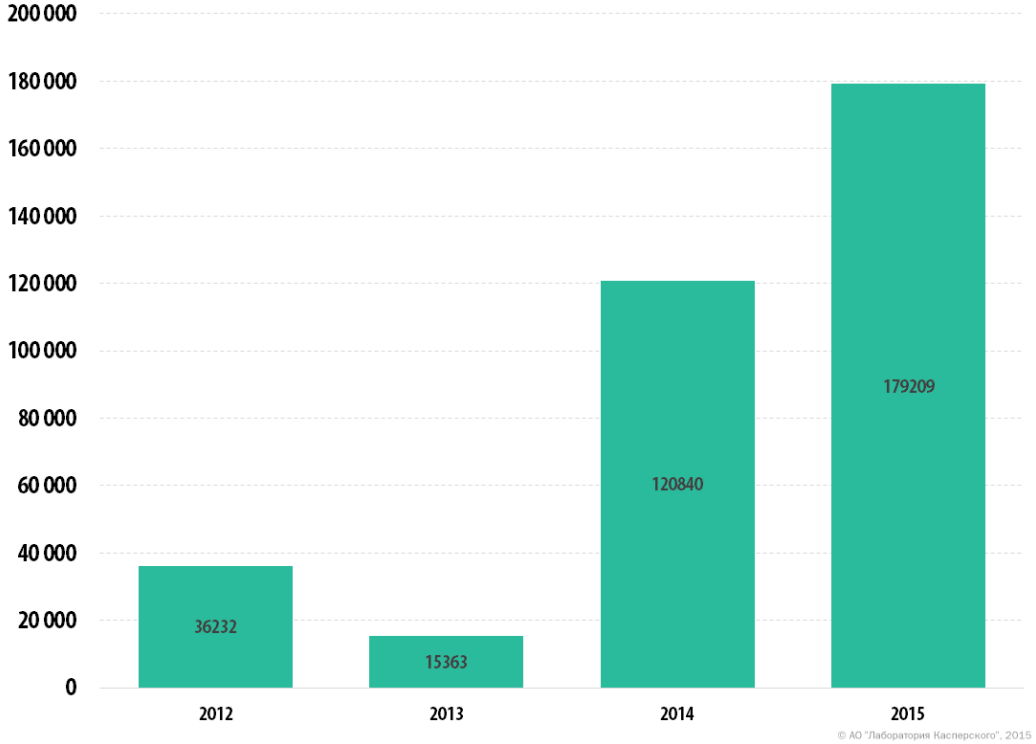
На следующей диаграмме представлен рост числа новых версий троянцев-шифровальщиков за последние несколько лет.



Число модификаций троянцев-шифровальщиков в коллекции «Лаборатории Касперского» (2013-2015 гг.)

На сегодняшний день в коллекции «Лаборатории Касперского» содержится около 11 тысяч модификаций троянцев-шифровальщиков. В 2015 году появилось десять новых семейств шифровальщиков.

Число пользователей, атакованных шифровальщиками



Число пользователей, атакованных троянцами-шифровальщиками (2012-2015 гг.)

В 2015 году шифровальщиками было атаковано **179 209** уникальных пользователей. Около 20% атак пришлось на корпоративный сектор.

Важно помнить, что реальное число инцидентов в несколько раз выше: статистика отражает только результаты сигнатурного и эвристического обнаружения, тогда как большая часть троянцев-шифровальщиков детектируется продуктами «Лаборатории Касперского» поведенческими методами.

TOP 10 стран, подвергшихся атакам троянцев-шифровальщиков

	Страна*	% пользователей, атакованных шифровальщиками**
1	Нидерланды	1,06
2	Бельгия	1,00
3	Российская Федерация	0,65
4	Бразилия	0,44
5	Казахстан	0,42
6	Италия	0,36
7	Латвия	0,34
8	Турция	0,31
9	Украина	0,31
10	Австрия	0,30

** При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (менее 10 000).*

*** Процент уникальных пользователей, компьютеры которых были атакованы троянцами-шифровальщиками, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.*

Первое место занимают Нидерланды. В этой стране наиболее распространено семейство шифровальщиков CTB-Locker (Trojan-Ransom.Win32/NSIS.Onion). В 2015 году злоумышленниками была запущена партнерская программа, использующая CTB-Locker, были добавлены новые языки, в том числе голландский. Пользователи заражаются в основном через электронные сообщения с вредоносными вложениями. Вероятно, в кампании по заражению компьютеров участвует носитель голландского – сообщения написаны на довольно неплохом голландском.

Похожая ситуация в Бельгии: здесь CTB-Locker тоже является самым распространенным троянцем-шифровальщиком.

В России список шифровальщиков, заражающих компьютеры пользователей, возглавляет Trojan-Ransom.Win32.Cryakl.

ВРЕДОНОСНЫЕ ПРОГРАММЫ В ИНТЕРНЕТЕ (АТАКИ ЧЕРЕЗ ВЕБ-РЕСУРСЫ)

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.

Угрозы в интернете: TOP 20

Всего в течение года нашим веб-антивирусом было задетектировано **121 262 075** уникальных вредоносных объектов (скрипты, эксплойты, исполняемые файлы и т.д.).

Мы выделили двадцать угроз, которые в 2015 году чаще всего встречались в интернете. Как и в прошлом году, рекламные программы и их компоненты заняли 12 позиций в этом TOP 20. В течение года рекламные программы и их компоненты были зафиксированы на 26,1% всех компьютеров пользователей, на которых сработал наш веб-антивирус. Увеличение количества рекламных программ, агрессивные способы их распространения и их противодействие детектированию со стороны антивирусов продолжают тренд 2014 года.

Хотя агрессивная реклама и доставляет неудобство пользователям, рекламные программы не наносят вреда компьютерам. Поэтому мы составили другой рейтинг, в который вошли только *вредоносные* объекты *(в нем не учитываются программы классов Adware и Riskware)*. На эти вредоносные объекты пришлось 96,6% атак *вредоносных* программ.

TOP 20 вредоносных объектов в интернете

	Название*	% от всех атак**
1	Malicious URL	75,76
2	Trojan.Script.Generic	8,19
3	Trojan.Script.Iframer	8,08
4	Trojan.Win32.Generic	1,01
5	Expoit.Script.Blocker	0,79
6	Trojan-Downloader.Win32.Generic	0,69
7	Trojan-Downloader.Script.Generic	0,36

	Название*	% от всех атак**
8	Trojan.JS.Redirector.ads	0,31
9	Trojan-Ransom.JS.Blocker.a	0,19
10	Trojan-Clicker.JS.Agent.pq	0,14
11	Trojan-Downloader.JS.Iframe.diq	0,13
12	Trojan.JS.Iframe.ajh	0,12
13	Exploit.Script.Generic	0,10
14	Packed.Multi.MultiPacked.gen	0,09
15	Exploit.Script.Blocker.u	0,09
16	Trojan.Script.Iframer.a	0,09
17	Trojan-Clicker.HTML.Iframe.ev	0,09
18	Hoax.HTML.ExtInstall.a	0,06
19	Trojan-Downloader.JS.Agent.hbs	0,06
20	Trojan-Downloader.Win32.Genome.qhcr	0,05

** Детектирующие вердикты модуля веб-антивируса. Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.*

*** Процент от всех веб-атак вредоносных программ, которые были зафиксированы на компьютерах уникальных пользователей.*

В TOP 20 представлены по большей части вердикты, которые присваиваются объектам, использующимся, как правило, в drive-by атаках. Они детектируются эвристически как Trojan.Script.Generic, Expoit.Script.Blocker, Trojan-Downloader.Script.Generic и другие. Такие объекты занимают семь позиций в нашем рейтинге.

Malicious URL – вердикт для ссылок из нашего черного списка (ссылки на веб-страницы с редиректами на эксплойты, сайты с эксплойтами и другими вредоносными программами, центры управления ботнетами, сайты-вымогатели и т.д.).

Под вердиктом Trojan.JS.Redirector.ads (8-е место) детектируется скрипт, который злоумышленники размещают на зараженных веб-ресурсах. Он перенаправляет пользователей на другие веб-сайты, например, на сайты онлайн-казино. Попадание данного вердикта в рейтинг должно служить напоминанием администраторам веб-ресурсов о легкости автоматического заражения их сайтов даже не самыми сложными программами.

Вердикт Trojan-Ransom.JS.Blocker.a (9-е место) представляет собой скрипт, который с помощью циклического обновления страницы пытается блокировать браузер и выводит сообщение о необходимости оплаты «штрафа» за просмотр неподобающих материалов. Деньги пользователю надо перевести на указанный электронный кошелек. Встречается данный скрипт в основном на порносайтах, детектируется в России и странах СНГ.

Скрипт с вердиктом Trojan-Downloader.JS.Iframe.diq (11-е место) также встречается на зараженных сайтах под управлением WordPress, Joomla и Drupal. Кампания по массовому заражению сайтов данным скриптом началась в августе 2015 года. Сначала он передает на сервер злоумышленников информацию о заголовке зараженной страницы, текущем домене и адресе страницы, с которой пользователь перешел на страницу со скриптом. После этого с помощью iframe в браузер пользователя загружается другой скрипт, который собирает информацию о системе на компьютере пользователя, временной зоне и наличии Adobe Flash Player. После этого и серий перенаправлений пользователь попадает на сайты, предлагающие установить под видом обновления Adobe Flash Player рекламную программу, либо предлагающие установить плагины для браузера.

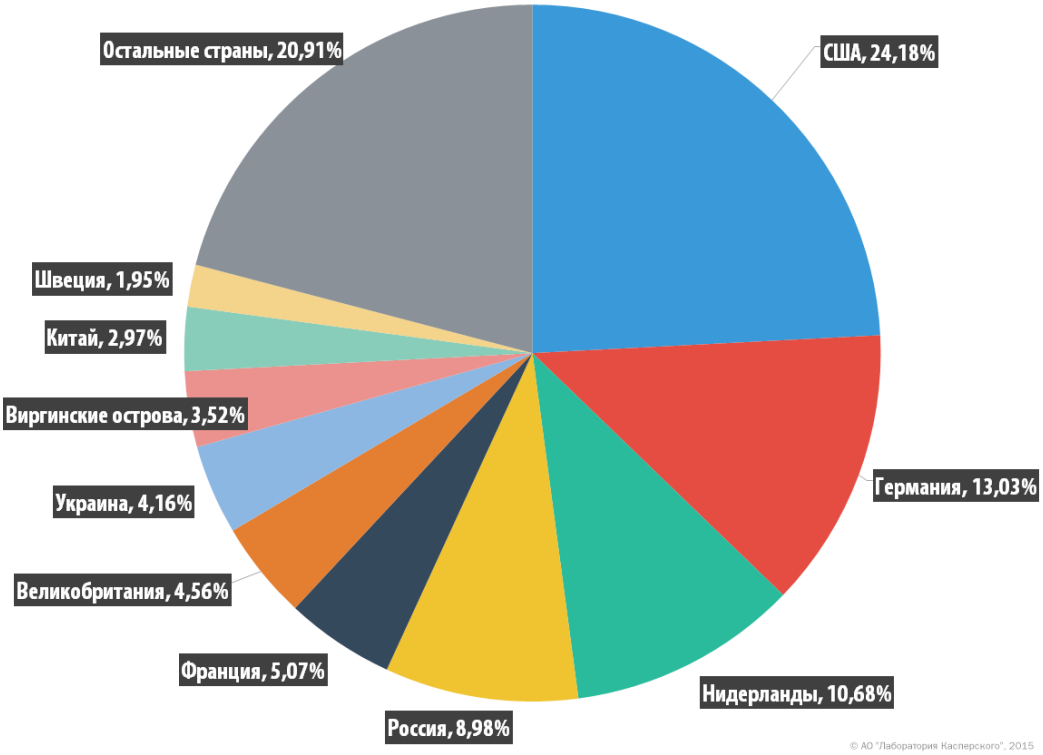
Страны - источники веб-атак: TOP 10

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. В данной статистике мы не учитывали источники распространения рекламных программ и хосты, связанные с деятельностью рекламных программ.

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 **798 113 087** атак через интернет, заблокированных в 2015 году, злоумышленники воспользовались **6 563 145** уникальными хостами.

80% нотификаций о заблокированных веб-атаках были получены при блокировании атак с веб-ресурсов, расположенных в десяти странах мира.



Распределение по странам источников веб-атак, 2015 год

Первые четыре места не изменились по сравнению с прошлым годом: США (24,15%), Германия (13,03%), Нидерланды (10,68%) и Россия (8,98%). Показатель каждой из этих стран уменьшился на несколько процентных пунктов. Франция (5,07%) набрала 2,08 п.п. и поднялась с седьмого места на пятое, Украина (4,16%) опустилась с пятого на седьмое место. Выбыли из топа Канада и Вьетнам, а новички – Китай (2,97%) и Швеция (1,95%) – разместились на девятом и десятом месте соответственно.

Данный топ демонстрирует, что киберпреступники предпочитают вести свою деятельность и использовать хостинги в развитых странах, рынок хостинг-услуг в которых очень развит.

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	Россия	48,90
2	Казахстан	46,27
3	Азербайджан	43,23
4	Украина	40,40
5	Вьетнам	39,55
6	Монголия	38,27
7	Белоруссия	37,91
8	Армения	36,63
9	Алжир	35,64
10	Катар	35,55
11	Латвия	34,20
12	Непал	33,94
13	Бразилия	33,66
14	Киргизия	33,37
15	Молдавия	33,28
16	Китай	33,12
17	Таиланд	32,92
18	Литва	32,80
19	ОАЭ	32,58
20	Португалия	32,31

Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.

** При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (меньше 10 тысяч).*

*** Процент уникальных пользователей, подвергшихся веб-атакам, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.*

Первые три страны в данном рейтинге не изменились по сравнению с 2014 годом. Россия по-прежнему сохраняет лидерство, однако процент уникальных пользователей там уменьшился на 4,9 п.п.

Покинули ТОР 20 Германия, Таджикистан, Грузия, Саудовская Аравия, Австрия, Шри-Ланка и Турция. Среди новичков – Латвия, Непал, Бразилия, Китай, Таиланд, ОАЭ и Португалия.

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

1. **Группа повышенного риска**

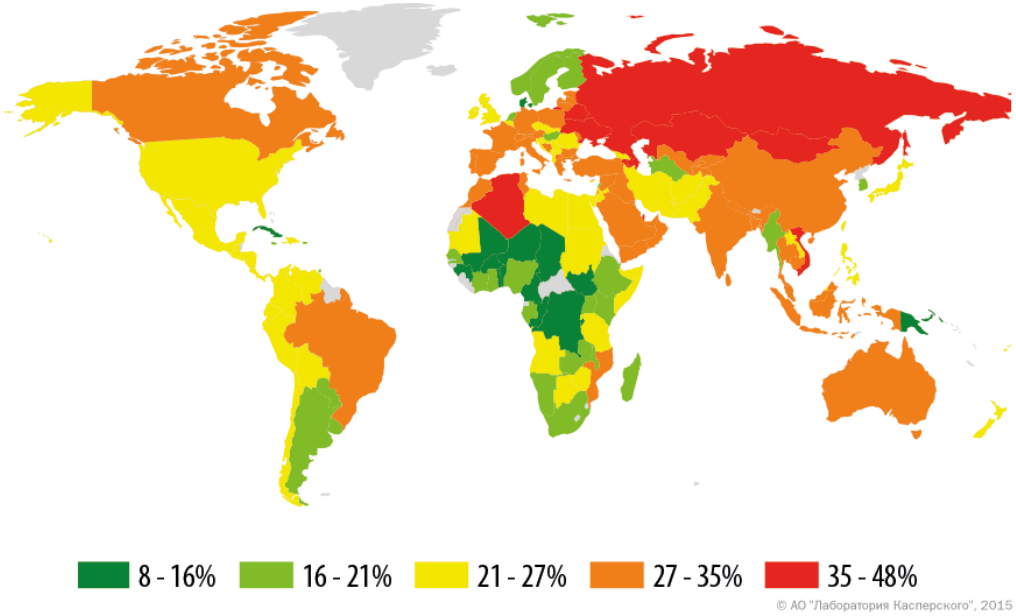
   В эту группу с результатом выше 41% вошли первые три страны из ТОР 20 – Россия, Казахстан и Азербайджан. Эта группа уменьшилась: по итогам 2014 года в нее входило 9 стран.

2. **Группа риска**

   В эту группу с показателями 21-40,9% попали 109 стран, в том числе: Франция (32,1%), Германия (32,0%), Индия (31,6%), Испания (31,4%), Турция (31,0%), Греция (30,3%), Канада (30,2%), Италия (29,4%), Швейцария (28,6%), Австралия (28,0%), Болгария (27,0%), США (26,4%), Грузия (26,2%), Израиль (25,8%), Мексика (24,3%), Египет (23,9%), Румыния (23,4%), Великобритания (22,4%), Чехия (22,0%), Ирландия (21,6%), Япония (21,1%).

3. **Группа наиболее безопасных стран (0-20,9%)**

   В эту группу попали 52 страны, в том числе: Кения (20,8%), Венгрия (20,7%), Мальта (19,4%), Нидерланды (18,7%), Норвегия (18,3%), Аргентина (18,3%), Сингапур (18,2%), Швеция (18%), Южная Корея (17,2%), Финляндия (16,5%), Дания (15, 2%).



В 2015 году при серфинге в интернете веб-атакам хотя бы раз подверглись 34,2% компьютеров пользователей интернета.

В среднем уровень опасности интернета за год снизился на 4,1 п.п. Данный тренд плавного снижения начался в 2014 году, и продолжается второй год подряд. Он может быть обусловлен несколькими факторами:

- Во-первых, свой вклад в борьбу с вредоносными сайтами стали вносить браузеры и поисковые системы, разработчики которых обеспокоились безопасностью пользователей.
- Во-вторых, все чаще пользователи отдают предпочтение для серфинга в интернете мобильным устройствам и планшетам.
- В-третьих, многие эксплойт-паки стали проверять, стоит ли у пользователя наш продукт. Если продукт стоит, то эксплойты не пытаются атаковать компьютер пользователя.

ЛОКАЛЬНЫЕ УГРОЗЫ

Важным показателем является статистика локальных заражений пользовательских компьютеров. Сюда попадают объекты, которые проникли на компьютер путем заражения файлов или съемных носителей либо изначально попали на компьютер не в открытом виде (например, программы в составе сложных инсталляторов, зашифрованные файлы и т.д.). Кроме того, в этой статистике учитываются объекты, которые были обнаружены на компьютерах пользователя после установки нашего продукта и первого сканирования системы файловым антивирусом.

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.

Всего в 2015 году было зафиксировано около **4 миллионов** вредоносных и потенциально нежелательных программ. Это в два раза больше, чем в прошлом году.

Вредоносные объекты, обнаруженные на компьютерах пользователей: TOP 20

Мы выделили двадцать угроз, которые в 2015 году чаще всего детектировались на компьютерах пользователей. В данный рейтинг также не входят программы классов Adware и Riskware.

	Название*	% уникальных атакованных пользователей**
1	DangerousObject.Multi.Generic	39,70
2	Trojan.Win32.Generic	27,30
3	Trojan.WinLNK.StartPage.gena	17,19
4	Trojan.Win32.AutoRun.gen	6,29
5	Virus.Win32.Sality.gen	5,53
6	Worm.VBS.Dinihou.r	5,40
7	Trojan.Script.Generic	5,01
8	DangerousPattern.Multi.Generic	4,93
9	Trojan-Downloader.Win32.Generic	4,36
10	Trojan.WinLNK.Agent.ew	3,42
11	Worm.Win32.Debris.a	3,24
12	Trojan.VBS.Agent.ue	2,79
13	Trojan.Win32.Autoit.cfo	2,61

	Название*	% уникальных атакованных пользователей**
14	Virus.Win32.Nimnul.a	2,37
15	Worm.Script.Generic	2,23
16	Trojan.Win32.Starter.lgb	2,04
17	Worm.Win32.Autoit.aiy	1,97
18	Worm.Win32.Generic	1,94
19	HiddenObject.Multi.Generic	1,66
20	Trojan-Dropper.VBS.Agent.bp	1,55

Данная статистика представляет собой детектирующие вердикты модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

** Детектирующие вердикты модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.*

*** Процент уникальных пользователей, на компьютерах которых файловый антивирус детектировал данный объект, от всех уникальных пользователей продуктов «Лаборатории Касперского», у которых происходило срабатывание антивируса на вредоносные программы.*

Первое место занимает вердикт DangerousObject.Multi.Generic (39,70%), используемый для вредоносных программ, обнаруженных с помощью облачных технологий. Эти технологии работают, когда в антивирусных базах еще нет ни сигнатуры, ни эвристики для детектирования вредоносной программы, но в облаке антивирусной компании уже есть информация об объекте. По сути, так детектируются самые новые вредоносные программы.

Продолжает падать доля вирусов: например, Virus.Win32.Sality.gen в прошлом году встречался у 6,69% пользователей, в 2015 – у 5,53%. Показатель Virus.Win32.Nimnul.a в 2014 году – 2,8%, в 2015 – 2,37%. Присутствующий в рейтинге на двадцатом месте вердикт Trojan-Dropper.VBS.Agent.bp представляет собой VBS-скрипт, который извлекает из себя и сохраняет на диск Virus.Win32.Nimnul.

Помимо эвристических вердиктов и вирусов в TOP 20 представлены вердикты для червей, распространяющихся на съемных носителях, и их компонентов. Их попадание в двадцатку обусловлено характером их распространения и созданием множества копий. Червь может продолжать свое распространение на протяжении длительного времени, даже если его серверы управления уже не действуют.

Страны, в которых компьютеры пользователей подвергались наибольшему риску локального заражения

Для каждой из стран мы подсчитали, насколько часто в течение года пользователи в ней сталкивались со срабатыванием файлового антивируса. Учитывались детектируемые объекты, 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.

ТОР 20 стран по уровню зараженности компьютеров

	Страна*	%**
1	Вьетнам	70,83
2	Бангладеш	69,55
3	Россия	68,81
4	Монголия	66,30
5	Армения	65,61
6	Сомали	65,22
7	Грузия	65,20
8	Непал	65,10
9	Йемен	64,65
10	Казахстан	63,71
11	Ирак	63,37
12	Иран	63,14
13	Лаос	62,75
14	Алжир	62,68
15	Камбоджа	61,66
16	Руанда	61,37
17	Пакистан	61,36
18	Сирия	61,00
19	Палестинская территория	60,95
20	Украина	60,78

Настоящая статистика основана на детектирующих вердиктах файлового антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

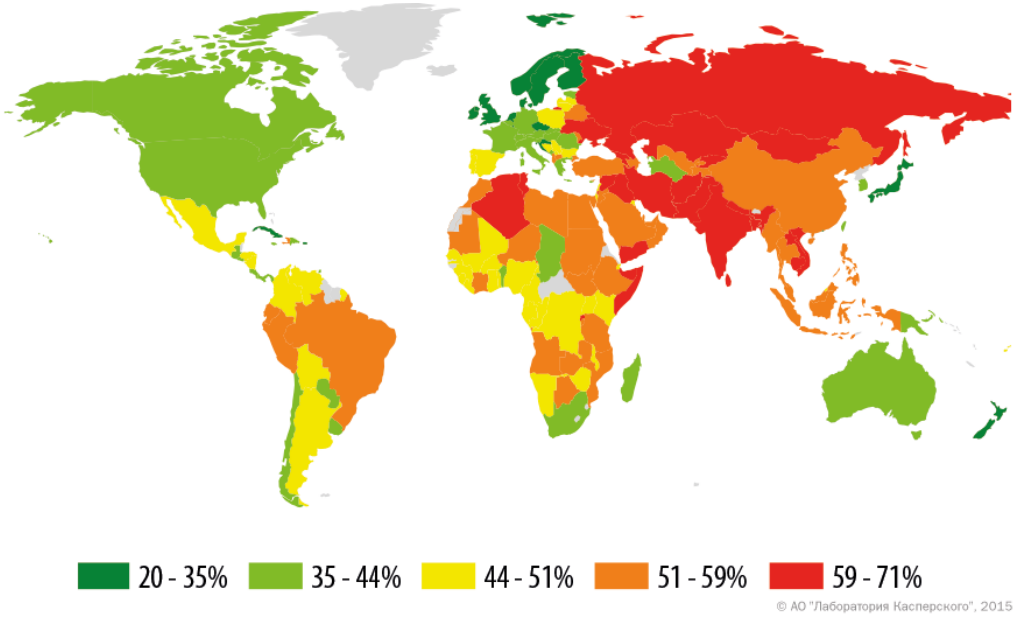
** При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (меньше 10 тысяч).*

*** Процент уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.*

Первое место в этом рейтинге третий год подряд занимает Вьетнам (70,83%). Монголия и Бангладеш в 2015 году поменялись местами: Монголия (66,30%) опустилась со второго на четвертое место, а Бангладеш (69,55%) поднялся с четвертого на второе. Россия (68,81%), не вошедшая в ТОР 20 в прошлом году, в 2015 году оказалась сразу на третьем месте.

Покинули ТОР 20 Индия, Афганистан, Египет, Саудовская Аравия, Судан, Шри-Ланка, Мьянма, Турция. Среди новичков – Россия, Армения, Сомали, Грузия, Иран, Руанда, Палестинская территория, Украина.

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 67,7% пользователей KSN, предоставляющих нам информацию, тогда как в 2014 году – у 58,7%.



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

1. **Максимальный уровень заражения** (более 60%)

   В эту группу вошли 22 страны, в том числе: Киргизия (60,77%), Афганистан (60, 54%).

2. **Высокий уровень заражения** (41-60%)

   В эту группу попали 98 страны мира, в том числе Индия (59,7%), Египет (57,3%), Белоруссия (56,7%), Турция (56,2%), Бразилия (53,9%), Китай (53,4%), ОАЭ (52,7%), Сербия (50,1%), Болгария (47,7%), Аргентина (47,4%), Израиль (47,3%), Латвия (45,9%), Испания (44,6%), Польша (44,3%), Германия (44,0%), Греция (42,8%), Франция (42,6%), Корея (41,7%), Австрия (41,7%).

3. **Средний уровень заражения** (21-40,9%)

   В группу вошли 45 стран, в том числе Румыния (40,0%), Италия (39,3%), Канада (39,2%), Австралия (38,5%), Венгрия (38,2%), Швейцария (37,2%), США (36,7%), Великобритания (34,7%), Ирландия (32,7%), Нидерланды (32,1%), Чехия (31,5%), Сингапур (31,4%), Норвегия (30,5%), Финляндия (27,4%), Швеция (27,4%), Дания (25,8%), Япония (25, 6%).

В десятку самых безопасных по уровню локального заражения стран попали:

	Страна	% пользователей*
1	Куба	20,8
2	Сейшельские острова	25,3
3	Япония	25,6
4	Дания	25,8
5	Швеция	27,4
6	Финляндия	27,4
7	Андорра	28,7
8	Норвегия	30,5
9	Сингапур	31,4
10	Чехия	31,5

** Процент уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.*

По сравнению с 2014 годом в этом списке произошли изменения – появились Андорра, покинула рейтинг Мартиника.

В среднем в десятке самых безопасных стран мира хотя бы раз в течение года было атаковано 26,9% компьютеров пользователей. По сравнению с прошлым годом этот показатель увеличился на 3,9 п.п.

ЗАКЛЮЧЕНИЕ

На основе анализа статистики мы можем выделить основные направления развития деятельности киберкриминала:

- Часть людей, занимавшихся киберкриминальной деятельностью, стремится минимизировать риски уголовного преследования и переключается с атак вредоносных программ на агрессивное распространение рекламного ПО.
- В используемом в массовых атаках ПО растет доля относительно несложных программ. Такой подход позволяет злоумышленникам быстро обновлять вредоносное ПО, чем и достигается эффективность атак.
- Злоумышленники освоили не-Windows платформы – Android и Linux: для этих платформ созданы и используются практически все виды вредоносных программ.
- В ходе своей деятельности киберкриминал активно использует современные технологии анонимизации – Tor для сокрытия командных серверов и Биткойны для проведения транзакций.

Все большая доля срабатывания антивируса приходится на «серую зону»: в первую очередь это различные рекламные программы и их модули. В нашем рейтинге веб-угроз 2015 года представители этого класса программ занимают двенадцать позиций в TOP 20. В течение года рекламные программы и их компоненты были зафиксированы на 26,1% всех компьютеров пользователей, на которых сработал наш веб-антивирус. Увеличение количества рекламных программ, агрессивные способы их распространения и их противодействие детектированию антивирусов продолжают тренд 2014 года. Распространение такого ПО приносит немалые деньги, и его создатели в погоне за наживой иногда используют приемы и технологии, характерные для вредоносных программ.

В 2015 году у вирусописателей выросла популярность эксплойтов для Adobe Flash Player. По нашим наблюдениям, лэндинг-страницы с эксплойтами чаще всего загружают именно эксплойты к Adobe Flash Player. Это можно объяснить двумя причинами: во-первых, в течение года было найдено большое количество уязвимостей в данном продукте. Во-вторых, в результате утечки данных от Hacking Team в публичном доступе оказалась информация о неизвестных ранее уязвимостях во Flash Player, чем и воспользовались злоумышленники.

В стане банковских троянцев произошло интересное изменение. Бесчисленные модификации троянца ZeuS, который долгие годы находился на первом месте, были вытеснены вредоносной программой Trojan-Banker.Win32.Dyreza. В течение 2015 года в рейтинге зловредов, нацеленных на кражу денег через системы интернет-банкинга, на первом месте был Upatre, закачивающий на компьютер жертвы троянцы-банкеры семейства, известного как Dyre/Dyzap/Dyreza. Среди всех банковских угроз доля атакованных Dyreza пользователей составила более 40%. Банкер использует эффективную схему веб-инъекций с целью воровства данных для доступа к системе онлайн-банкинга.

Также отметим, что целых два семейства мобильных банковских троянцев – Faketoken и Marcher – попали в TOP 10 банковских зловредов по итогам года. Исходя из трендов, можно предположить, что в следующем году мобильные банкеры будут занимать куда больший процент в нашем рейтинге.

В 2015 году произошел ряд изменений и в стане троянцев-вымогателей:

1. В то время как популярность программ-блокеров постепенно падает, количество пользователей, атакованных программами-шифровальщиками за год выросло на 48,3%. Шифрование файлов вместо простой блокировки компьютера – метод, который в большинстве случаев не дает жертве возможности простым способом восстановить доступ к информации. Особенно активно злоумышленники используют шифровальщики в атаках на бизнес-пользователей, которые идут на оплату выкупа куда охотнее, чем обычные домашние пользователи. Подтверждением этого является и появление в 2015 году первого троянца-шифровальщика под Linux, нацеленного на веб-серверы.
2. При этом крипторы становятся многомодульными и, помимо функционала собственно шифрования, обзаводятся функционалом кражи данных с компьютера.
3. Если на Linux злоумышленники только-только обратили свое внимание, то первый троянец-вымогатель для Android был обнаружен еще в 2014 году. В 2015 число атак, нацеленных на Android OS, стремительно росло, и по итогам года 17% атак программ-вымогателей были заблокированы именно на устройствах под управлением Android OS.
4. Угроза активно распространяется по всей планете: продукты «Лаборатории Касперского» обнаружили троянцев-вымогателей в 200 странах и территориях, то есть практически везде.

В 2016 году мы ожидаем продолжения развития шифровальщиков, нацеленных на не-Windows платформы: увеличение доли Android и появление шифровальщиков, нацеленных на Mac OS. Учитывая, что Android активно используется и в бытовой электронике, могут произойти и первые атаки крипторов на «умные» устройства.

ПРОГНОЗЫ НА 2016 ГОД: КОНЕЦ АРТ-УГРОЗ – КАКИМИ МЫ ИХ ЗНАЕМ...

ВВЕДЕНИЕ

Год подходит к концу, и для нас это повод, подводя его итоги, проанализировать, как развивалась индустрия и представить свой прогноз на предстоящие годы. Во время недавней общей встречи сотрудников Глобального центра исследований и анализа угроз (GReAT) и антивирусных исследователей-экспертов (такие встречи проводятся нечасто) мы воспользовались возможностью и набросали идей относительно вероятного развития событий. Мне выпала честь отобрать некоторые из наиболее интересных и вероятных прогнозов – как на ближайший год, так и на более отдаленное будущее. Перспективы нашей быстро развивающейся отрасли заставляют задуматься; ясно, что нам предстоит и впредь сталкиваться со множеством интересных вызовов. Возможно, ооперируя сухими цифрами и фактами, мы сумеем избежать нагнетания страха в духе научной фантастики и взамен предложить точные прогнозы и на короткий, и на долгий срок.

КОНЕЦ АРТ

Прежде, чем вы начнете праздновать, следует отметить, что мы имеем в виду только те аспекты АРТ-угроз, которые связаны с продолжительностью и сложностью атак (APT – Advanced Persistent Threats, целевые продолжительные атаки повышенной сложности). Киберпреступники готовы с радостью отказаться от обоих аспектов ради скрытости атак. Мы ожидаем, что злоумышленники будут уделять меньшее внимание продолжительности атак, отдавая большее предпочтение резидентным, или бесфайловым, вредоносным программам. Смысл в том, чтобы уменьшить количество следов, оставляемых в зараженной системе, и, благодаря этому, избежать обнаружения. Еще одно изменение в подходе будет связано с уменьшением акцента на сложность вредоносного ПО. По нашим прогнозам, злоумышленники будут чаще отдавать предпочтение переориентации готового вредоносного ПО на новые задачи вместо того, чтобы инвестировать в буткиты, руткиты и специализированный вредоносный код, становящийся бесполезным после его обнаружения экспертами по безопасности. Значение этого не только в том, что вредоносная платформа теперь не будет терять актуальность после своего обнаружения, но еще и в том, что АРТ-группировке будет легче спрятаться и скрыть свои намерения за широкими возможностями применения стандартного, легально продаваемого RAT (remote administration tool – инструмента удаленного администрирования). Когда эйфория от возможностей нестандартного вредоносного ПО сойдет на нет, окупаемость инвестиций будет играть не последнюю роль в принятии решений о финансировании злоумышленников, действующих при поддержке государственных структур. Как известно, низкие первоначальные вложения – залог отличной окупаемости.

ПРОДОЛЖЕНИЕ КОШМАРА С ТРОЯНЦАМИ-ВЫМОГАТЕЛЯМИ

По нашему мнению, в обозримом будущем программы-вымогатели ожидает неизменный успех и открытие новых горизонтов. У этого вида вредоносного ПО есть два преимущества для злоумышленников перед традиционными банковскими угрозами: прямая монетизация и относительно низкие затраты в расчете на жертву. Эта угроза мало беспокоит обладающие значительными ресурсами сторонние организации, такие как банки, и о ней редко поступают жалобы в правоохранительные органы. Мы ожидаем, что программы-вымогатели не только отвоюют часть рынка у банковских троянцев, но и будут осваивать новые для себя платформы. Слабые попытки реализовать программы-вымогатели на мобильных (Simplelocker) и Linux-устройствах (Ransom.Linux.Cryptor и Trojan-Ransom.FreeBSD.Cryptor) уже делались, однако, вероятно, OS X – более желанная платформа для киберпреступников. Мы ожидаем, что программы-вымогатели перейдут Рубикон и будут не только заражать компьютеры Mac, но и требовать у жертв выкуп «по ценам Mac». Затем, в более дальней перспективе, существует вероятность появления программ-вымогателей для «интернета вещей». И вот вопрос: сколько вы готовы заплатить за возвращение доступа к просмотру телепрограмм? К холодильнику? К автомобилю?

ФИНАНСОВЫЕ ПРЕСТУПЛЕНИЯ НА САМОМ ВЫСОКОМ УРОВНЕ: ИГРА ПРОТИВ ЗАВЕДЕНИЯ

Слияние киберпреступности и APT-угроз воодушевило финансово мотивированных преступников, позволив им элегантно перейти от атак на конечных пользователей к преследованию обслуживающих их финансовых организаций. В уходящем году мы видели множество примеров атак на кассовые терминалы и банкоматы, не говоря уже о дерзких ограблениях Carbanak, в ходе которых злоумышленникам удалось украсть сотни миллионов долларов. Мы ожидаем, что киберпреступники будут и дальше действовать в том же духе и возьмут в оборот новинки рынка – такие как альтернативные платежные системы (ApplePay и AndroidPay). При этом растущее число пользователей этих систем должно давать злоумышленникам новый способ прямой монетизации. Еще одна группа объектов, которые неизбежно вызовут интерес, – это фондовые биржи, настоящая золотая жила. В то время как лобовые атаки могут принести быстрый доход, нельзя сбрасывать со счетов возможности, связанные с более тонким вмешательством, таким как взлом используемых при высокочастотном трейдинге алгоритмов «черного ящика», чтобы обеспечить продолжительное получение выгоды при минимальном риске быть пойманными.

АТАКИ НА ПРОИЗВОДИТЕЛЕЙ ЗАЩИТНЫХ СИСТЕМ

Исходя из роста числа атак на производителей систем для обеспечения безопасности, мы прогнозируем появление интересного вектора атаки, который заключается во взломе применяемых игроками отрасли стандартных инструментов реверс-инжиниринга, таких как IDA и Hiew, средств отладки, таких как OllyDbg и WinDbg, или средств виртуализации – таких как комплекс VMware и продукт VirtualBox. Приведем в качестве примера уязвимость в реализации утилиты Strings в Linux – CVE-2014-8485. Это одна из уязвимостей, обнаруженных в сложном инструментарии, применяемом экспертами по безопасности при проведении исследований. Такие уязвимости могут пытаться эксплуатировать злоумышленники, всерьез намеревающиеся атаковать самих экспертов по IT-безопасности. Еще одно направление, открытое для злоупотреблений, – это обмен бесплатным исследовательским инструментарием через репозитории кода, такие как Github. Дело в том, что пользователи зачастую берут код из репозитория и запускают его на своих системах без элементарных мер предосторожности. Возможно, стоит также с подозрением взглянуть на популярные реализации PGP, которые охотно используют представители сообщества экспертов по информационной безопасности.

ВРЕДИТЕЛЬСТВО, ВЫМОГАТЕЛЬСТВО И ПРЕДАНИЕ ПОЗОРУ

От размещения в Сети обнаженных фото знаменитостей до взлома систем компаний Sony и Ashley Madison и публикации содержимого серверов HackingTeam – все говорит о том, что случаи доксинга (DOXing – это публикация личных данных в Сети без согласия владельца), публичного опозоривания и вымогательства становятся все более и более частыми. Хактивисты, преступники и злоумышленники, опирающиеся на государственную поддержку, – все они прибегают к хорошо продуманному размещению частных фото, данных, клиентских списков и кода с целью опозорить своих жертв. В то время как некоторые из подобных атак являются частью хорошо спланированных кампаний, другие – результат приспособленчества, использование низкого уровня кибербезопасности для демонстрации своей «хакерской силы». К сожалению, распространенность подобных явлений продолжит расти по экспоненте.

КОМУ ДОВЕРЯТЬ?

Возможно, самый серьезный дефицит в наш век интернета – это дефицит доверия. Злоупотребление доверенными ресурсами будет способствовать дальнейшему усилению этого дефицита. Злоумышленники снова и снова будут использовать для своих вредоносных целей библиотеки с открытым исходным кодом и ресурсы, внесенные в белые списки. По нашим прогнозам, злоупотребления затронут еще один вид доверенных объектов – внутренние ресурсы компаний. В поисках возможностей закрепиться в зараженной сети и продвинуться вглубь нее коварные киберпреступники могут обратить свой взор на ресурсы, доступные только через корпоративный интранет – например, организовывать атаки типа watering hole на корпоративный Sharepoint-портал, файловый сервер или портал ADP. Не исключено даже, что мы столкнемся с крайней формой и без того вопиющего злоупотребления доверенными сертификатами, если киберпреступники организуют от начала до конца сфабрикованный центр сертификации, который будет выписывать цифровые сертификаты на их вредоносные программы.

APT-ГРУППИРОВКИ: ЧТО НАС ЖДЕТ В БУДУЩЕМ

Наши враги не могли не обратить внимание на выгодность кибершпионажа. Как мы и ожидали, на сцену начали выходить наемники. Эта тенденция будет только усиливаться: спрос на возможности для проведения кибератак порождает предложение. И компании, и известные APT-группировки ищут способы переложить задачи, не имеющие критической важности, на сторонних исполнителей и не подвергать риску свой инструментарий и инфраструктуру. Здесь был бы уместен термин «APT как сервис» (APT-as-a-Service), но, вероятно, еще интереснее то, что развитие целевых атак, по нашим прогнозам, приведет их к уровню, который можно условно назвать «Доступ как сервис» (Access-as-a-Service). Речь идет о продаже доступа к системам жертв высокого уровня, на которых уже были успешно проведены атаки наемников.

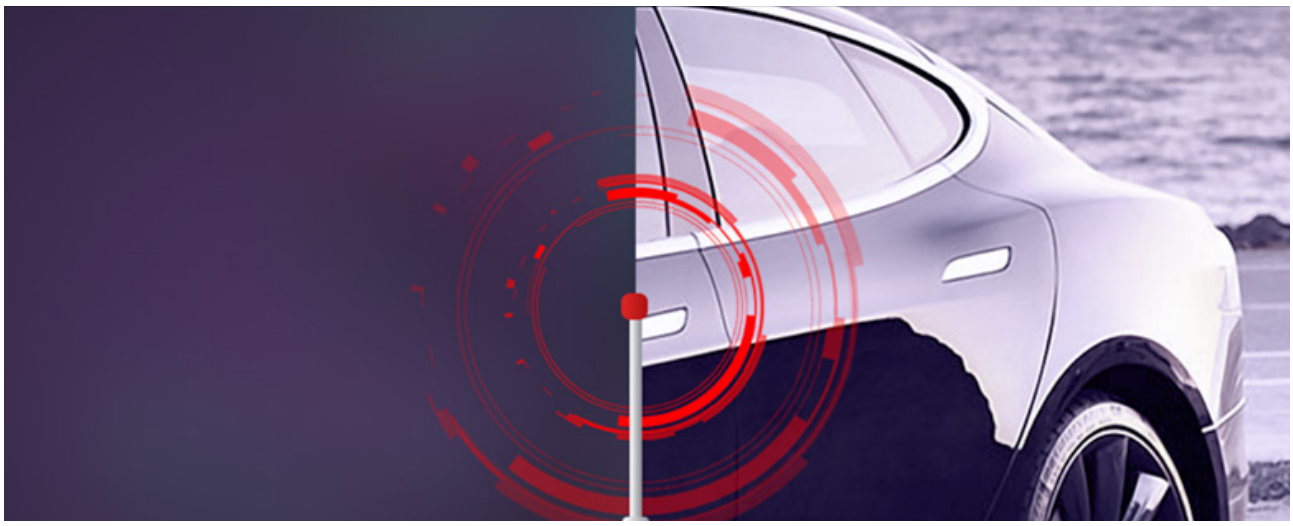
Заглядывая дальше в будущее кибершпионажа, мы видим возможный выход из тени членов наиболее серьезных APT-группировок (если угодно, «элиты APT-мира»). Возможны два разных сценария такого выхода из тени: переход представителей этих группировок в частный сектор экономики в связи с распространением практики «ответных ударов» (hacking back) со стороны жертв хакерских атак или передача ими информации сообществу экспертов по информационной безопасности – например путем участия в конференциях с целью представить собственную версию ситуации. Тем временем, можно ожидать появления еще нескольких новых языков в вавилонском столпотворении APT.

БУДУЩЕЕ ИНТЕРНЕТА

В последние годы появились признаки напряжения и разрывов в инфраструктуре самого интернета. Появление огромных ботнетов из маршрутизаторов, перехват BGP-сессий и BGP dampening, различные атаки на DNS-серверы и использование серверов для проведения DDoS-атак – все это говорит о безнаказанности и отсутствии в Сети регулирования и контроля в глобальном масштабе. Если говорить о долгосрочных прогнозах, можно представить себе, во что превратится интернет, если будет и дальше терять свою роль связующего звена, делающего мир единой глобальной «деревней». Мы можем прийти к раздробленному («балканизированному») интернету, разделенному государственными границами. В этом случае доступность ресурсов может быть ограничена атаками на связующие звенья, обеспечивающие соединения между различными сегментами интернета, или, возможно, геополитической напряженностью, препятствующей использованию физических каналов, соединяющих крупные группы интернет-ресурсов. Можно даже предположить, что мы столкнемся с появлением черного рынка соединений. Кроме того, можно ожидать, что по мере того как технологии, формирующие уязвимые точки интернета, будут становиться общедоступными и все более широко применяться, разработчики, связанные с теневыми рынками, биржами и форумами, будут создавать более современные технологии, которые позволят подпольным ресурсам оставаться в глубокой тени.

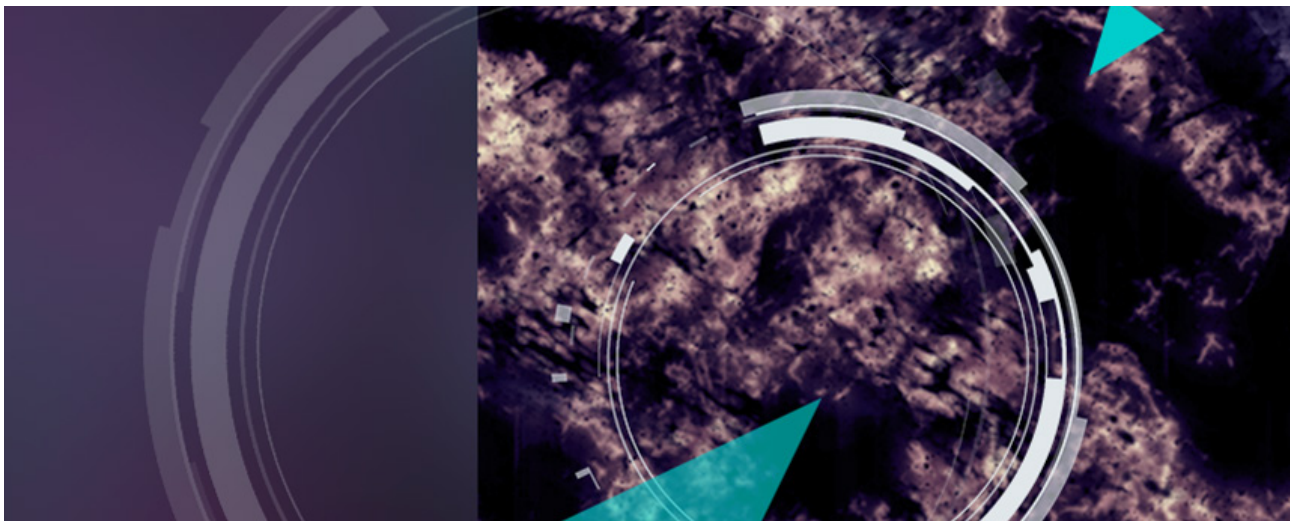
БУДУЩЕЕ ТРАНСПОРТА

В наши дни значительные инвестиции и наиболее передовые исследовательские ресурсы направляются на разработку автономных транспортных средств как для личного, так и для коммерческого применения. Такой транспорт потребует создания распределенных систем для управления маршрутами и крупными потоками подобных транспортных средств. Возможно, атаки будут направлены не на сами распределенные системы, а на перехват и подмену трафика, передаваемого по протоколам, лежащим в основе этих систем (концептуальную схему эксплуатации уязвимостей в широко используемой системе спутниковой связи Global Star в этом году на конференции BlackHat представил эксперт из компании Synack). Можно предположить, что целью подобных атак может стать кража ценного имущества или организация аварий движущихся транспортных средств с человеческими жертвами.



ПРИБЛИЖЕНИЕ КРИПТОАПОКАЛИПСИСА

И наконец, невозможно переоценить важность криптографических стандартов для поддержания функциональной роли интернета как непревзойденного средства взаимодействия и обмена информацией. В основе применяемых сегодня криптографических стандартов лежит представление о том, что вычислительные мощности, необходимые для взлома данных, зашифрованных на основе этих стандартов, превышают возможности всех людей вместе взятых. Но что произойдет, если наши вычислительные возможности перейдут на качественно новый уровень, как обещают предстоящие прорывы в области квантовых вычислений? Несмотря на то что поначалу квантовые вычисления не будут доступны обычным киберпреступникам, можно говорить об исчерпании ресурсов надежности текущими стандартами шифрования и необходимости создания новой, «постквантовой» криптографии. Учитывая, что даже современные высококачественные криптографические системы зачастую не применяются или реализуются некорректно, нельзя ожидать гладкого перехода к прогрессивным стандартам, который позволил бы избежать масштабных проблем, связанных с неадекватностью криптозащиты в новых условиях.



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

Следите за нами

Сайт «Лаборатории Касперского»

Блог Евгения Касперского

B2C блог «Лаборатории Касперского»

B2B блог «Лаборатории Касперского»

Новостная служба «Лаборатории Касперского»

Блог Kaspersky Academy