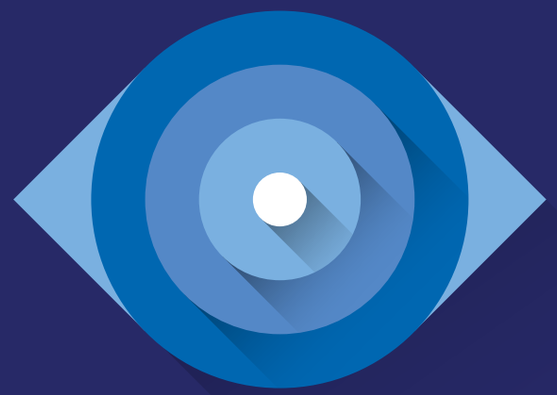
КИБЕР-БЕЗОПАСНОСТЬ ПРОГНОЗ НА 2017



panda

pandalabs

1. Анализ

2. Рейтинг атак 2016 года

- Шифровальщики
- Вредоносная почта
- Внутрикорпоративный фишинг
- Мобильные устройства
- Интернет вещей
- Кибер-войны
- Кибер-преступления
- DDoS-атаки
- POS-терминалы и банковские карты
- Финансовые учреждения
- Социальные сети

3. Какие кибер-кошмары готовит нам 2017 год?

- Компании
- Интернет вещей
- DDoS
- Мобильные телефоны
- Кибер-войны

4. О PandaLabs

1.АНАЛИЗ

1 Анализ

Технологическая революция. Сегодня - это бесспорный факт: цифровые технологии трансформируют мир бизнеса, работу и государственную службу. Важно, чтобы мы создавали климат цифрового доверия, способствующий защите пользователей. Поэтому кибер-безопасность стала важнейшим элементом.

Этот год начался с более чем 20 миллионов новых образцов вредоносных программ, обнаруженных и нейтрализованных в PandaLabs (в среднем - 227 000 в день). Это чуть больше, чем в первом квартале 2015 года (в среднем - 225 000 в день). В течение 2016 года мы видели, как **количество новых образцов стало чуть меньше, чем годом ранее: в среднем до 200 000 в день. Хотя атаки стали более эффективными.**

Кибер-преступники стали все более уверенными в своих силах, и даже несмотря на то, что мы заканчиваем год с более оптимистическими показателями, мы все равно не можем терять бдительность. Хакеры концентрируют свои усилия на более прибыльных атаках, совершенствуя свою тактику, что позволяет им получать быстрые и легкие деньги более эффективно.

Хакеры переключили свое внимание на организации, которые обрабатывают огромные объемы данных, особенно персональной информации (больницы, фармацевтика, отели и т.д.). Как только они получают доступ к таким организациям, они заражают максимально возможное число компьютеров с помощью шифровальщиков, в результате чего могут требовать от своих жертв любые деньги в виде выкупа или продавать эти данные на "черном рынке".

Если что и не изменилось в этом году, так это класс наиболее популярных вредоносных программ - речь идет про трояны, которые вкупе с шифровальщиками продолжают оставаться на вершине "рейтинга" уже многие годы.

2.РЕЙТИНГ АТАК 2016 ГОДА

2

Рейтинг атак 2016 года

Шифровальщики

Мы знаем, что шифровальщики - это серьезный бизнес у кибер-преступников, но его невероятно сложно измерить с высокой степенью достоверности. Мы видели эволюцию таких атак, наряду с такими усовершенствованиями, как прямой чат жертвы с хакерами для "обсуждения" платежей. Техники также стали более совершенными, а иногда они особенно агрессивны, как в случае с **Petya**, который вместо шифрования документов поражает сразу главную загрузочную запись (MBR) компьютера и делает его непригодным до уплаты выкупа.

Также все чаще мы видим злоупотребления системной утилитой **PowerShell** (что мы прогнозировали в ежегодном отчете PandaLabs за 2015 год), установленной по умолчанию в Windows 10 и часто используемой при атаках во избежание обнаружения со стороны решений безопасности, установленных на компьютерах жертв.

Во втором квартале мы видели одну из самых странных атак шифровальщика на компанию из Словении. Ее руководитель службы безопасности получил письмо из России, сообщающее о том, что их сеть взломана, и вскоре на всех их компьютерах будет запущен шифровальщик, если они не заплатят примерно 9000 евро (в биткоинах) в течение 3 дней. Чтобы доказать наличие доступа к сети, хакеры прислали им список всех устройств, подключенных к внутренней сети компании.

Конечно, многие жертвы предпочли заплатить выкуп, хотя восстановление данных при этом не гарантируется.

В третьем квартале мы наблюдали более высокие уровни специализации на атаках шифровальщиками.

Лучший пример этого показали создатели шифровальщиков Petya и Mischa, которые специализировались на разработке вредоносного ПО и соответствующих платежных платформ, передав вопросы распространения третьим лицам - такая практика была названа **Ransom as a Service** (RaaS). По сути, после того как они сделали свою часть работы, они привлекли дистрибьюторов для заражения жертв. Все как в легальном бизнесе: прибыль дистрибьюторов зависит от объема "заработанных" денег. Чем выше продажи, тем выше процент, который они получают.

Вредоносная почта

Атаки приходят не только со стороны вредоносной рекламы или взломанных сайтов. Огромное количество атак все еще осуществляется через электронную почту в виде ложных счетов или различных уведомлений.

Подобная атака была проведена как минимум в двух странах Европы - в Польше и Испании, где хакеры выдавали себя за местные электрокомпании.

В их сообщении не было вложений, а была только платежная информация в виде текста и ссылка для просмотра более детальной информации.

Подвох заключался в непомерно высоких суммах в счете, которые заставляли получателя возмущаться и, не думая, нажимать на ссылку для просмотра детализации. При нажатии на ссылку пользователь направлялся на ложный сайт, сильно похожий на реальный сайт обслуживающей его энергокомпании, где он мог скачать счет. Если клиент скачивал и открывал файл, то он заражался шифровальщиком.

Внутрикорпоративный фишинг

Этот вид атак стремительно набирает популярность.

Хакеры якобы от лица президента или финансового директора компании запрашивают трансфер у сотрудника.

Прежде, чем сделать это, они изучают работу компании изнутри, получая информацию о своих жертвах через соцсети, что делает их аферу более правдоподобной.

Яркий пример этого года - инцидент в компании **Mattel**, известном производителе Barbies и Hot Wheels.

Высокопоставленный руководитель получил сообщение от недавно назначенного руководителя компании с заданием на перевод 3 млн. долларов США на банковский счет в Китае. После того как трансфер был осуществлен, он сообщил руководителю, что все сделано. Тот был ошарашен этим, потому что никакого задания на трансфер он ему не давал. Они срочно обратились в госорганы США

и банк, но было слишком поздно, т.к. деньги уже были переведены.

Однако им повезло: у банка в Китае был выходной день, а потому у них было достаточно времени, чтобы предупредить китайские власти. Счет был заморожен, и Mattel сумел вернуть свои деньги.

Мобильные устройства

SNAP - одна из самых популярных уязвимостей этого года.

От нее пострадали мобильные телефоны LG G3. Проблема происходила из ошибки в приложении Smart Notice, предоставляющей права на запуск любого JavaScript. В BugSec обнаружили эту уязвимость и сообщили в LG, которая оперативно опубликовала патч для устранения проблемы.

Gugi, троян под Android, сумел преодолеть барьеры безопасности в Android 6 для кражи банковских регистрационных данных из приложений, установленных на телефоне. Для этого поверх окна легитимного приложения Gugi накладывал свое окно, запрашивая банковские данные пользователя, которые без его ведома отправлялись непосредственно кибер-преступникам.

В августе компания Apple опубликовала срочное обновление своей операционной системы для мобильных устройств iOS 9.3.5. В нем устранялись три уязвимости "нулевого дня", использующиеся **шпионским ПО, известным как Pegasus**, разработанным израильской компанией NGO Group, которая выпускает продукты, аналогичные решениям компании Hacking Team.

Интернет вещей

Автомобильный сектор очень подвержен риску. Сотрудники Университета из Бирмингема показали, как они могут взламывать систему блокировки дверей любой машины, проданной Volkswagen Group за последние 20 лет. Чарли Миллер и Крис Валашек, которые ранее взламывали Jeep Cherokee, пошли еще дальше и показали, как они могут манипулировать дроссельной заслонкой, тормозами и даже рулем движущегося автомобиля.

"Умные дома" также уязвимы перед кибер-атаками. Исследователь Эндрю Тирни показал разработанный им способ взлома термостата. После того как он смог получить контроль над ним (вставив в него SD-карту), он поднял температуру до 99 градусов по Фаренгейту и запросил PIN-код для деактивации. Термостат подключался к IRC-каналу, предоставляя MAC-адрес в виде идентификатора каждого скомпрометированного устройства. У пользователя запрашивался биткоин в обмен на PIN-код, который менялся каждые 30 секунд.

Кибер-войны

В сфере кибер-войн, 2016 показал, что США решили пойти в атаку, признавшись в запуске кибер-атак на ИГИЛ.

Роберт Уорк, заместитель министра обороны США, предельно ясно об этом сказал в интервью CNN.

В июне **власти Южной Кореи раскрыли атаку со стороны КНДР.** Предположительно, атака началась примерно год назад, и ее основной целью стали 140 000 компьютеров, принадлежащих организациям и государственным органам, а также оборонным предприятиям. Но данная атака была обнаружена только в феврале этого года. По заявлению полиции, было украдено свыше 42000 документов, из которых 95% были связаны с вопросами обороны, такими как, например, документы по планам и спецификациям на истребитель F35.

В разгар президентских выборов в США одним из наиболее актуальных обнаруженных инцидентов стало раскрытие **атаки на Национальный комитет Демократической партии США (Democratic National Commettee), в результате чего были украдены огромные объемы данных**, ставших впоследствии достоянием общественности.

Продолжая тему выборов, ФБР предупредило об обнаружении двух атак на сайты, связанные с выборами. При этом как минимум один из хакеров (иностранец) сумел снять с регистрации некоторых избирателей.

В августе группа, именующая себя как **"The Shadow Brokers", объявила, что она взломала АНБ**, и опубликовала некоторые виды украденного "кибер-оружия", обещая продать остальные образцы.

Кибер-преступления

В июне преступник, которого окрестили "Властелин тьмы", выставил на продажу на черном рынке информацию о пациентах трех институтов из США.

Он украл информацию о более чем 650 000 пациентов и запросил за них порядка 700 000 долларов США. Вскоре после этого он выставил на продажу персональные данные 9,3 миллионов клиентов агентства медицинского страхования за 750 биткоинов (примерно 0,5 млн. долларов).

В последние месяцы Dropbox также стал жертвой кибер-преступников. Недавно стало известно, что популярный файлообменный сервис подвергся атаке в 2012 году.

Итог: кража данных 68 миллионов пользователей.

Но если о каком грабеже и говорить, то это об инциденте с **Yahoo**. Хотя он произошел еще в 2014 году, но об этом стало

известно совсем недавно. Всего было скомпрометировано **500 млн. аккаунтов**, что стало крупнейшей кражей в истории.

2 августа произошла одна из крупнейших биткоин-краж в истории. Компания **Bitfinex**, которая занимается торговлей и обменом криптовалюты, стала жертвой атаки, в результате которой была украдена сумма, равная **60 млн. долларам**. Эти деньги принадлежали клиентам, которые хранили свои биткоины в этом "банке".

До сих пор нет улик, указывающих на преступников, и компания пока не предоставляет какой-либо информации о произошедшем, т.к. правоохранительные органы до сих пор проводят расследование.

DDoS-атаки

В сентябре известный журналист в сфере безопасности Брайан Кребс раскрыл vDOS - "компанию", которая предлагала услуги DDoS-атак.

Вскоре после этого были арестованы организаторы, которые за 2 года провели 150 000 атак и заработали 618 тысяч долларов.

Затем веб-сайт Кребса подвергся сокрушительной DDoS-атаке, которая отключила его на неделю. В конце концов, Google, в рамках своего Project Shield, сумел защитить его сайт, после чего он снова стал доступен в онлайне.

В последнем квартале года прокатилась волна масштабных кибер-атак против американского интернет-провайдера DynDNS, от которых пострадали веб-сайты многих крупных глобальных корпораций и международных коммуникационных средств, таких как Netflix, Twitter, Amazon и The New York Times. Обслуживание было прервано почти на 11 часов, от чего пострадало свыше миллиарда пользователей.

POS-терминалы и банковские карты

Популярная сеть быстрого питания Wendy's столкнулась с заражением вредоносными программами свыше 1000 своих PoS-терминалов, из-за чего была украдена информация о банковских картах ее клиентов.

Мы в PandaLabs обнаружили эту атаку, выполненную с помощью известной угрозы PunkeyPOS, которая использовалась для заражения свыше 200 ресторанов в США.

Еще одна подобная атака была обнаружена нашей лабораторией в этом году. И снова пострадали рестораны в США: примерно **300** учреждений, чьи POS-терминалы были заражены с помощью вредоносной программы **PosCardStealer**.

Финансовые учреждения

В этом году Центральный банк Бангладеша стал жертвой атаки, в ходе которой были сделаны трансферы на 1 млрд. долларов.

К счастью, удалось большую часть этих переводов заблокировать, хотя преступники все же смогли украсть около 81 миллиона долларов США.

Вскоре после этого мы наблюдали еще два аналогичных случая: один был против банка во Вьетнаме, а второй - против банка в Эквадоре.

Социальные сети

Безопасность **117 миллионов пользователей LinkedIn** была подвержена риску после того, как был опубликован список адресов электронной почты и их соответствующие хэши паролей.

32 миллиона логинов и паролей пользователей Twitter были выставлены на продажу примерно за 6000 долларов.

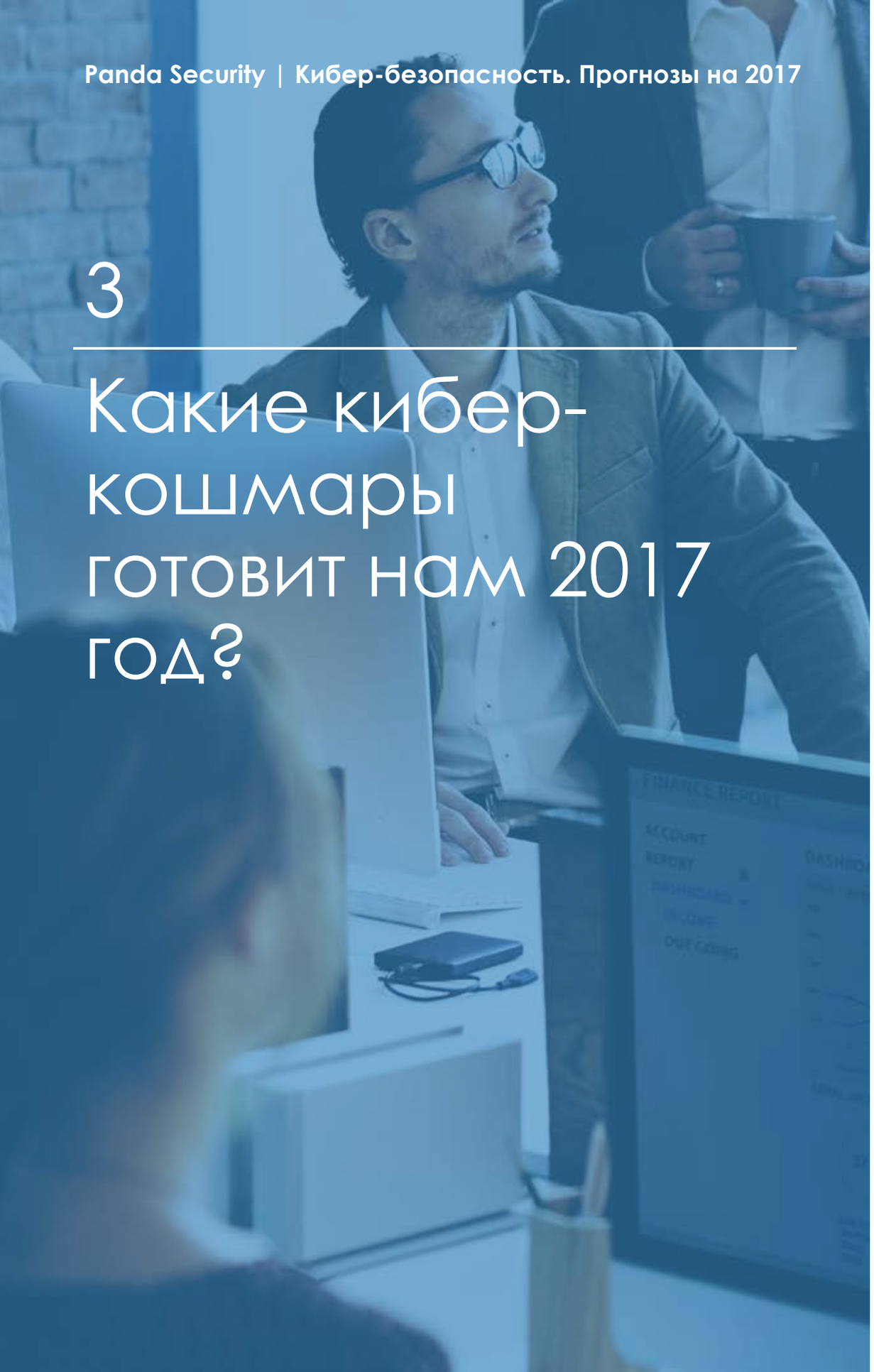
Эта социальная сеть отрицает, что информация по аккаунтам была получена с их серверов. На самом деле, пароли были представлены в виде текста и большинство из них принадлежали пользователям из России, и есть подозрение, что они были получены в результате фишинга или с помощью троянов.

Кстати, был атакован **MySpace**, хотя он практически уже не используется. Атака произошла в 2013 году, хотя до мая этого года о ней ничего не было известно. Были украдены имена пользователей, пароли и адреса электронной почты у примерно **360 миллионов пользователей**.

Пострадавший пользователь может уже годами не пользоваться MySpace, но если у него есть привычка использовать одинаковый пароль, то сейчас самое время отказаться от нее и включить двухступенчатую авторизацию.

Использование двухступенчатой авторизации, создание сложных паролей и запрет на использование одинаковых паролей на разных веб-сайтах - вот основные советы по информационной безопасности, которые должны быть приняты во внимание.

3. КАКИЕ КИБЕР-КОШМАРЫ ГОТОВИТ НАМ 2017 ГОД?



3

Какие кибер-кошмары готовит нам 2017 год?

Шифровальщики

В течение 2016 года они были в центре внимания, и скорее всего так будет и в 2017 году. В некотором роде, **этот вид атаки заменил собой другие, более традиционные способы** кражи информации. Шифровальщики позволяют намного проще "зарабатывать" деньги, исключая посредников и нежелательные риски.

Атаки на компании

Атаки на компании будут более многочисленными и сложными.

Компании уже стали первоочередной целью для кибер-преступников. Их информация более ценна по сравнению с данными частных пользователей.

Кибер-преступники всегда ищут слабые места в корпоративных сетях, чтобы проникнуть в них. После этого они получают доступ к ресурсам, которые содержат искомую информацию. Они могут также запустить масштабные атаки с помощью шифровальщиков, заражающих все доступные устройства, чтобы потом запросить астрономические суммы денег за восстановление данных.

Интернет вещей

Интернет вещей (IoT) - это следующий кошмар информационной безопасности. Любой вид устройств, подключенных к сети, может быть использован для того, чтобы

проникнуть в корпоративные сети. Большинство таких устройств не имеют должного уровня безопасности.

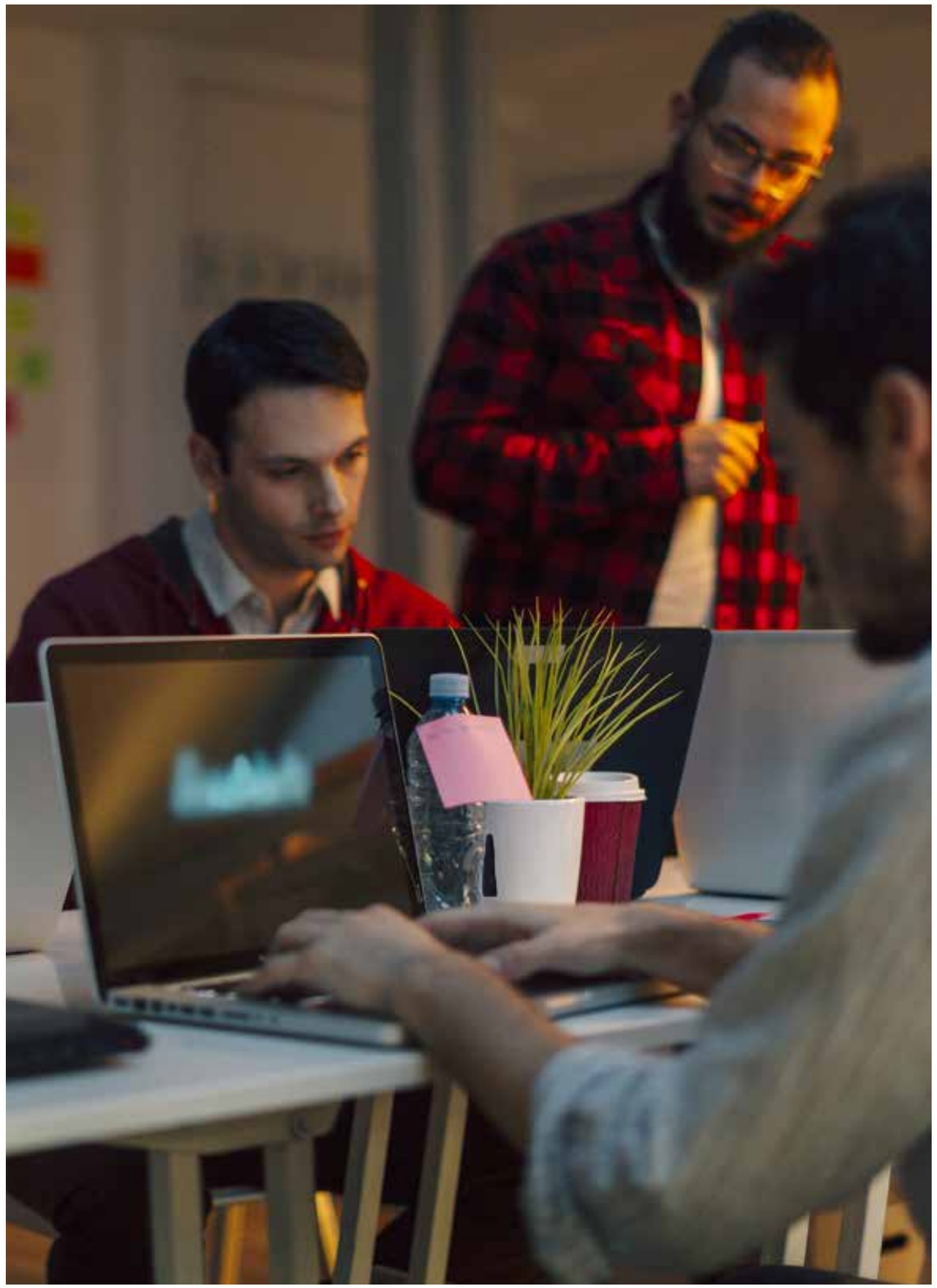
Как правило, они не получают автоматические обновления безопасности, используют слабые пароли, причем часто на тысячах устройств используются одинаковые пароли по умолчанию и т.д. Все это вместе делает их очень уязвимыми для внешних атак.

DDoS

В последние месяцы 2016 года мы стали свидетелями наиболее мощных в истории DDoS-атак. Они начались в сентябре с атаки на **Брайана Кребса** после того, как он сообщил о деятельности израильской компании, которая предлагает услуги по запуску таких атак.

Другая крупная атака была проведена против французской компании OVH (трафик - до 1 ТБ/сек), а еще одна - против американской компании Dyn, которая оставила несколько крупных интернет-гигантов без интернет-сервисов.

Эти атаки были совершены бот-сетями, в основе которых лежали тысячи зараженных IoT-устройств (IP-камеры, роутеры и пр.). Мы можем быть уверены в том, что в 2017 году мы увидим рост числа подобных атак, которые **обычно используются для нанесения ущерба деловой репутации компаний или для блокировки ее деятельности** (блокируя доступ к Интернету, затрудняя онлайн-продажи и пр.).



Мобильные телефоны

Здесь цель вполне понятна: **больше всего достанется устройствам Android.** Не секрет, что Android имеет самую большую долю рынка, а эта операционная система установлена на большинстве устройств. Apple сохраняет скромную долю с iOS, а остальные системы имеют незначительную долю рынка. Кибер-преступникам будет проще сфокусироваться на одной операционной системе, чтобы достичь максимальных прибылей.

Решение проблемы зависит не только от того, что может сделать Android с помощью своевременных обновлений, но еще и от того, как каждый из производителей мобильных устройств решит, когда и как их включить в свой пакет (если вообще делать это). Учитывая количество инцидентов, возникающих ежемесячно, такая ситуация только повышает риски у пользователей.

Кибер-войны

Мы переживаем один из наиболее сложных этапов развития международных отношений за последние годы: угрозы торговых войн, шпионаж, конфронтация между ведущими державами. Все это, несомненно, может иметь тяжелые и серьезные последствия в сфере кибер-безопасности.

Правительства разных стран стремятся получить доступ к еще большим объемам информации (в то время, когда шифрование становится все более популярным), а потому спецслужбы будут еще более заинтересованы в том, чтобы получать информацию, которая может принести пользу промышленности своих стран.

Такая глобальная тенденция может препятствовать инициативам по обмену данными, которыми уже обмениваются крупные компании, чтобы лучше защитить себя от кибер-преступников, внедряя стандарты и международные правила взаимодействия.

4. О PANDALABS

4 О PandaLabs

PandaLabs - это антивирусная лаборатория и центр исследований и разработки компании Panda Security, где:

- PandaLabs создает автоматизированные системы, работающие в режиме реального времени, необходимые для защиты клиентов Panda Security во всем мире от всех типов вредоносного кода.
- PandaLabs отвечает за выполнение тщательного анализа всех типов вредоносных программ с целью повышения уровня защиты, предлагаемой клиентам Panda Security, а также информирования общественности о данных угрозах.

Кроме того, PandaLabs постоянно находится в состоянии повышенной бдительности, внимательно отслеживая различные тенденции и события, происходящие в области вредоносных программ и безопасности.

Это необходимо для предупреждения и оповещения общественности о неизбежных опасностях и угрозах, а также для прогнозирования будущих событий.

pandalabs

Не допускается копирование, воспроизведение, хранение в поисково-информационных системах или передача данного отчета целиком или частично без предварительного письменного разрешения со стороны Panda Security.

© Panda Security 2016. Все права защищены.

panda

pandalabs