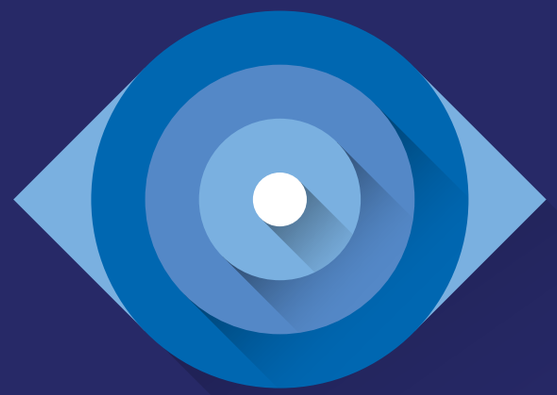
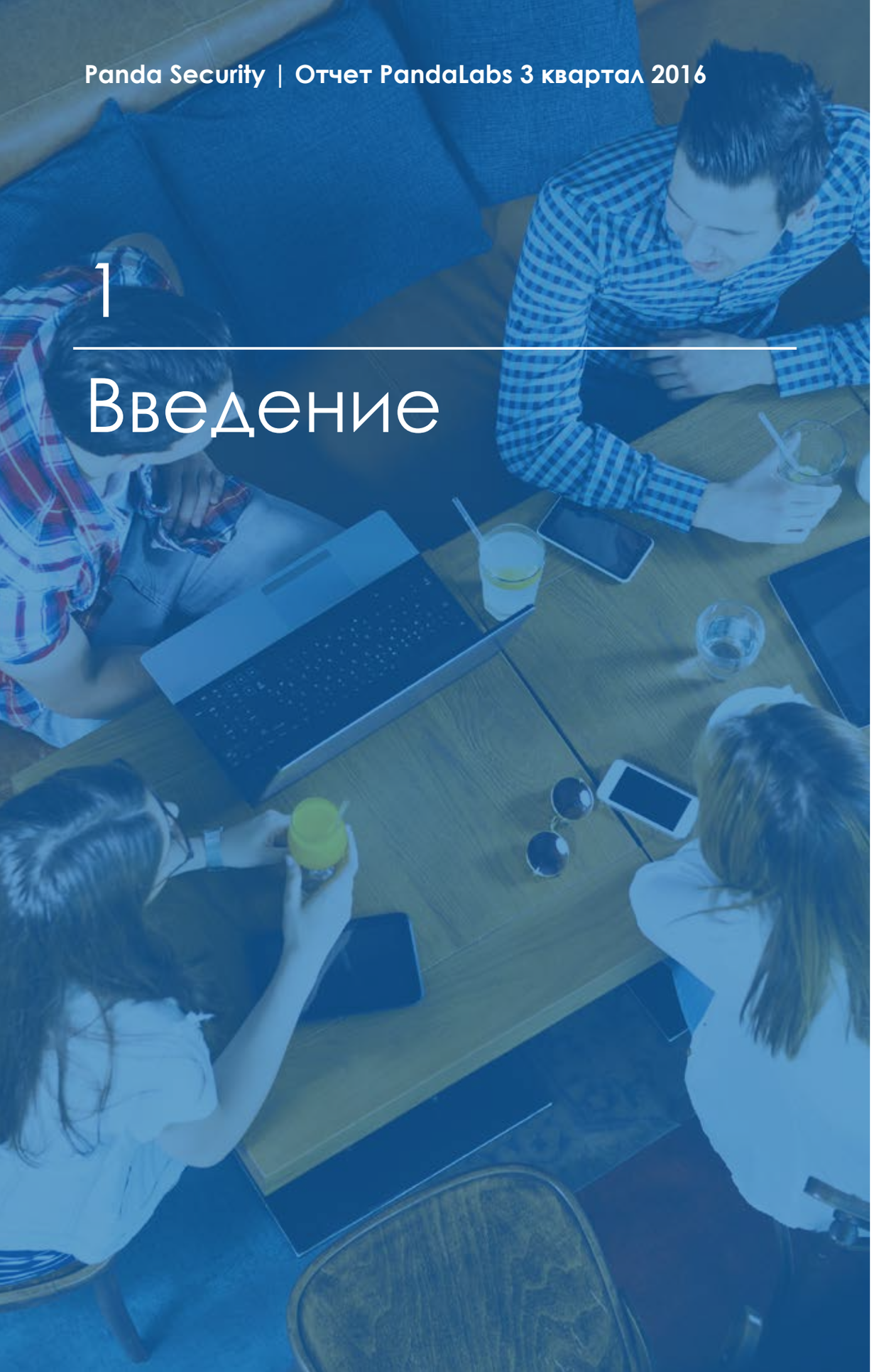
ОТЧЕТ PANDALABS
3 квартал 2016



panda

pandalabs

1. ВВЕДЕНИЕ



1 Введение

В ближайшее время уровень кибер-преступности не снизится. В этом квартале кибер-преступники стали еще более изобретательными, используя инновационные технологии и новые инструменты для распространения своих "творений". Антивирусная лаборатория PandaLabs компании Panda Security перехватила в 3 квартале более 18 миллионов новых образцов вредоносных программ (в среднем свыше 200 000 в день): настораживающие проблемы кибер-угроз были актуальны и в последние месяцы тоже.

В этом квартале трояны снова лидируют среди вредоносных программ, а вместе с шифровальщиками они составляют подавляющее большинство.

В этом квартале возросло число атак с шифровальщиками, что принесло преступникам миллионы долларов.

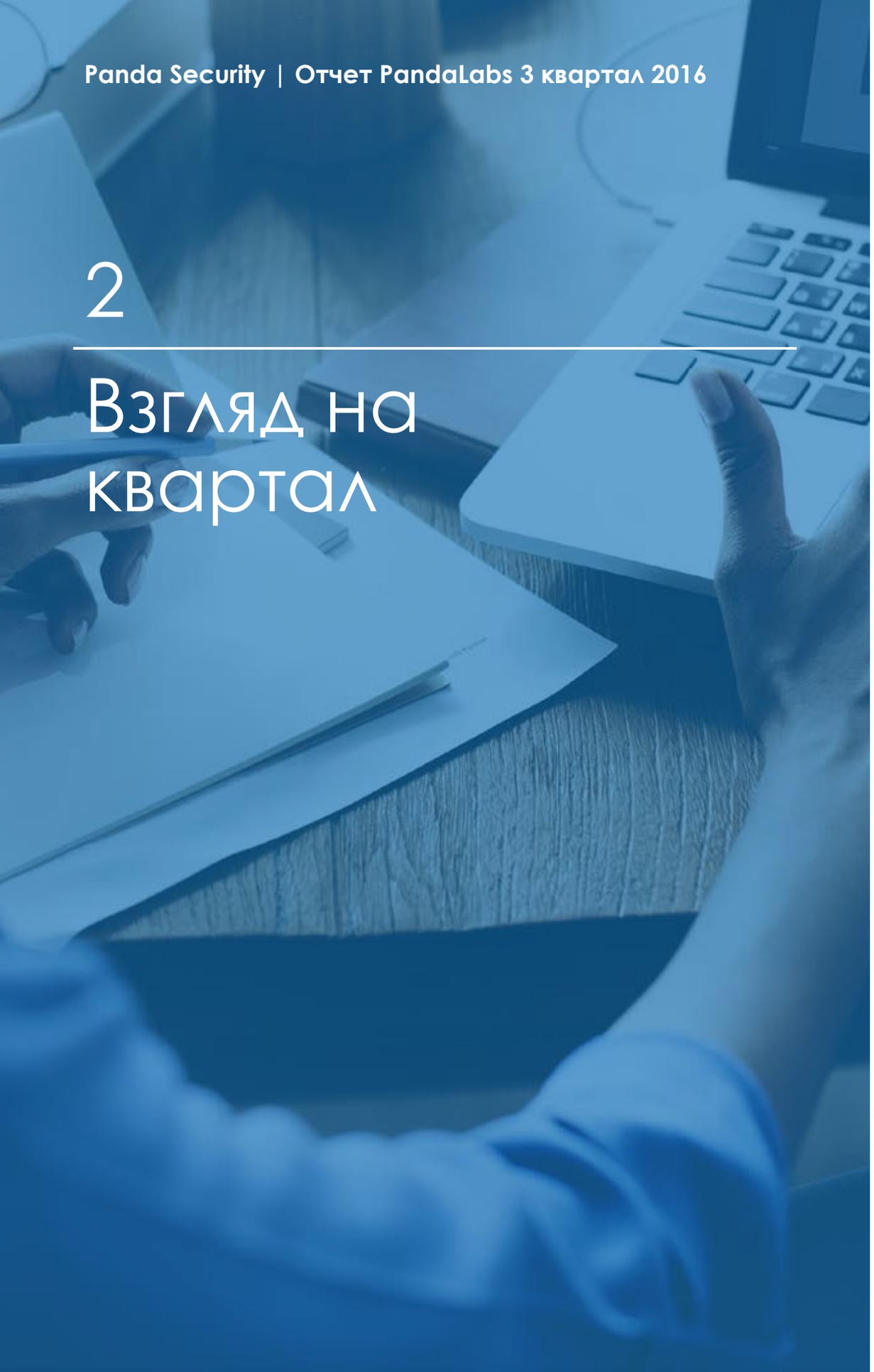
PoS-терминалы в отелях, ресторанах и других публичных местах становятся все более желанной целью для хакеров.

Информация, которую мы собрали за последние 3 месяца, отслеживая поведение вредоносных программ и создание новых угроз, показала проведение **ряда массированных DDoS-атак (Distributed Denial of Service)**, которые во многих случаях были связаны с бот-сетями, основанных не на ПК, а на смарт-устройствах, например, IP-камерах.

Мы рассмотрим последние атаки, связанные с Интернетом вещей (IoT), например, **взломы подключенных к Интернету машин** таких авторитетных марок как Jeep и Tesla. Недавно одна из моделей Tesla стала жертвой расследования, показавшего, как она может удаленно контролироваться без физического доступа.

Что касается мобильных телефонов, то мы проанализируем различные ситуации, связанные с нападениями на устройства с Android, и увидим, как волны шифровальщиков нацеливаются на устройства с iOS.

2. ВЗГЛЯД НА КВАРТАЛ



2

Взгляд на квартал

Шифровальщики

Шифровальщики - это бизнес, который обещает кибер-преступникам высокие прибыли. Т.к. это направление развивается и становится все более изощренным, то и доходы также растут. В июле создатели шифровальщиков Petya и Mischa начали разрабатывать вредоносные программы и соответствующие платежные платформы, оставив вопросы распространения другим людям. Такая новая модель известна как **Ransomware as a Service (RaaS).**

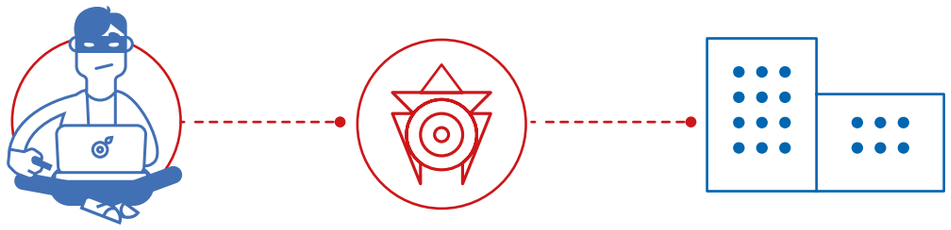
С помощью RaaS разработчики создают шифровальщики, а дистрибьюторы ответственны за заражение жертв. Как и с дистрибьюцией в законном бизнесе: они могут получать более высокие прибыли за счет увеличения своей активности. Чем больше жертв заражено и чем больше денег они заплатили, тем выше становятся доходы дистрибьюторов. Их заработки обычно начинаются с 25%, но потенциально дистрибьютор может повысить свою долю до 85%, если он сможет **выкачивать с жертв свыше 125 биткоинов** (примерно 75 000$) в неделю.

Мы в PandaLabs внимательно следим за эволюцией шифровальщиков. Два раза в месяц мы публикуем в Медиа-центре Panda Security статьи из цикла "Истории Ransomwhere", где мы рассказываем о последних разработках в этой сфере. Мы анализировали, как хакеры используют и злоупотребляют PowerShell - программой, которая по умолчанию идет с Windows 10 - чтобы осуществлять атаки шифровальщиков без необходимости загружать файлы из Интернета или из документа Word с макросами, отправленного по электронной почте. Эти атаки являются кошмаром для разработчиков решений компьютерной безопасности, т.к. в первую очередь они предлагают защиту периметра устройства, тем более, что в данном случае шифровальщик никогда не присутствует на компьютере.

Мы видели очень яркие тому примеры с семейством Locky, которое внедряется в "оффлайновом" режиме, что позволяет зловреду шифровать файлы даже в том случае, если решения безопасности не позволяли ему связаться с сервером, предоставляющим пароль для шифрования.

В дополнение к традиционным техникам заражения через эксплойты и спам, есть и некоторые другие весьма эффективные техники, специально направленные на предприятия.

Мы видели это в сентябре, когда группа хакеров успешно установила шифровальщик Crysis на сервере одной французской компании.



После расследования произошедшего было установлено, что у сервера служба Remote Desktop Protocol была подключена к Интернету. Хакеры пытались проникнуть на сервер, перебирая возможные варианты пароля в течение четырех месяцев. В итоге, осуществив свыше 100 000 попыток, они смогли подобрать регистрационные данные.

Кибер-преступления

Очень сложно оценить уровень кибер-преступности. Специалисты по ИБ, кто ежедневно борется с этими угрозами, понимают его массовость и знают, что эта сфера продолжает расти и развиваться.

Но так ли это все опасно?

Кто-то может подумать, что крупные компании в сфере ИБ, как Panda, очень заинтересованы в том, чтобы показывать рост кибер-преступности, т.к. эти проблемы приносят нам дополнительные прибыли. Однако данные говорят сами за себя. Все больше независимых организаций предоставляют статистику, помогающую нам оценить текущую ситуацию.

Национальное криминальное агентство Великобритании опубликовало отчет, показывающий, что в настоящее время кибер-преступность составляет свыше 50% всех преступлений в стране.

Одно из крупнейших биткоин-ограблений в истории случилось 2 августа. Сумма в биткоинах, равная 60 млн. долларов, была украдена у Bitfinex - компании, которая продает и обменивает криптовалюту. Эти деньги принадлежали клиентам, которые держали их на депозитах в этом "банке". До сих пор нет доказательств того, кто совершил эту атаку, а Bitfinex не предоставил данных о том, как она могла случиться. В настоящее время правоохранительные органы ведут расследование.

В сентябре известный журналист в сфере информационной безопасности Брайн Кребс раскрыл vDOS - "бизнес",

который предлагает сервисы DDoS-атак. Вскоре после этого хакеры vDOS были арестованы (они могли запустить 150 000 атак и заработать 618 000 $ за два года). Сразу после их ареста сайт Кребса подвергся массированной DDOS-атаке, что привело к сбою в его работе на неделю. В конце концов, вмешался Google и защитил его веб-сайт через Project Shield, после чего сайт снова стал работать. Кребс рассказал о возможных последствиях этих атак в своей статье под названием Демократизация цензуры.

Серверы Battle.net компании Blizzard были атакованы группой под названием PoodleCorp, которая взломала три игры (World of Warcraft, Overwatch, Diablo 3). На протяжении квартала было много подобных атак. Подробнее мы поговорим о них в разделе "Интернет вещей", т.к. большинство из них были запущены с использованием бот-сетей на основе таких смарт-устройств как IP-камеры, роутеры и пр.

За последние три месяца было много случаев краж данных, от которых пострадали миллионы людей во всем мире. В июле были взломаны форумы Ubuntu, где пользователи обсуждают все аспекты этой открытой операционной системы на базе GNU/Linux, в результате чего были украдены адреса почты, логины и IP-адреса, принадлежащие 2 миллионам людей. Black Hats также обратили свои взоры на форумы, связанные с популярной игрой для мобильных устройств **Clash of Kings**, видя, что они могли бы взломать их аналогичным образом. В этом случае **хакеры украли персональные данные 1,6 миллиона пользователей.**

Пользователи игры Dota 2 компании Valve также стали жертвами атаки в этом квартале. Был взломан их форум, где была украдена персональная информация 1,9 миллионов пользователей (регистрационные данные, адреса почты и пр.). Эти же хакеры украли 9 миллионов игровых кодов после взлома веб-сайта DLH.net.

Хакеры "озолотились", когда стали взламывать игровые сайты.

Добавьте еще: кража данных у 200 000 пользователей GTAGaming.com; атака на www.minecraftworldmap.com, после чего хакеры опубликовали информацию о 71 000 пользователей.

Еще одна спорная атака на **порнографический сайт Brazzers**, в результате чего были украдены **данные 800 000 пользователей**. Еще одна выдающаяся атака произошла с сервисом обмена мгновенными сообщениями QIP.ru, где были украдены данные 33 миллионов пользователей.

Даже Dropbox не смог избежать проблем. Известный файлообменник недавно обнаружил, что в 2012 году был подвержен атаке. Результат: потеря данных, принадлежащих 68 миллионам пользователей. Но есть одно ограбление, о котором невозможно забыть - это случай с **Yahoo**. Хотя это случилось в 2014 году, но об этом не было известно до сих пор. Всего **было взломано 500 миллионов аккаунтов, что сделано ее самой крупной кражей в истории.**

POS-терминалы - еще одна зона интересов кибер-преступников в наши дни.

PandaLabs обнаружила атаку, от которой пострадали **200 американских учреждений**, большинство из которых рестораны. В результате были украдены данные банковских карт с помощью **вредоносной программы PunkeyPOS.**

Популярная сеть ресторанов быстрого питания Wendy's стала жертвой аналогичной атаки: с помощью другого варианта PunkeyPOS были заражены терминалы оплаты в более чем 1000 ее торговых точках.

Наша лаборатория обнаружила еще одну подобную атаку, И снова жертвами стали рестораны в США, но в этом случае **300 POS-терминалов** были заражены с помощью вредоносной программы **PosCardStealer.**

Еще одна критическая сфера, о которой мы писали в прошлых отчетах PandaLabs, - это отели.

В этом квартале был атакован ряд отелей HEI Hotels. Мошенники использовали вредоносную программу для кражи данных банковских карт в их PoS-терминалах. Среди пострадавших гостиниц оказались гостиницы Sheraton, Westin, Hyatt и Marriot.

Но кибер-преступники бросили свой взгляд на что-то более амбициозное, нежели платежные терминалы. В июле были обворованы банкоматы First Bank (Тайвань). Это преступление было совершено в организованной форме. Хакеры находились рядом с каждым банкоматом, изъяв в общей сложности свыше 2 миллионов долларов. Мы знаем, что они установили на эти банкоматы вредоносные программы (конечно, после взлома внутренней сети банка), а затем они извлекли деньги без физического контакта с ними, используя удаленные команды, что подтверждается записями с камер видеонаблюдения.

Успешная атака на финансовое учреждение может принести миллионы долларов.

В августе SWIFT распространила заявление об осуществлении ряда атак, подобных случаю с банком Бангладеша. Правда, они не сообщили о количестве атакованных банков и суммах похищенного. Однако упоминается о том, что эти банки не предпринимали достаточных мер безопасности.

Программы вознаграждения для тех, кто находит уязвимости.

Технологический гигант **Apple** - одна из крупнейших компаний в мире, кто предлагает программу вознаграждений. Компания предлагает до **200 000$** тем, кто сможет найти уязвимости в продуктах Apple. Удивительно то, что Apple долгое время не имела такой программы, в то время как другие технологические гиганты уже предлагали вознаграждения за поиск уязвимостей.

Интересно, что такие программы вознаграждений имеют различные типы организаций. Хотя, как правило, они выплачивают их деньгами, но есть и такие, которые предоставляют их в натуральной форме, например, **United Airlines.** В августе компания наградила одного из специалистов по безопасности миллионом миль, который обнаружил в их ПО 20 дыр безопасности. "Белые" хакеры в Offensi.com также были награждены **1 000 000 миль,** которые они щедро пожертвовали трем благотворительным фондам.

В июле пять членов банды по отмыванию денег были арестованы в Лондоне. Все они были россиянами, а лидерами банды были 30-летний Аслан Абазов (получил 7,5 лет тюрьмы) и 29-летний Аслан Гергов (7 лет и 3 месяца).

Эдвард Майерчик признал себя виновным в краже фотографий знаменитостей, в итоге получил 9 месяцев тюремного заключения (изначально прокуратура просила 5 лет). Майерчик признался, что он получил доступ к аккаунтам своих жертв в iCloud в результате запуска фишинговой атаки, которая позволила ему получить их регистрационные данные.

Для некоторых людей взлом таких знаменитых людей считается высоким достижением. Например, 44-летний румын Марчел Лехел Лазар был приговорен к 52 месяцам тюремного заключения за взлом ряда влиятельных людей. Среди примерно 100 его жертв оказались Хиллари Клинтон, Джордж Буш (отец и сын), Колин Пауэл, Николь Кидман и Роберт Рэдфорд.

Мобильные угрозы

Устройства с Android по-прежнему "на линии огня". Люди продолжают приобретать смартфоны, а кибер-преступники продолжают их атаковать. Т.к. операционная система Android имеет самую большую долю рынка и позволяет пользователям устанавливать программы не только из официального магазина, то это делает ее легкой мишенью для злоумышленников, хотя, к счастью, Google усиливает безопасность. Различные меры защиты (которые следуют из последней версии ядра Linux) будут активированы в Nougat (7 версия Android).

Однако в большинстве случаев таких мер защиты недостаточно. Производитель решений безопасности компания **Checkpoint обнаружила четыре проблемы безопасности, которые потенциально могут скомпрометировать 900 моделей устройств с Android, оснащенных процессорами Qualcomm Snapdragon.**

Gugi, троян под Android, способен преодолеть барьеры безопасности в Android 6: он может красть банковские данные и информацию с других приложений, установленных на этих устройствах.

Как он это делает? Когда пользователи используют легитимное приложение, Gugi накладывает другой экран и запрашивает информацию, которая без ведома жертвы будет отправлена непосредственно хакерам.

В последнее время растет число атак шифровальщиков на iPhone и iPad. Но в отличие от атак под Windows, для атак на данные устройства кибер-преступники не используют вредоносные программы. Вместо этого они используют остроумие. Для выполнения атаки они используют AppleID жертвы и их пароль (которые они, возможно, получают в результате фишинговых атак или в силу того, что пользователи используют одинаковые регистрационные данные с другими онлайн-сервисами), а затем активируют режим Lost из приложения “Найти мой iPhone” и добавляют сообщение о том, чтобы жертва заплатила выкуп в биткоинах вместо того, чтобы предоставить пароль для разблокировки.

В августе Apple срочно опубликовал версию iOS 9.3.5 своей операционной системы для мобильных устройств. Данная версия исправляла три уязвимости "нулевого дня", которые использовались шпионской программой Pegasus. Pegasus был разработан израильской компанией NSO Group, которая предлагает хакерские продукты, подобные тем, что предлагает Hacking Team.

Интернет вещей

В ходе конференции DefCon, проходившей в августе в Лас-Вегасе (США), исследователь Эндрю Тирни показал, как можно взломать термостат, который он сам модифицировал. После того как он получил контроль над ним (вставив в него SD-карту), температура поднялась до 99 градусов по Фаренгейту (примерно 37 градусов по Цельсию), отменить которую можно было только с помощью PIN-кода. Термостат, подключенный к IRC-каналу, запрашивал биткоин за получение PIN-кода. Хот это было всего лишь доказательство концепции, а к устройству все же был необходим физический доступ, но мы можем понять, что атаки, с которыми мы столкнемся в ближайшем будущем, будут непосредственно направлены на огромное количество бытовых устройств, подключенных к Сети.

Не стоит ждать, потому что уже миллионы устройств из "Интернета вещей" были скомпрометированы. Бот-сеть LizardStressed, созданная группой Lizard Squad, запустила разрушительную DDoS-атаку одновременно против Playstation и Xbox, при этом в основном она состояла из подобного рода устройств.

По данным Arbor Networks, большинство таких устройств являются IP-камерами, и они могут быть взломаны просто за счет перебора комбинаций "имя пользователя - пароль". Т.к. многие пользователи не меняют регистрационные данные, установленные производителями по умолчанию, то получить к ним доступ довольно просто. Уже запускались атаки до 400 Гбит/сек. Другое любимое устройство, используемое для подобного рода атак, - это роутеры, причем они используются уже достаточно длительное время.

В конце сентября французская хостинговая компания **OVH столкнулась с массивной DDoS-атакой, достигавшей 799 Гбит/сек.** А в конце атаки трафик превысил 1 Тбит/сек. Глядя на данные, предоставленные OVS, атака была запущена со 152000 устройств, а большинство из них принадлежали к категории "Интернет вещей" (IP-камеры, видеорегистраторы и пр.).

Что касается автомобильной сферы, то исследователи из **Университета Бирмингема** продемонстрировали, как они смогли **взломать системы открытия дверей на любых автомобилях, проданных Volkswagen Group** за последние 20 лет. Через обратный инжиниринг, они сумели сделать это с помощью криптографического ключа, использующегося всеми машинами VW. Как ни странно, после получения ключа им пришлось стоять на расстоянии 300 метров от взламываемого автомобиля в ожидании определенной команды на радиоустройстве, чтобы перехватить другой ключ, уникальный для каждого автомобиля. После получения этой информации они смогли легко клонировать пульт дистанционного управления, который открывает и закрывает двери машины.

Исследователи **Чарли Миллер и Крис Валашек**, которые **в прошлом году показали, как можно удаленно взломать Jeep Cherokee**, в этом году пошли еще дальше, показав, как можно перехватить сигналы и отключить стояночный тормоз, отключить руль или по команде повернуть руль на любой скорости. В отличие от предыдущей ситуации, чтобы получить контроль над машиной, им пришлось непосредственно подключить к ней компьютер. Важно, что мы обращаем отдельное внимание на эти взломы, угрожающие жизни: Ваша жизнь может быть в опасности, если хакеры смогут манипулировать управляемой Вами машиной.

В сентябре китайские ученые из Keen Security Labs показали, как удаленно взломать машину Tesla, будь она припаркована или находясь в движении. В их видео Вы можете увидеть, как можно удаленно контролировать машину без физического контакта с ней: можно открыть или закрыть двери, при движении машины можно открыть багажник, они даже смогли удаленно контролировать тормоза. Ученые заранее отправили информацию производителям, чтобы они смогли исправить обнаруженные проблемы в последней версии своей прошивки.

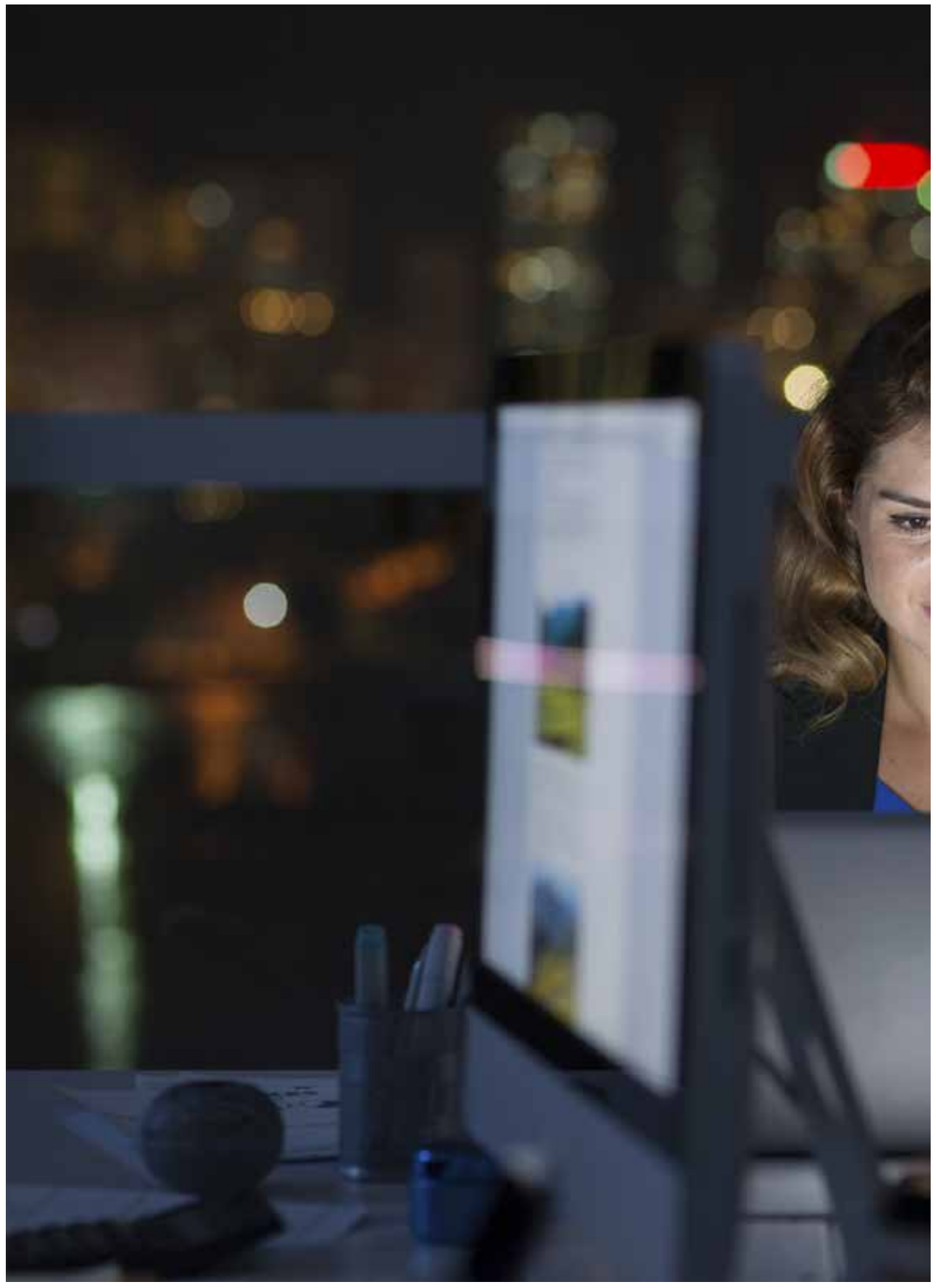
Кибер-войны

В середине предвыборной кампании в США случилась атака против **Национального комитета Демократической партии (DNC).** Во время этой кибер-атаки **были похищены и опубликованы все виды конфиденциальных данных.** Очень сложно, а иногда и невозможно, определить, кто стоит за атаками, но в данном случае сразу же обвинили русских хакеров, за которыми стоит Правительство России, пытающееся навредить успехам Демократической партии на выборах Президента США. Видимо, за атакой стоит две разные группы хакеров (обе из России), и одна из них **опубликовала 20 000 электронных писем в WikiLeaks.**

В продолжение темы выборов, **ФБР предупредило о том, что были взломаны два сайта избирательной кампании,** и как минимум один из зарубежных хакеров смог получить информацию о регистрации избирателей.

Правительства понимают всю важность кибер-безопасности. Президент США Б. Обама признал, что впереди еще много работы, особенно если вспомнить, что сеть Белого дома в прошлом уже была взломана. В сентябре он назвал **первого Руководителя Службы информационной безопасности в истории США.**

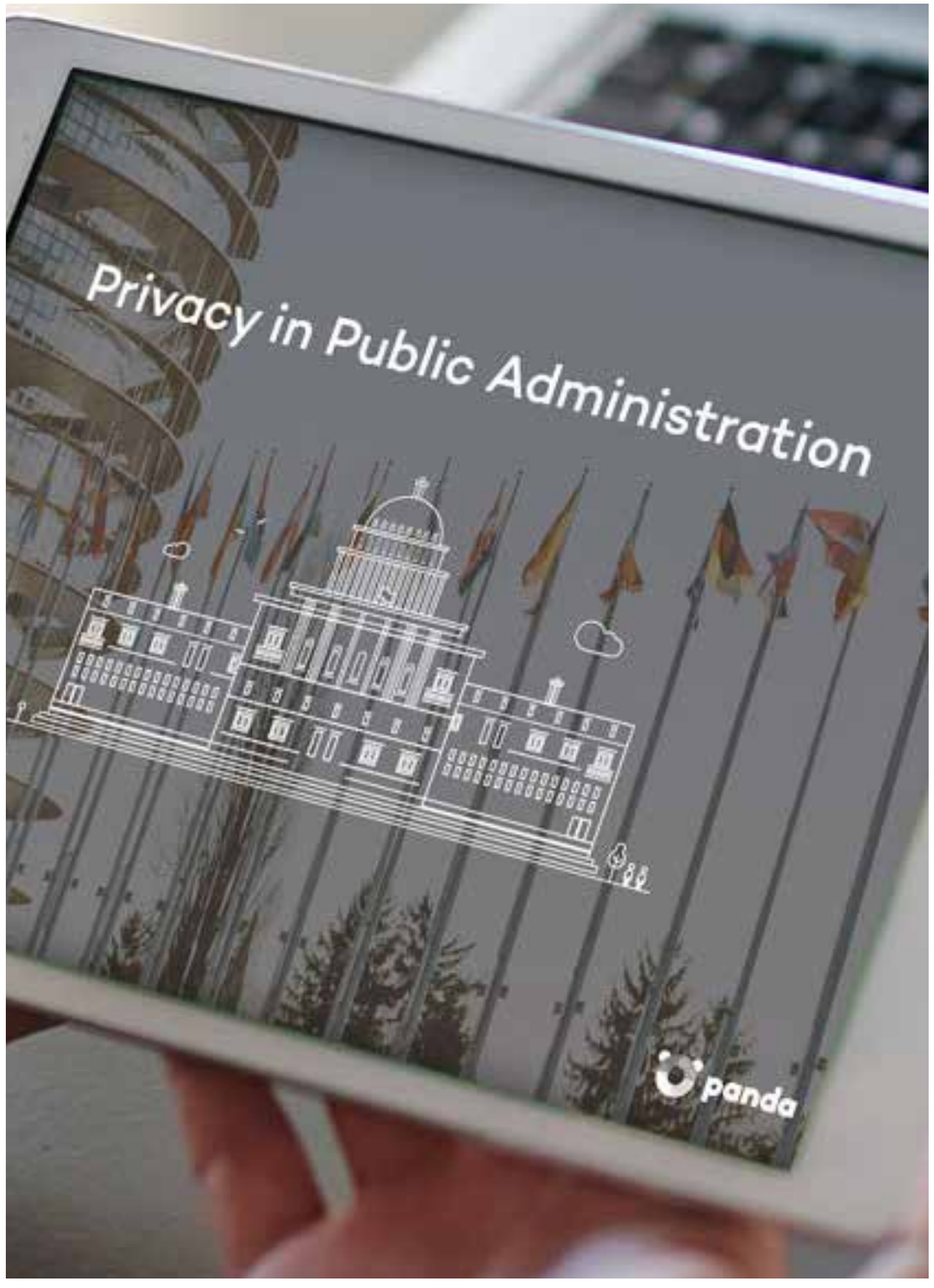
В августе группа под названием **"The Shadow Brokers" заявила, что они взломали Агентство национальной безопасности (АНБ).** Они рассказали о некоторых похищенных видах кибер-оружия и обещали продать их по высокой цене. До сих пор неизвестно, кто стоял за данной атакой, но было предположение, что, скорее всего, как всегда, виновата Россия. В любом случае, кажется, что они использовали такие же инструменты для запуска своей атаки на АНБ.



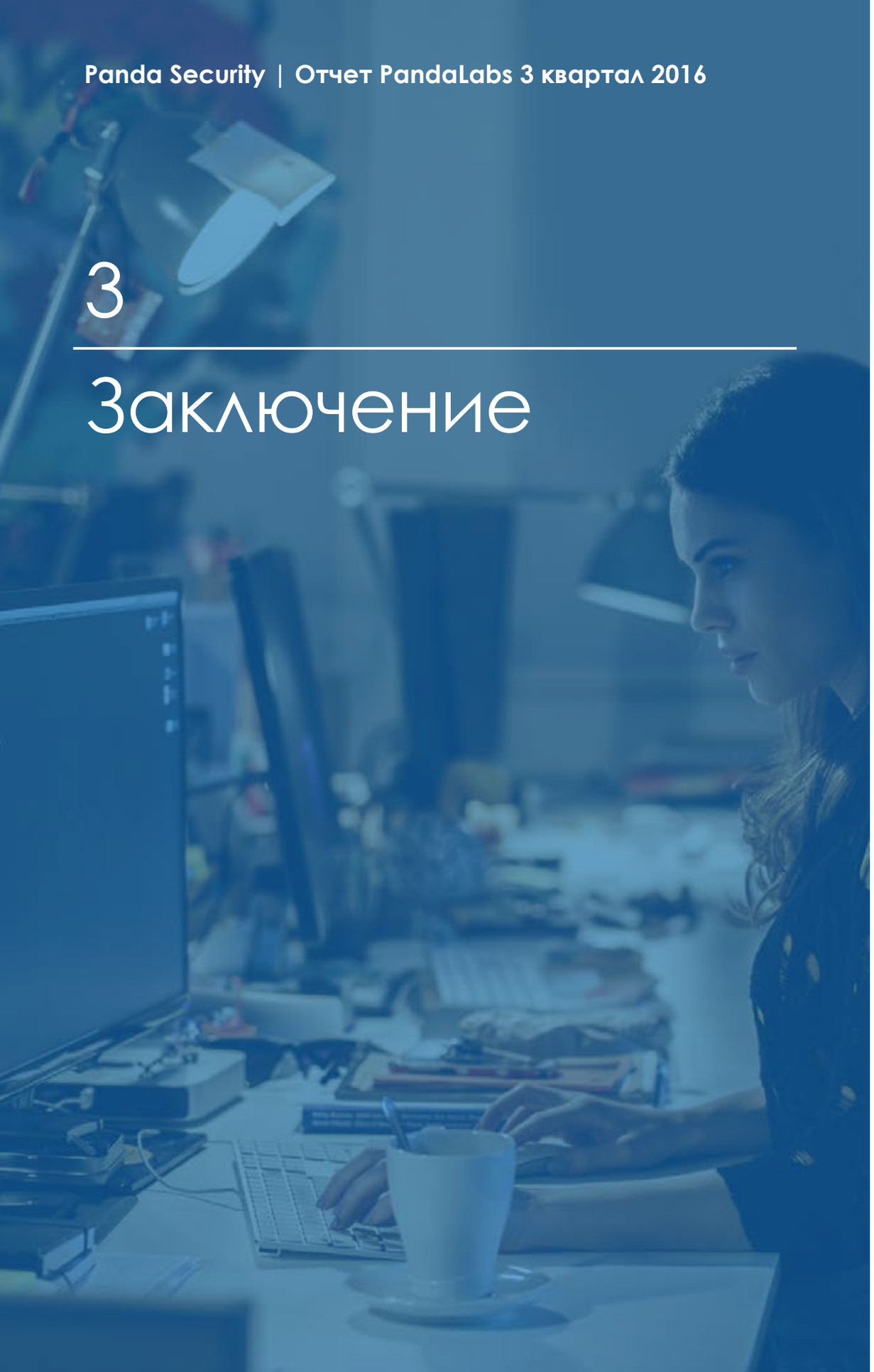
Во многих случаях мы обсуждаем атаки, которые, возможно, спонсируются правительствами разных стран, но как и в случае с кибер-преступниками, практически невозможно определить виновных. Мы были удивлены, узнав, что **Google** уведомляет своих пользователей в том случае, когда они обнаруживают такой тип атаки, о чем заявила Дайана Грин. В настоящий момент они отправляют порядка **4 000 уведомлений каждый месяц.**

Прокуратура **Южной Кореи** считает, что северокорейцы были ответственны за **взлом десятков аккаунтов электронной почты, принадлежащих государственным чиновникам.**

И снова критические инфраструктуры стали главными новостными темами после того как выяснилось, что **Иран удалил вредоносные программы с двух нефтехимических заводов. Общеизвестно, что на этих двух заводах перед этим произошли пожары**, так что теперь ведется расследование, по итогам которого станет понятно, имеют ли к ним какое-либо отношение найденные вредоносные программы.



3. ЗАКЛЮЧЕНИЕ



3 Заключение

Конец 2016 года уже не за горами, и **мы должны продолжать обращать внимание на эволюцию DDoS-атак.** Сочетание миллионов **взламываемых IoT-устройств** и все более быстрого Интернет-подключения дома может превратить одну из таких атак в один из самых крупных Интернет-кошмаров, способных навредить каждому Интернет-пользователю, особенно компаниям, на которые нацелены эти профессиональные вымогатели.

Растет число случаев краж данных, превысив уровень предыдущего квартала. В 3 квартале были украдены данные 500 миллионов пользователей Yahoo. **Так что в наши дни очень важно предпринимать соответствующие меры защиты: никогда не забывайте про двухэтапную авторизацию**, когда Вы регистрируетесь в онлайн-сервисах, потому что она позволит предотвратить взлом Вашего аккаунта, даже если Ваши регистрационные данные были украдены.

Мы будем ждать Вас через три месяца, чтобы проанализировать и обсудить 4 квартал 2016 года. Тем временем, PandaLabs продолжит информировать Вас обо всех новостях информационной безопасности на нашем сайте и на страницах наших аккаунтов в соцсетях:

http://www.pandasecurity.com/mediacenter/
https://www.facebook.com/PandaCloudRus
http://www.vk.com/PandaCloudRus
http://twitter.com/#!/PandaCloudRus

pandalabs

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

panda

pandalabs