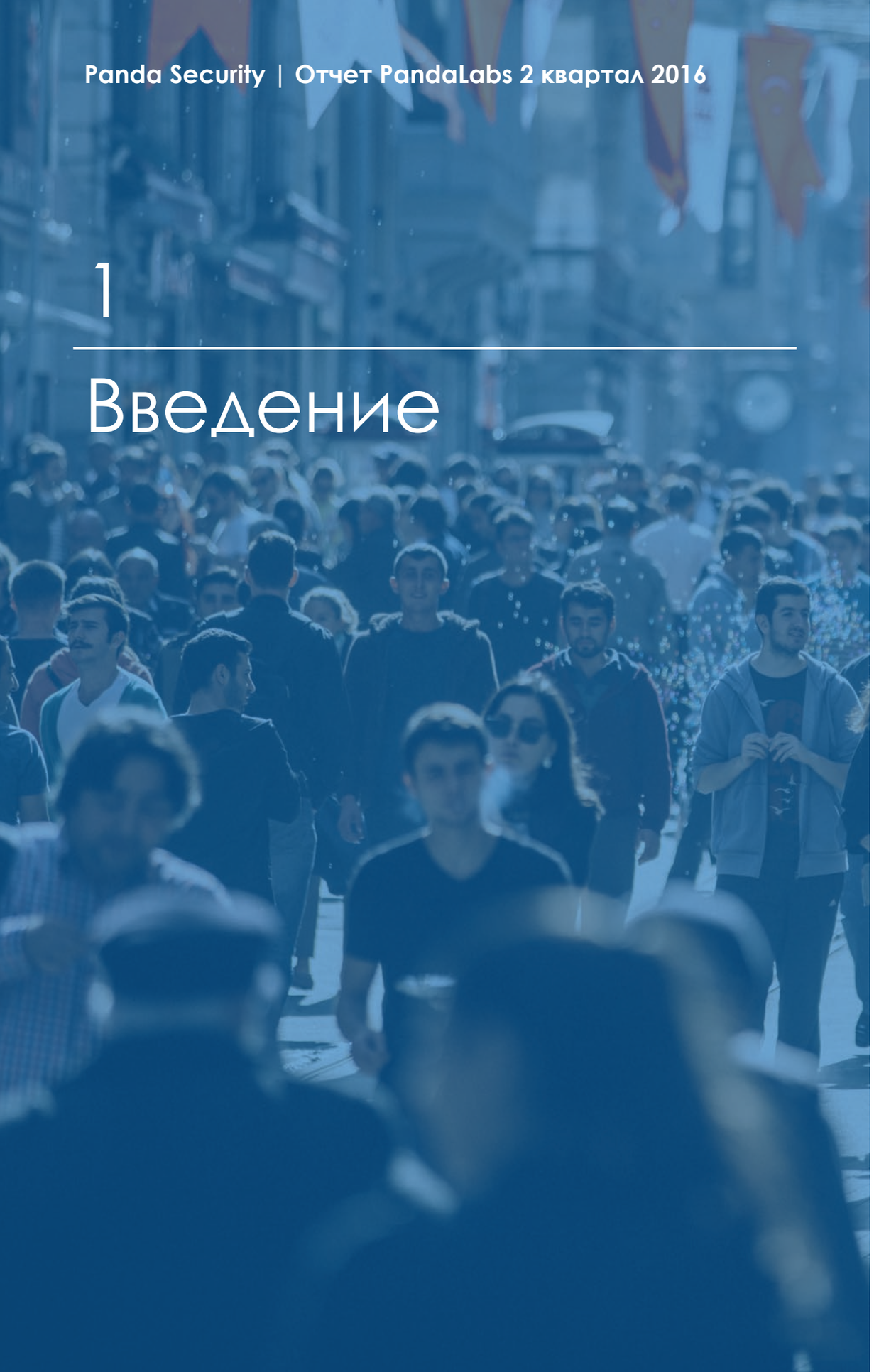
ОТЧЕТ PANDALABS
2 квартал 2016

panda

pandalabs

1. ВВЕДЕНИЕ



1 Введение

Кибер-пространство стало неотъемлемой частью нашей повседневной жизни. Цифровая трансформация затронула домашних и корпоративных пользователей, т.к. количество устройств, подключенных к Сети, продолжает расти.

Такие понятия как «цифровой дом» или «BYOD» (Bring Your Own Device) уже являются частью нашей цифровой Вселенной: все больше Интернет-пользователей работают из дома или используют свои собственные устройства как в личных, так и в профессиональных целях. Это означает, что становится все больше дыр безопасности.

По данным PandaLabs в течение квартала было обнаружено свыше 18 млн. новых образцов вредоносного ПО.

Трояны сохранили свою лидирующую позицию в списке выявленных угроз, показав рост числа атак шифровальщиков в этой категории. Среднее количество новых угроз, обнаруживаемых каждый день – 200 000. Этот показатель чуть ниже показателя первого квартала в 227 000 образцов. **Наряду с атаками шифровальщиков, большинство других атак в этом квартале было нацелено на кражу персональной информации и регистрационных данных пользователей.**

Также наблюдается **ощутимый бум в сфере «Интернета вещей»**. Это породит новые атаки и потенциально может серьезно повлиять на нашу жизнь. Например, в ближайшем будущем кибер-атаки позволят кибер-преступникам осуществлять кражу наших машин, удаленно деактивируя противоугонные сигнализации и разрешая запуск двигателя.

Каждый день мы видим все больше уязвимостей среди мобильных телефонов. Напомним, что большинство проблем, которые возникают в результате этих дыр безопасностей, по большей части связаны с отсутствием (или запоздалостью) обновлений, поступающих от различных производителей аппаратного обеспечения.

2. ВЗГЛЯД НА КВАРТАЛ

2

Взгляд на квартал

Шифровальщики

Мы знаем, что шифровальщики – это огромный бизнес для кибер-преступников, но очень сложно оценить его реальные масштабы. В 2015 году Министерство юстиции США опубликовало данные о том, что Центр рассмотрения жалоб по фактам совершения интернет-преступлений (Internet Crime Complaint Center, IC3) получил 2500 жалоб на атаки шифровальщиков.

Жертвами этих зловредов суммарно было выплачено примерно 24 миллиона долларов США. Шифровальщики – это глобальное явление. Принимая во внимание общую сумму выкупа в данном примере и повсеместный рост этих вредоносных программ во всем мире, **мы можем сделать вывод, что годовые доходы кибер-преступников от действий шифровальщиков составляют миллиарды долларов США**.

Оглядываясь назад, мы можем вспомнить различные случаи атак шифровальщиков на учреждения здравоохранения. Данный квартал начался с новой жертвы: *MedStar Health*. Эта некоммерческая медицинская организация пострадала от атаки шифровальщика настолько серьезно, что они вынуждены были отключить свои системы на несколько дней.

В случае с MedStar Health, кажется, была направленная атака, использовавшая существующие в их системах уязвимости. Тем не менее, большинство подобных атак осуществляются с помощью вредоносных почтовых вложений или взломанных интернет-сайтов. Что и произошло в апреле с компанией Maisto International, производителем игрушек с дистанционным управлением: посетители ее сайта неосознанно становились жертвами шифровальщика. Их взломанный веб-сайт заражал своих посетителей с помощью хорошо известного набора эксплойтов Angler. Его цель – идентифицировать у пользователя популярные программные продукты (flash, java и т.д.), а затем использовать различные уязвимости этих установленных приложений для поражения компьютера.

Впрочем, атаки через веб-сайты – это не единственный способ. Кибер-преступники используют другую популярную ныне тактику, известную как malvertising (вредоносная реклама): размещение рекламы в публичных местах на высоко посещаемых сайтах для заражения пользователей этих сайтов.

Известный блог perezhilton.com недавно стал жертвой двух атак вредоносной рекламы. Хакеры ежедневно заражали свыше 500 000 пользователей, используя набор эксплойтов Angler.

Направленные атаки используют уязвимости в системе. Распространенные угрозы: взломанные сайты и вредоносная реклама

Один из наиболее интересных случаев с шифровальщиками, которые мы наблюдали в данном квартале, произошел с компанией из Словении.

Сотрудник компании, ответственный за IT, получил по почте письмо из России, в котором сообщалось о взломе их сети. Российские кибер-преступники взломали сеть и приготовили ее для запуска шифровальщика на всех компьютерах сети. **Если словенская компания откажется заплатить выкуп в размере 9000 евро (в биткоинах) в течение 3 дней**, то шифровальщик будет запущен. В доказательство того, что у них есть доступ к корпоративной сети, они отправили файл со списком всех устройств, подключенных к внутренней сети предприятия.

Многие жертвы шифровальщиков предпочитают платить выкуп, но это вовсе не гарантирует возврата похищенных (зашифрованных) данных. В мае *кардиологическая больница в Канзасе (США)* была атакована шифровальщиком, и руководство решило заплатить выкуп за возврат данных. В результате они были шокированы тем, что присланный пароль позволял расшифровать только часть информации. Чтобы восстановить оставшуюся информацию, хакеры потребовали второй платеж. Но больница отказалась платить второй раз.

Профессиональная команда CSLFR, участвующая в NASCAR, стала свидетелем атаки шифровальщика на три свои ПК. Он зашифровал информацию, которая оценивалась в 3 миллиона долларов США. В этом случае CSLFR также заплатил выкуп (500 долларов США), но, к счастью, в этом случае они получили возможность восстановить всю информацию.

Стоит ли платить выкуп?

Давайте скажем так: если жертвы платят выкуп кибер-преступникам, они повышают результативность атак.

Если атака успешна и принесла прибыль, то хакеры будут атаковать еще большее число пользователей. В долгосрочной перспективе эти атаки могут навредить нам всем.

Оплата выкупа за восстановление информации еще больше способствует преступной деятельности.

Платить или не платить – этот вопрос остается спорным. В апреле Джеймс Трэйнор, помощник директора «кибер-дивизиона» в ФБР, вполне четко обозначил позицию в своем публичном обращении:

"Оплата выкупа не гарантирует организации, что она получит свои данные назад: мы видели случаи, когда организации никогда не получали ключ для расшифровки после оплаты выкупа. Оплата выкупа не только поощряет действующих кибер-преступников атаковать больше организаций, но также дает стимул для других злоумышленников заниматься подобной нелегальной деятельностью. И, наконец, оплатив выкуп, организация может таким образом способствовать финансированию других видов незаконной деятельности, связанных с преступлениями».

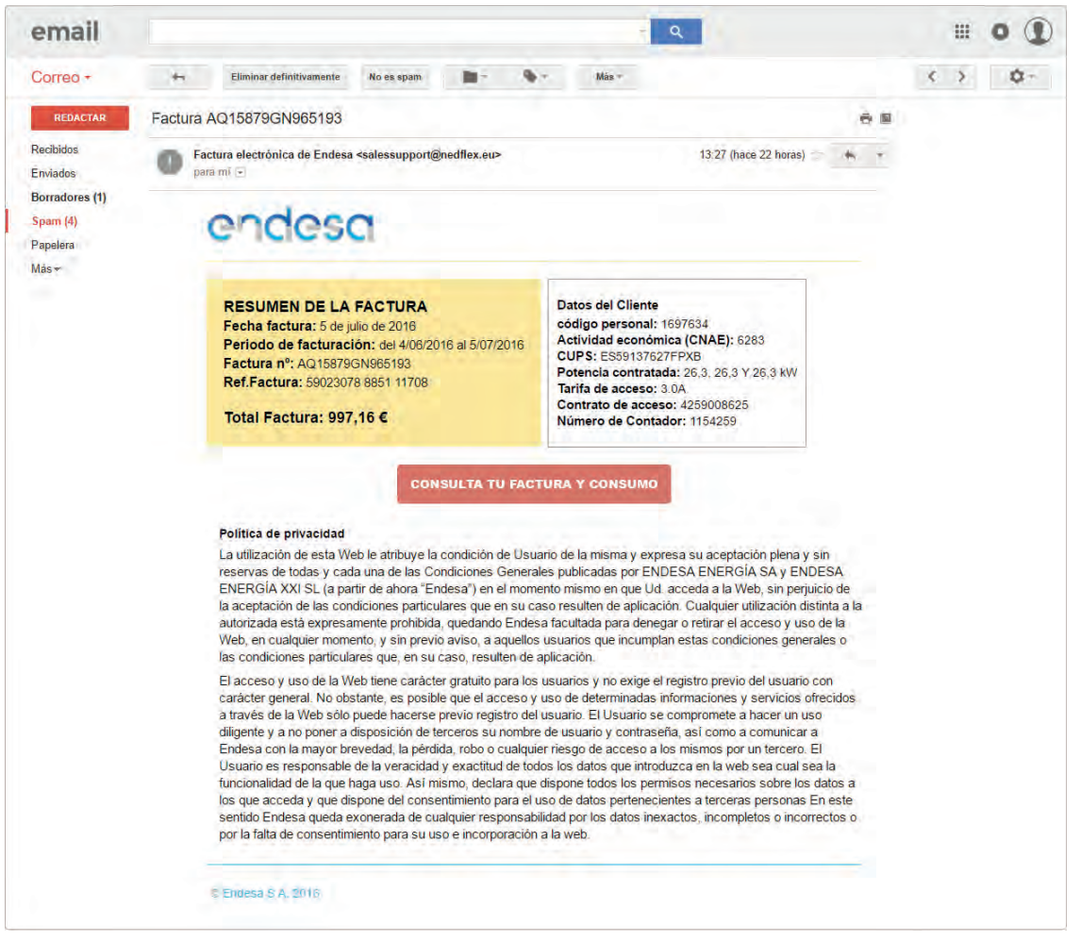
Эволюция вредоносных писем

Исходная точка данных атак – это не только использование вредоносной рекламы или взломанных сайтов. Существенная часть таких атак начинается с электронных писем, которые замаскированы под счета или уведомления.

Одна из таких атак с помощью почты произошла в Польше и Испании, где кибер-преступники маскировались под известные энергокомпании, работающие в этих странах.

Преступники отправили жертвам вредоносные письма, которые не содержали вложений: в тексте письма содержался счет со ссылкой для просмотра «расшифровки счета».

При нажатии на эту ссылку пользователь перенаправлялся на ложный веб-сайт, являющийся точной копией сайта настоящей энергетической компании.



Там пользователь мог скачать «счет». Если пользователь скачивал и открывал «счет», то его компьютер заражался шифровальщиком.

Если бы у Вас был шанс, что бы Вы сказали кибер-преступнику, который «положил на Вас свой глаз»?

Мы стали свидетелями эволюции шифровальщиков. Как правило, жертвам предоставляют подробную инструкцию о том, как заплатить выкуп. В некоторых вариантах шифровальщиков (например, новый вариант семейства Jigsaw) **хакеры пошли дальше и предложили чат-сервис, где пользователи могут пообщаться с вымогателями в реальном времени и обсудить условия оплаты выкупа.**

Теперь можно общаться с кибер-преступниками, чтобы обсудить оплату выкупа за украденную информацию.

Одна из наиболее оригинальных атак шифровальщиком за последний квартал (и самая опасная!) произошла в России.

Ее уникальность в способе распространения, потому что вредоносная программа отправлялась по почте, но фактически не выполнялась. Она была написана в виде специального обновления для программы одного из крупных производителей ПО в России (свыше миллиона корпоративных пользователей в России и бывшем СССР), и работала только в том случае, если на компьютере стояла данная программа.

Она заставляла пользователей обновить свою программу, и если пользователь осуществлял это, то зловред подключался к базе данных программы, осуществлял в ней поиск контрагентов и отправлял себя по найденным адресам электронной почты. Одновременно с этим он заражал компьютер шифровальщиком, зашифровывал файлы и далее, как обычно, требовал выкуп.

Кибер-преступления

Мы видели, как это может быть сделано различными способами: через шифровальщики, за счет кражи информации у людей и предприятий, а иногда с помощью направленных атак на определенные банки. В последние месяцы эти случаи стали очень серьезными, и когда мы их изучаем, то можно увидеть, какое влияние они оказывают на предприятия (от благотворительных фондов или финансовых компаний до порнографических сайтов и сайтов для голосования)… страдает даже полиция. Рискует каждый.

Кража информации

Team Skeet - веб-сайт, который распространяет порновидео и принадлежит *Paper Street Media network*, недавно пережил атаку, в результате которой были украдены данные 237 000 пользователей. Причем были украдены не только регистрационные данные и адреса почты пользователей, но и их фактический адрес проживания. **Позже эти данные были проданы в онлайне по 400 долларов США за пользователя**, что в сумме могло составить порядка 95 миллионов долларов США. Но наверняка преступники предложили хорошие скидки в зависимости от объема данных.

Шифровальщики и кража данных у людей и предприятий - это тактика кибер-преступлений.

Благотворительная организация *National Childbirth Trust* (NCT, Лондон) 7 апреля столкнулась с нарушением безопасности. Во время атаки были похищены данные 15 085 пользователей, включая логины, зашифрованные пароли и адреса почты.

Acer, известный производитель оборудования, также стал жертвой атаки на свой интернет-магазин, где были украдены данные 34 500 их клиентов. **Самое ужасное, что их сайт был взломан на протяжении года (с мая 2015 по апрель 2016), о чем компания и не подозревала**.

В июне хакер по прозвищу "*TheDarkOverlord*" выставил на продажу данные пациентов трех разных американских компаний. В целом за украденные данные более чем 650 000 пользователей TheDarkOverlord запросил 700 000 долларов США. Вскоре этот же человек попытался продать данные 9,3 миллионов клиентов одной страховой медицинской компании за 750 биткоинов (примерно полмиллиона долларов США).

В Испании **группа Anonymous опубликовала список персональных данных 5 000 сотрудников национальной полиции**. Данные были получены не с серверов полиции, а в результате атаки на веб-сайт организации, занимающейся социальным обеспечением полицейских.

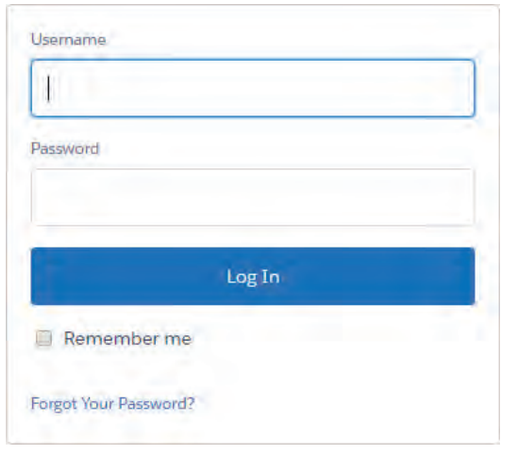
Когда речь идет о расследованиях по борьбе с кибер-преступностью, то при упоминании имени *Крис Викери* надо звонить в колокола. Этот специалист по безопасности нашел на Amazon сервер, где кто-то оставил **базу данных, содержащую 93,4 миллиона записей об избирателях в Мексике**: почтовые адреса, официальные идентификаторы и пр. Викери сообщил об этом в органы власти Мексики, а база данных была уничтожена. Можно предположить, что кто-то украл данные и использовал облако Amazon для временного хранения.

Крис Викери также обнаружил другой инцидент с кражей информации. В этом случае были украдены контактные данные 1,1 миллиона пользователей с веб-сайта beautifulpeople.com. Несмотря на то, что Викери сообщил об этом владельцам сайта, преступники продавали эту базу данных на черном рынке.

Помимо преступников и организаций, чья основная цель - причинить вред всем в Интернете, существуют также вполне легитимные инструменты, которые могут работать против нас.

В случае с популярной утилитой удаленного доступа *TeamViewer*, были украдены данные огромного числа пользователей, чьи компьютеры открывались для удаленного доступа. В силу огромного числа жертв, первая мысль была связана с тем, что кто-то вошел в TeamViewer и взял их базы для последующего несанкционированного доступа. Позже выяснилось, что украденная информация пришла от самих пользователей, использующих одинаковые регистрационные данные для подключения к различным сервисам.

Это широко распространенная тактика хакеров: **если они украли регистрационные данные от одного сайта, то они пытаются получить доступ к другим сервисам, используя одинаковую комбинацию имя пользователя и пароль**. Они знают, что многие люди используют одинаковые регистрационные данные на разных веб-сайтах.



В этом случае, как только хакеры получали доступ к ПК жертвы, они подключались к его аккаунту PayPal и грабили все деньги.

Рост инцидентов с PoS-терминалами

Другой широко распространенный и популярный способ кражи осуществляется через терминалы в точках продаж. PoS-терминалы подвержены определенным вредоносным инфекциям, которые специально разрабатываются для кражи данных с банковских карт через такие терминалы.

Чаще всего жертвами становятся отели, что мы могли видеть на примере *Hard Rock Hotel & Casino* в Лас-Вегасе (США). Известно, что PoS-терминалы были заражены в период с октября 2015 до марта 2016 г., а за это время были украдены данные банковских карт, использованных в этой организации.

Такие происшествия случаются во всем мире. Недавно была атакована испанская сеть люксовых отелей. К счастью, атака вовремя была остановлена, не достигнув PoS-терминалов, а потому ограбление было предотвращено. Эта атака была специально разработана для данной сети отелей. Чтобы разрешить внешние подключения и остаться не обнаруженными, хакеры зарегистрировали домен с именем одной из жертвы из африканской страны.

PoS-терминалы в гостиницах, ресторанах и на предприятиях становятся более привлекательными для хакеров

Но на "линии огня" оказались не только PoS-терминалы и отели. Кибер-преступники для кражи данных банковских карт обратили свою внимание на рестораны. Свыше 1000 заведений, принадлежащих популярной сети фаст-фудов *Wendy's*, стали жертвами зловредов для PoS. Преступники сумели извлечь данные банковских карт клиентов Wendy's.

Мы в антивирусной лаборатории Pandalabs обнаружили атаку, запускающую известную вредоносную программу (PunkeyPOS), которая заразила свыше 200 ресторанов в США.

На рисунке: изображение одного из ресторанов Wendy's.
Это не означает, что заражено именно данное учреждение.

Финансовые учреждения также востребованы

Какая кража может быть самой результативной? Конечно же, - это ограбление непосредственно самих банков, однако это намного сложнее, чем грабить другие учреждения. Хотя...

Было установлено, что *Центральный банк Бангладеш* подвергся атаке, в результате которой хакеры могли украсть свыше 1 миллиарда долларов США. К счастью, когда банк узнал об этом, он сумел заблокировать огромное число трансферов, хотя преступники смогли заполучить примерно 81 миллион долларов США.

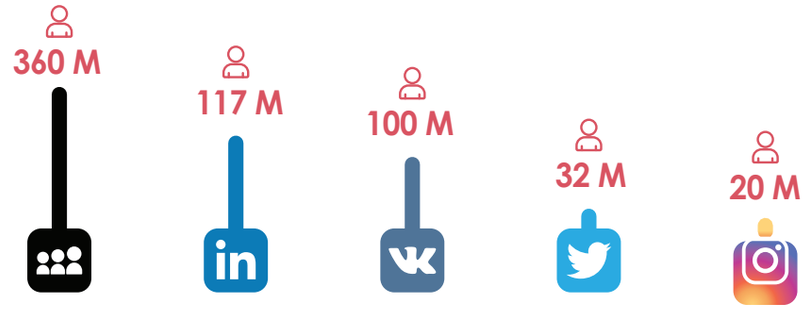
Впоследствии произошло еще два аналогичных случая: один случился с банком во Вьетнаме, а другой - в Эквадоре.

Даже если охота за кибер-преступниками является очень сложной и требует много времени, это все равно может дать свои результаты. В апреле в России был приговорен к 7 годам тюремного заключения *Дмитрий Федотов*, известный как “Paunch” ("Пузо") и автор набора эксплойтов Blackhold.

Александр Панин, 27-летний гражданин России был приговорен в США к 9,5 годам тюремного заключения. Панин стоял за хорошо известным банковским трояном SpyEye.

Социальные сети

Если говорить о соцсетях, то во втором квартале в них наблюдалось бесчисленное количество случаев кражи регистрационных данных, которые почти всегда попадают в чужие руки. Ниже представлены самые популярные соцсети:



Linkedin

Безопасность 117 миллионов пользователей LinkedIn оказалась под угрозой после того как был опубликован список адресов электронной почты и паролей. Хотя взлом произошел еще в 2012 году, полный список до сих пор еще не был опубликован.

Лучший способ защитить себя от таких типов атак - это использование двухфакторной авторизации. В этом случае, если даже Ваши регистрационные данные окажутся в чужих руках, все равно невозможно будет подключиться к Вашему аккаунту.

Twitter

32 миллиона имен пользователей и паролей для доступа в Twitter были выставлены на продажу за 10 биткоинов, или примерно 6 000 долларов США. Хотя данная соцсеть опровергла слухи о том, что эти данные были получены с их сервера. На самом деле, пароли были в виде обычного текста, а большинство из них принадлежало российским пользователям. Это может говорить о том, что они были похищены с помощью фишинговых атак или троянов.

VKontakte

"Русский Facebook" столкнулся с продажей данных **100 миллионов своих пользователей**, включая адреса электронной почты, имена, фактические адреса проживания, номера телефонов и пароли. В этом случае произошло то же самое, что и в случае с LinkedIn, когда на продажу были выставлены данные, украденные задолго до этого.

Instagram

Консультант по безопасности Арне Свиннен нашел ошибку безопасности в Instagram, которая позволила **взломать 20 миллионов их аккаунтов**. После сообщения этой информации, Facebook (владелец Instagram) заплатил ему 5000 долларов США в рамках своей бонусной программы. Причем, это не самая большая награда, которая была вручена в этом квартале: Facebook заплатил награду в 10 000 долларов США 10-летнему ребенку из Финляндии. Этот финский вундеркинд нашел ошибку безопасности, которая позволяла удаление комментариев в любом аккаунте Instagram.

MySpace

В наши дни он перестал быть сильно популярным, но он все еще уязвим для атак, от которых могут пострадать миллионы пользователей. Случай произошел в 2013 году, но о нем не было известно до мая этого года. В этой атаке хакеры украли имена пользователей, пароли, адреса почты. Утверждается, что **было скомпрометировано свыше 360 миллионов аккаунтов**. Возможно, Вы не подключались к MySpace уже несколько лет, но если Вы привыкли использовать одинаковые регистрационные данные для разных сайтов, то сейчас самое время изменить их и подключить двухфакторную авторизацию.

Если Вы не верите нам, то просто спросите об этом **Марка Цукерберга**, основателя Facebook. Цукерберг стал свидетелем того, как были взломаны его аккаунты в Twitter, Pinterest и Instagram группой шутников, которые называли себя OurMine. Видимо, пароль, используемый в LinkedIn, был одинаков для всех аккаунтов, что значительно упростило *OurMine* задачу получить доступ ко всем этим аккаунтам.

Следуйте двум важным советам: используйте двухфакторную авторизацию и не используйте одинаковые логин и пароль на различных веб-сайтах.

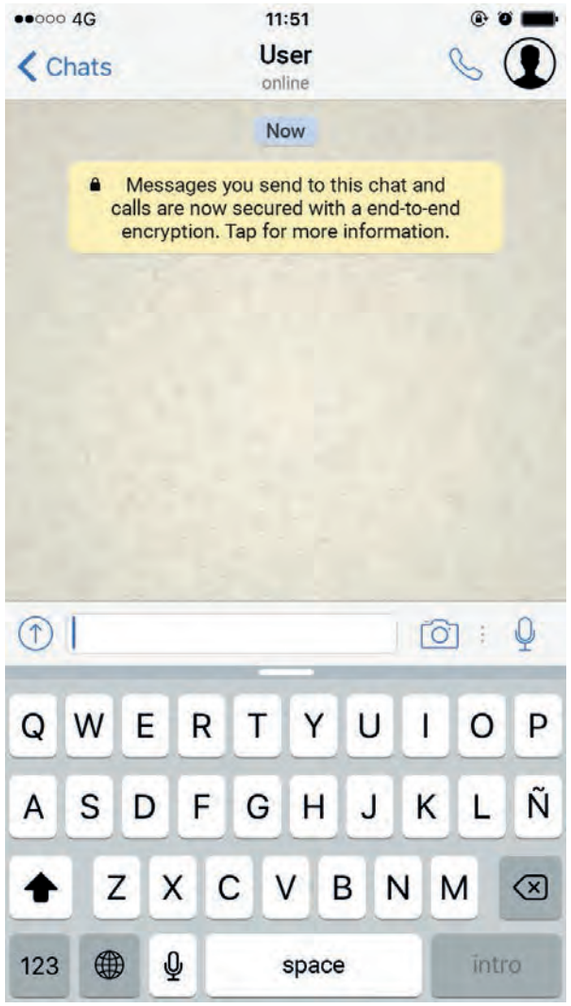
Кроме того, важно использовать сложные пароли. Исследование Kore Logic проанализировало 117 миллионов паролей и продемонстрировало, что большинство пользователей выбирают слишком простые пароли. Ниже в таблице приведены 10 наиболее часто используемых паролей:

Кол-во пользователей	Пароль
1 135 936	123456
207 488	linkedin
188 380	password
149 916	123456789
95 854	12345678
85 515	111111
75 780	1234567
51 969	654321
51 870	qwerty
51 535	sunshine

В этой связи мы должны аплодировать инициативе *Microsoft* по запрету часто используемых паролей, которые можно найти в приведенной выше таблице. Мы надеемся, что и другие последуют их примеру.

Звезды в *Whatsapp* - еще один пример хорошей практики в сфере информационной безопасности. Самое популярное приложение для обмена мгновенными сообщениями и его владелец, Facebook, решили повысить конфиденциальность пользователей за счет шифрования всех сообщений, пересылаемых через данное приложение.

Аналогичные действия в ближайшие несколько месяцев будут реализованы и в Facebook Messenger.



Мобильные угрозы

Кажется, Google решил серьезно закрыть все дыры безопасности в своих операционных системах. С помощью ежемесячных обновлений для устранения всех новых обнаруженных уязвимостей, они смогли только в мае исправить 25 уязвимостей (некоторые из них были настолько серьезными, что позволяли удаленное выполнение кода). Хотя вроде бы ни одна из этих уязвимостей ни была использована хакерами, но это было самое крупное обновление Google… на сегодняшний день.

Несмотря на улучшения, экосистема Android все еще "дрожит" из-за вопросов безопасности.

Бесспорно, одна из самых больших проблем Android - это их медленные обновления, которые в значительной части зависят от каждого производителя различных устройств с Android. В то время как продукты, которые контролируются непосредственно со стороны Google, получают такие обновления почти мгновенно (например, мобильные телефоны и планшеты Nexus), другие пользователи Android вынуждены ждать месяцами для получения патчей. А в некоторых случаях патчи так и не доходят до пользователей.

Отсутствие обновлений делает устройства больше уязвимыми перед известными проблемами безопасности, а т.к. число атак постоянно растет, **то это делает экосистему Android реально опасной**.

Интернет вещей

В последнее время в этом разделе отчета почти всегда были новости о взломанных машинах, так что сегодня поговорим про Mitsubishi Outlander. Этот гибрид имеет собственную сеть Wi-Fi, которая подключается к приложению, в котором Вы можете управлять температурой и другими параметрами.

Специалист по безопасности *Кен Мунро* вычислил пароль к сети Wi-Fi с помощью атаки типа "brute force". Проникнув в сеть, Мунро смог бы навредить автомобилю (например, полностью израсходовав батарею электрического мотора). Но самое серьезное заключается в том, что он мог бы удаленно деактивировать сигнализацию, чем могли бы воспользоваться реальные преступники.

Консалтинговая компания Gartner опубликовала интересный отчет о безопасности Интернета вещей. В этом документе прогнозируется, что **к 2020 году IoT-устройства будут вовлечены в 25% атак на предприятия**. Ожидается, что в 2016 году 6,4 миллиарда таких устройств будет подключено к Сети (на 30% больше, чем в 2015 году), а в 2018 году прогнозируется, что количество таких устройств превысит 11,4 миллиарда.

Расходы на безопасность Интернета вещей будут постоянно расти, хотя принимая во внимание прогнозы, представленные в таблице ниже, их, скорее всего, будет недостаточно:

Прогноз расходов на IoT-безопасность в мире
(миллионов долларов США)

2014	2015	2016	2017	2018
231,86	281,54	348,32	433,5	547,20

Источник: Gartner (апрель, 2016)

Кибер-войны

В прошлом году мы писали о том, как компания *Hacking Team* была полностью скомпрометирована. Она хорошо известна в мире тем, что продает хакерское ПО (вредоносное ПО) для правительств и спецслужб многих стран мира. Они попали в заголовки новостей после того, как итальянская газета "Il Fatto Quotidiano" сообщила о том, что "Hacking Team" лишилась своей экспортной лицензии, в результате чего она не сможет продавать свои программы за пределы Евросоюза, по крайней мере, без необходимости прохождения длительных бюрократических процедур.

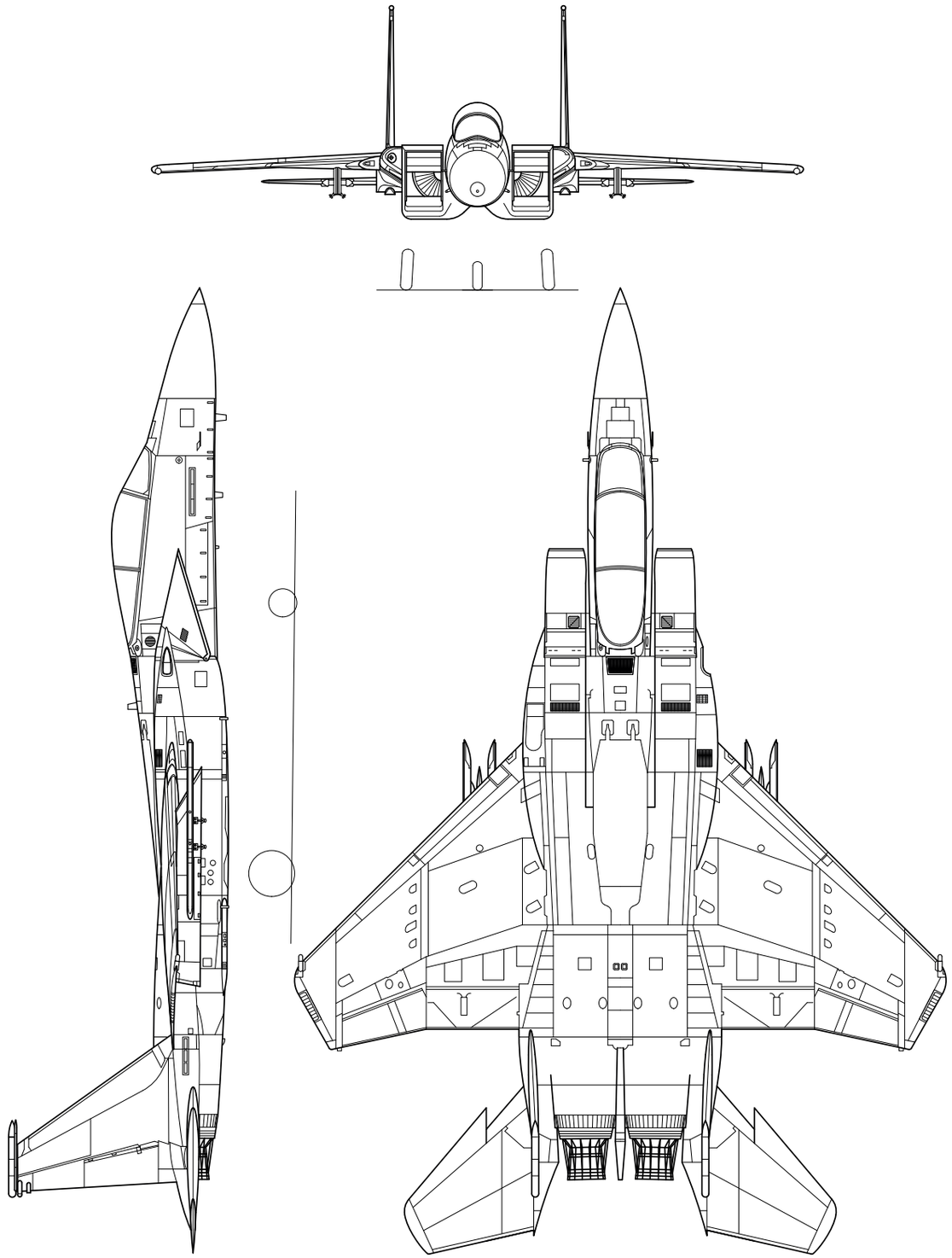
Когда мы обсуждаем кибер-войны, то в большинстве случаев мы говорим об атаках, которые, возможно, спонсируются различными странами, хотя очень сложно найти факты, доказывающие ответственность определенных должностных лиц за организацию и проведение таких атак.

Впрочем, США перешли к наступлению, признав, что они запускают кибер-атаки против ДАИШ (также известно как ИГИЛ). Заместитель министра обороны США Роберт Уорк сказал:

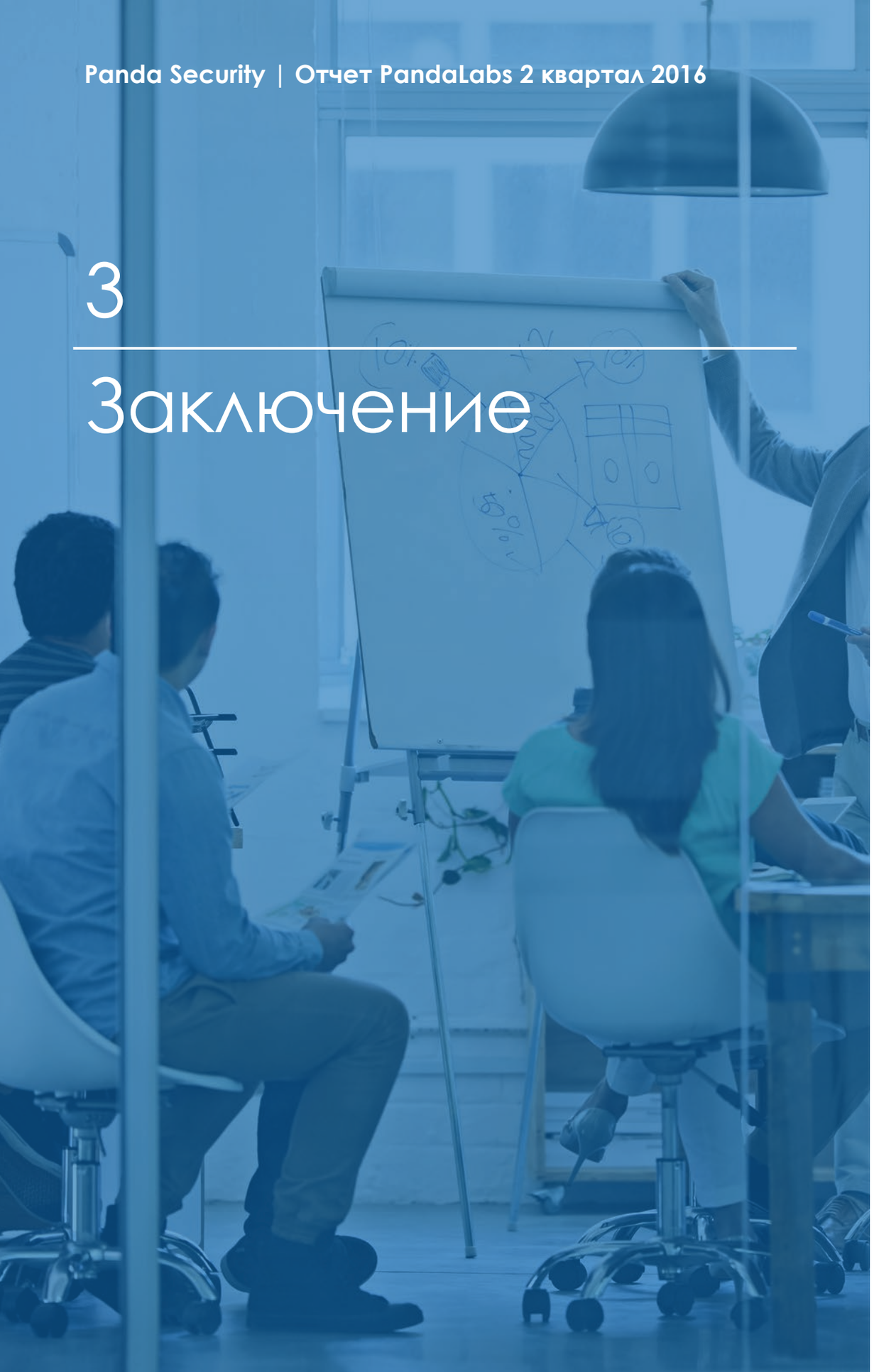
> "*Мы сбрасываем кибер-бомбы. Мы никогда не делали этого раньше. Подобно тому, что мы проводим военно-воздушную кампанию, я хочу иметь и кибер-кампанию. Я хочу использовать все возможности, которые у меня есть*".

В июне Департамент полиции Южной Кореи сообщил об атаке со стороны Северной Кореи. Видимо, атака началась примерно год назад, и она была ориентирована на 140 000 компьютеров, принадлежащих организациям и государственным учреждениям, а также подрядчикам Министерства обороны. Данная атака была обнаружена только в феврале этого года. По данным полиции, **было украдено свыше 42 000 документов, из которых 95% были связаны с вопросами обороны страны**, например, схемы и спецификации крыльев американского военного самолета F15.

Национальный комитет Демократической партии США признался, что их системы были взломаны примерно год назад (возможно, и больше). Они уверены, что хакеры принадлежали к российским спецслужбам. Нападавшие получили доступ к электронным письмам, чатам и всем видам исследовательских работ. **Все компьютеры, принадлежащие исследовательскому департаменту, были доступны хакерам, а некоторые файлы были украдены**.



3. ЗАКЛЮЧЕНИЕ



3 Заключение

Продолжает расти количество атак, используемых для кражи информации и денег. Пользователи сталкиваются с кражей их регистрационных данных или аккаунтов, причем во многих случаях они не были атакованы напрямую. Вместо этого их информация была обнаружена в базах данных, которые были украдены из взломанных сетей различных компаний.

Кроме этого, некоторые пользователи повторно используют свои пароли на других сервисах, что облегчает кражу, при этом данная проблема достаточно просто решается за счет двухфакторной авторизации, доступной у большинства сайтов. Другая возможность связана с тем, что сервис-провайдеры заставляют своих пользователей предпринимать определенные меры безопасности, что в наши дни уже не кажется чем-то невероятным, т.к. удобство не имеет приоритета над безопасностью.

Атаки шифровальщиков стали достаточно сложными. Хакеры зарабатывают огромные прибыли. В ближайшие месяцы мы увидим рост подобных атак.

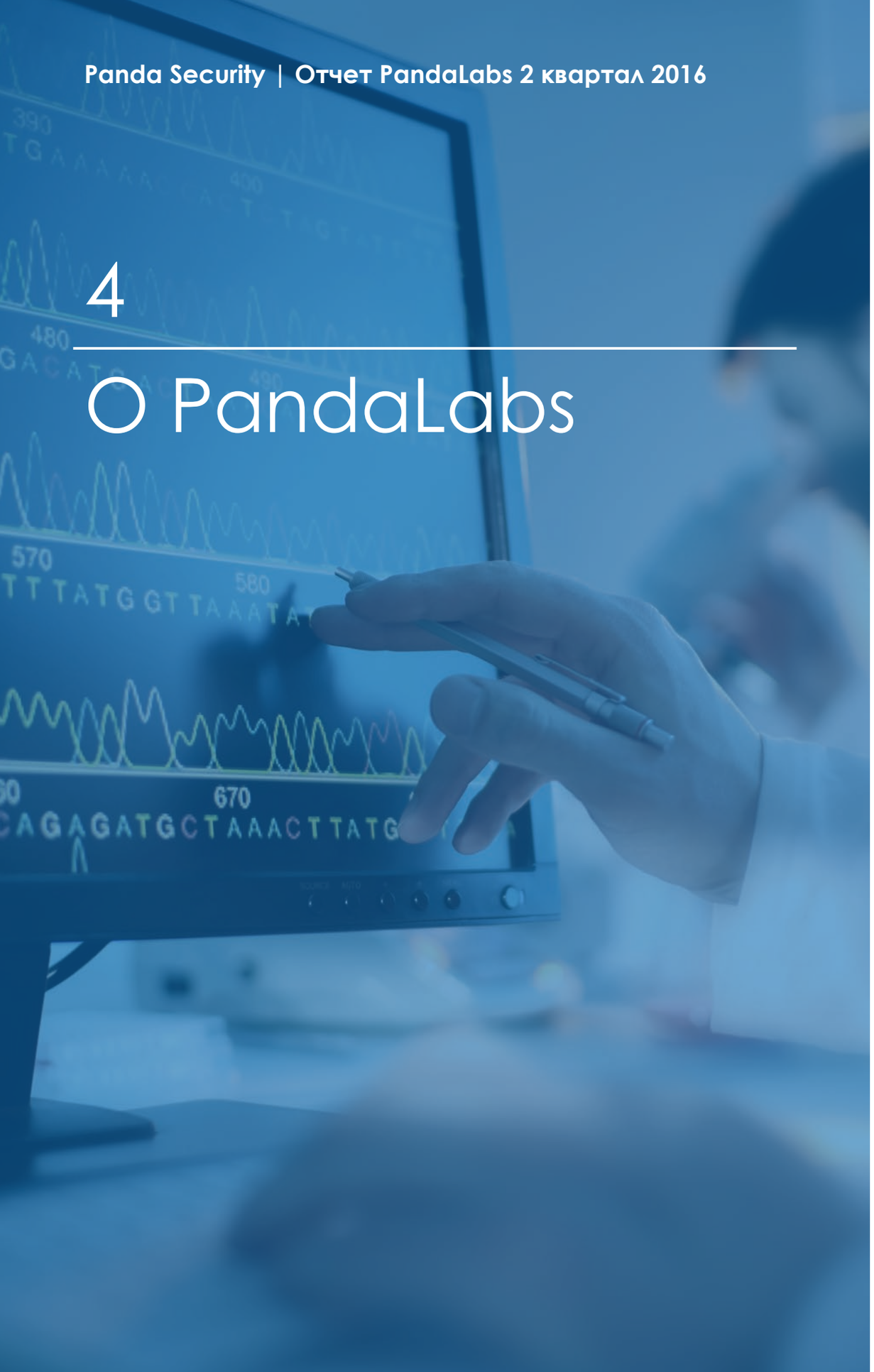
Еще одна тревожная тенденция - это кража данных с банковских карт через PoS-системы, где большинство пострадавших учреждений - это малые предприятия (рестораны, бары и пр.), у которых, что вполне очевидно, нет выделенной команды специалистов по IT-безопасности. Учитывая то, насколько легко продавать эту украденную информацию на "черном рынке" и получать прибыль, складывается впечатление, что кибер-преступники будут развивать данное направление атак.

Мы будем ждать Вас через три месяца, чтобы проанализировать и обсудить 3 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.

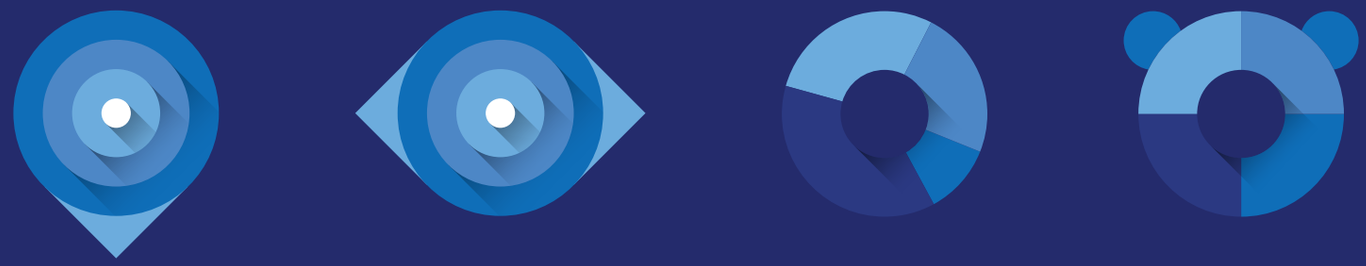
Кроме того, PandaLabs постоянно находится в состоянии повышенной бдительности, внимательно отслеживая различные тенденции и события, происходящие в области вредоносных программ и безопасности.

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

pandalabs

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