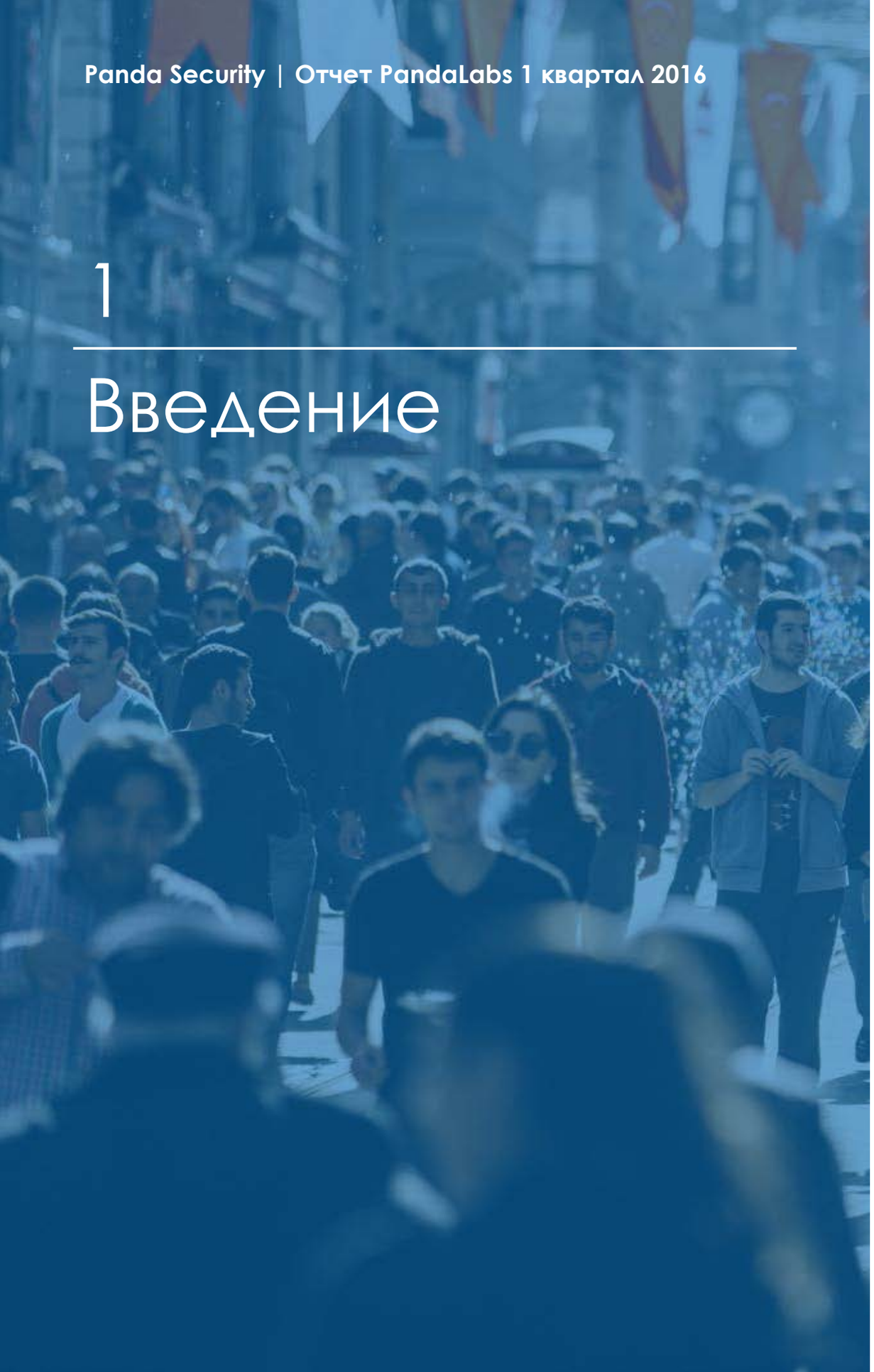
ОТЧЕТ PANDALABS
1 квартал 2016

panda

pandalabs

1. ВВЕДЕНИЕ



1 Введение

2016 год уже изобилует новостями в мире безопасности. Уровень создания вредоносных программ продолжает бить все рекорды, достигнув отметки в 20 миллионов новых образцов, которые были идентифицированы в PandaLabs на протяжении первого квартала (в среднем - 227 000 образцов ежедневно).

Все больше и больше компаний попадают в ловушки шифровальщиков. В настоящем отчете мы покажем Вам все новости, связанные с этими типами атак (включая атаки на Linux, Mac и даже веб-страницы). Мы увидим, как можно спасти несколько сотен миллионов евро, а также проанализируем кибер-атаки на больницы, которые произошли за последние несколько месяцев.

Критические инфраструктуры - это очень чувствительные зоны, на которые сосредотачивают свое внимание кибер-преступники. Одна из крупнейших атак недавно произошла на Украине. Зимой хакеры на несколько часов смогли удаленно отключить электроснабжение примерно 200 000 человек.

Атаки продолжают расти и в другом направлении: смартфоны. Кроме этого, благодаря Интернету вещей мы узнали, как можно атаковать такие, казалось бы, необычные с точки зрения атак объекты, как дверной звонок.

2.КВАРТАЛ В ЦИФРАХ

2

Квартал в цифрах

Мы начали этот год с более чем 20 миллионов новых образцов вредоносных программ, которые были обнаружены и нейтрализованы в PandaLabs - антивирусной лаборатории компании Panda Security (в среднем - 227 000 образцов ежедневно). Это чуть больше, чем было обнаружено в первом квартале 2015, когда ежедневно обнаруживалось примерно 225 000 образцов.

Из всех образцов трояны являются самым разрушительным типом вредоносных программ, оставаясь "лидером" на протяжении многих последних лет.

Обратите внимание, что число атак с помощью шифровальщиков, которые также относятся к данной категории троянов, существенно возросло.

Данные ниже показывают распределение вредоносных программ, созданных в первом квартале 2016 года, по типу угроз:

НОВЫЕ ОБРАЗЦЫ ПО ТИПУ УГРОЗ В ПЕРВОМ КВАРТАЛЕ 2016

Трояны являются самым популярным типом вредоносных программ, на долю которых приходится 66,81% от всех созданных в первом квартале образцов, что выше показателя предыдущего года. На втором месте идут вирусы (15,98%), далее - черви (11,01%), потенциально нежелательные программы (4,22%), шпионы и рекламное ПО (1,98%).

Благодаря данным, предоставленным "Коллективным разумом", мы можем проанализировать инфекции, вызванные вредоносными программами во всем мире. Мы можем видеть, что большинство инфекций также вызваны троянами (65,89%). Давайте посмотрим, как инфекции распределены по типу угроз:

ИНФЕКЦИИ ПО ТИПУ УГРОЗ В ПЕРВОМ КВАРТАЛЕ 2016

Принимая во внимание рост инфекций с помощью шифровальщиков, трояны вновь занимают первое место. Они остаются самым популярным инструментом проведения кибер-преступных атак, т.к. позволяют хакерам зарабатывать деньги одновременно простым и безопасным способом. Потенциально нежелательные программы заняли второе место с четвертью инфекций, оставив далеко позади шпионы и рекламное ПО (4,01%), черви (3,03%) и вирусы (1,95%). Агрессивные техники, используемые для распространения вредоносных программ, подразумевают использование вполне легитимных программ потенциально нежелательными программами. Такой подход позволяет добиться высоких показателей установки на компьютерах пользователей.

Если мы посмотрим на общую долю зараженных компьютеров в 33,32%, то она несколько выше, чем в прошлом году, за счет роста числа атак с применением шифровальщиков и ПНП. Следует отметить, что данный процент показывает лишь случаи "встречи" с вредоносными программами, но это не значит, что компьютеры в итоге были заражены. Лидером среди самых зараженных стран мира остается Китай (51,35% компьютеров), далее идут Турция (48,02%) и Тайвань (41,24%).

10 стран с наибольшим уровнем заражения:

СТРАНЫ С НАИБОЛЬШИМИ УРОВНЯМИ ЗАРАЖЕНИЯ

Китай	51,35%
Турция	48,02%
Тайвань	41,24%
Эквадор	39,59%
Гватемала	38,01%
Россия	37,98%
Мексика	36,32%
Перу	36,02%
Польша	35,55%
Бразилия	34,00%

Азия и Латинская Америка - это регионы с самыми высокими уровнями инфекций. Другие страны с уровнем заражения выше среднемирового: Уругвай (33,98%), Чили (33,88%), Колумбия (33,54%) и Испания (33,05%).

Анализируя менее зараженные страны, мы можем увидеть, что практически все они расположены в Европе. Как всегда скандинавские страны заняли весь "пьедестал": Швеция - лидер с показателем 19,80%, а рядом Норвегия (20,23%) и Финляндия (20,45%).

10 стран с наименьшим уровнем заражения:

СТРАНЫ С НАИМЕНЬШИМИ УРОВНЯМИ ЗАРАЖЕНИЯ

Нидерланды	26,15%
Дания	25,43%
Япония	24,99%
Германия	23,64%
Великобритания	23,61%
Бельгия	22,87%
Швейцария	21,43%
Финляндия	20,45%
Норвегия	20,33%
Швеция	19,80%

Другие страны, уровень заражения которых ниже среднемирового значения, но при этом они не попали в первую десятку: Австралия (26,79%), Франция (27,20%), Португалия (27,47%), Австрия (28,69%), Канада (30,30%), США (30,84%), Венгрия (31,32%), Италия (32,48%), Венесуэла (32,89%) и Коста-Рика (33,01%).

3. ВЗГЛЯД НА КВАРТАЛ

3

Взгляд на квартал

Изучая все, что произошло за последние несколько месяцев, мы решили ввести новый подраздел, который будет посвящен только шифровальщикам. Да, мы уже рассматривали эти атаки в наших отчетах, но т.к. их распространенность продолжает расти (особенно в корпоративном секторе), мы решили выделить их отдельно.

Шифровальщики

Мы можем предполагать прибыльность подобных атак по тому, как они атакуют различные платформы: помимо обычных атак на Windows, мы также видели новые и улучшенные варианты Linux/Encoder, использующие операционную систему с "пингвином". Не пожалели даже Apple: мы видели шифровальщик под названием KeRanger, который заражал пользователей Apple.

Впрочем, эти атаки шифруют не только файлы пользователей на компьютерах, но они также начали атаковать и веб-сайты, шифруя их содержимое.

В частности, мы наблюдали случаи, когда хакеры проникали на сайты, созданные с помощью Wordpress, шифровали файлы и меняли страницы index.php или index.html, показывая сообщение, в котором говорилось о необходимости выплаты выкупа за восстановление сайта. Они также включали чат для контакта непосредственно с хакерами для "оформления" платежа.

Совершенствуются техники, а в некоторых случаях они становятся слишком агрессивными (как в случае с Petya), когда вместо зашифрованных документов угрозы проникают непосредственно в MBR компьютера, оставляя его непригодным для использования до оплаты выкупа.

Также возросло злоупотребление системой PowerShell (как мы прогнозировали в ежегодном отчете PandaLabs за 2015 год), установленной по умолчанию в Windows 10, которая все чаще используется при атаках, когда необходимо избежать обнаружения со стороны решений безопасности, установленных на ПК жертвы.

Атаки на компании становятся все более изощренными. В последнее время мы стали свидетелями атак, когда после взлома сервера компании предпринимаются действия и для заражения максимального числа ПК в корпоративной сети с помощью шифровальщиков (так можно получить больше денег).

За последние месяцы возрос уровень распространения шифровальщиков, и мы даже видели случаи атаки на "топовые" сайты (The New York Times, BBC, MSN, AOL и т.д.) для заражения посетителей.

Веб-сайты не взламываются: атаки совершаются с помощью показываемой на них рекламы, управляемой кибер-преступниками и обращающейся к серверу с определенным типом эксплойтов (Angler и т.д.), чтобы заражать пользователей, у которых обновлены не все приложения.

По результатам опроса, проведенного Cloud Security Alliance, некоторые компании готовы платить до миллиона долларов за восстановление своих данных. Хотя это может показаться преувеличением, но стоит иметь в виду, что некоторые атаки не только шифруют корпоративную информацию, но и копируют ее себе, в результате чего даже при наличии бэкапов компании вынуждены платить, чтобы предотвратить публикацию украденной информации.

В январе The Economic Times в Индии сообщил, что три крупных банка и одна фармацевтическая компания стали жертвами атаки шифровальщиков.

Атака началась со взлома IT-менеджеров из различных компаний, после чего заражались ПК и других сотрудников, а выкуп достигал 1 биткоина за каждый зараженный ПК. Итоговый выкуп достиг нескольких миллионов долларов.

Один из секторов бизнеса, который целенаправленно страдает от подобных атак, - это больницы. За последние месяцы мы видели многократный рост атак на них. Ниже мы укажем самые шокирующие случаи.

Голливудский пресвитарианский медицинский центр в Лос-Анджелесе (США) заявил о "чрезвычайном положении" и оставил своих сотрудников без доступа к почте, медицинским записям пациентов и другим системам. В итоге некоторые пациенты не получили лечение, а часть из них были отправлены в другие больницы.

Запрашиваемый выкуп составил 3,7 млн. долларов. Директор больницы договорился с хакерами и заплатил 17 000 долларов за восстановление взломанных файлов.

MedStar Health вынужден был отключить некоторые свои системы в больницах Балтимора (США) из-за подобной атаки.

Methodist Hospital в Хендерсоне (штат Кентукки, США) также стал жертвой. И в этом случае они заплатили 17 000 долларов (однако некоторые источники сообщили, что размер выкупа был намного выше данной суммы).

Prime Healthcare Management, Inc. также стал жертвой кибер-преступников. У них было атаковано две больницы (Chino Valley Medical Center и Desert Valley Hospital). Но в этом случае компания не платила выкупа.

Но пострадали не только больницы в США. В Европе мы наблюдали аналогичные случаи. Deutsche Welle сообщила, что несколько больниц Германии были атакованы шифровальщиками (например, Lukas Hospital в Нойсе и Klinikum Arnsberg в Северном Рейне-Вестфалии). Никто из них не платил выкуп.

Кибер-преступления

Neiman Marcus сообщил, что примерно 5200 аккаунтов его клиентов были взломаны хакерами. Видимо, компания не пострадала от кражи регистрационных данных, но хакеры использовали учетные записи, украденные из других компаний, чтобы проверить, какие из них будут работать в данном интернет-магазине. Это напоминает нам о важности двухэтапной авторизации.

Сеть отелей Rosen Hotel & Resort была жертвой атаки с сентября 2014 до февраля 2016. Она предупредила своих клиентов, что если в указанное время они использовали банковскую карту в любом из учреждений сети, то их данные могли быть украдены хакерами.

Чилийская группа хактивистов украла 304 189 записей из базы данных CONADI, правительственного учреждения по развитию коренных народов. Хакеры опубликовали базу данных вместе с сообщением, которое выявило слабость систем безопасности и потребовало отставки Президента Чили.

Американский сервис Verizon пал жертвой атаки. Были украдены данные, принадлежавшие 1,5 миллионам их клиентов. По словам Брайна Кребса, который обнаружил данный инцидент, кибер-преступники продали украденную информацию примерно за 100 000 долларов (они также продавали ее по частям за 10 000 долларов).

Новая уязвимость в OS X могла предоставить хакерам полный доступ. Уязвимость могла пропускать Защиту целостности системы (SIP), впервые представленную в “El Capitan”.

Когда мы говорим о фишинге, мы обычно думаем о типичных письмах, похожих на сообщения нашего банка и пытающихся обмануть нас для получения наших регистрационных данных. Однако есть и более сложные и амбициозные атаки, вроде той, от которой пострадала компания Mattel, производитель Барби и Hot Wheels.

Исполнительный директор получил сообщение от вновь назначенного генерального директора с просьбой перевести три миллиона долларов на счет в Китай. После проведения платежа (чему гендиректор был удивлен, т.к. он не отправлял заявку), Mattel связалась с властями США и своим банком, но было слишком поздно, т.к. деньги уже были переведены.

Однако им повезло, т.к. в Китае были официальные праздники, а потому было достаточно времени предупредить власти Китая. Они заморозили счет и Mattel сумел получить свои деньги назад.

Такой тип атаки стал очень популярным. Хакеры выдают себя за руководителя компании и запрашивают у "своих" сотрудников осуществления денежных переводов. Для обмана используется информация, публикуемая ими в социальных сетях, что делает его более правдоподобным.

Клиника 21st Century Oncology Holdings во Флориде (США), специализирующая на лечении рака, предупредила в марте 2,2 миллиона своих пациентов и сотрудников, что их персональные данные могли быть украдены.

Атака произошла в октябре 2015 года, однако ФБР просила не раскрывать эту информацию до тех пор, пока шло расследование. Хакеры смогли украсть персональные данные (ФИО, номер социальной страховки, диагноз, лечение, данные медицинского страхования, сведения о банковской карте и пр.).

Многие помнят известный "полицейский вирус", предшественника современных шифровальщиков, который выдавал себя за местные правоохранительные органы и требовал оплаты штрафа в 100 евро. Одна из таких кибер-банд была поймана испанской полицией, а в первом квартале ее члены были осуждены. Банда состояла из 12 человек. Лидер банды Александр Краснокутский приговорен к 6 годам, его заместитель Дмитро Ковальчук получил три года, братья Сергей и Иван Барковы получили по два года каждый. Остальные члены банды получили по 6 месяцев тюремного заключения.

Если Flash - это номер один среди плагинов браузеров для заражения новых жертв (больше дыр и больше атак), то Java идет рядом на втором месте. Но в этом плане у нас есть хорошие новости:

Компания Oracle, разработчик Java, объявила о закрытии продукта.

Новая и последняя версия плагина будет опубликована в сентябре этого года. Основные производители браузеров остановили поддержку этих плагинов из-за множества проблем (преимущественно связанных с безопасностью). Некоторые уже запланировали прекратить их использование.

ФБР удалось идентифицировать 1500 человек, торгующих детской порнографией.

В прошлом году они изъяли серверы Playpen - сайта из теневого Интернета, который был опубликован в августе 2014 года и позволял пользователям загружать и скачивать изображения по данной тематике. Этот сайт вырос до 225 000 зарегистрированных пользователей. В течение двух недель ФБР, среди прочего, пытался с помощью собственных серверов и инструментов установить IP-адрес посетителей сайта.

Если на нормальном сайте вполне просто установить IP-адрес посетителя, то в теневом Интернете такая задача намного сложнее. Фактически, посетители Playpen были

взломаны с помощью уязвимостей в некоторых браузерах для теневого Интернета. После того как Вы получали доступ к компьютеру, посетившим данный сайт, утилита собирала требуемую информацию (IP-адрес, MAC-адрес, версия операционной системы, имя пользователя и т.д.).

Говоря о взломах со стороны правоохранительных органов, в Германии Министерство внутренних дел разрешило использование троянов для доступа к компьютерам и смартфонам подозреваемых. Троян был разработан самими полицейскими и позволял им получить доступ к коммуникациям этих устройств.

Мобильные угрозы

Мы поговорим об уязвимостях в телефонах. Мы наблюдали уязвимости, которые влияют на эти устройства с разных сторон: ПО, установленное производителем, процессор устройства, операционная система...

SNAP - это название уязвимости для телефонов LG G3. проблема возникает из-за ошибки в уведомительном приложении Smart Notice LG, которое позволяет выполнять любой тип JavaScript.

Исследователи из BugSec, обнаружившие эту уязвимость, сообщили о ней в LG, которая быстро выпустила обновление для устранения инцидента.

Metaphor - это название уязвимости, присвоенное компанией NorthBit. Данная уязвимость позволяет взламывать терминалы Android всего за 10 секунд после

посещения веб-сайта, содержащего вредоносный медиа-файл.

Многие технари знают имя Snapdragon, который, возможно, является самым известным процессором Qualcomm, использующимся на более чем 1 миллиарде устройств (в основном, мобильных). Коллеги из Trend Micro обнаружили в этих процессорах две уязвимости, которые позволяют хакеру получить рутовский доступ к устройству. Google выпустил обновление, которое решает данную проблему.

Apple был главным героем за последние три месяца. Во-первых, было опубликовано открытое письмо руководителя компании Тима Кука по поводу конфиденциальности пользователей после того, как ФБР запросило компанию предоставить им секретный вход для доступа к устройствам iPhone в тех случаях, когда речь идет о национальной безопасности. Но на самом деле все началось с теракта в Сан-Бернардино, когда ФБР изъял iPhone, принадлежащий одному из террористов, и хотел получить доступ к сообщениям. Многие технологические компании поддержали письмо Кука

(Facebook, Google, Microsoft, Twitter, LinkedIn и другие.). В конечном итоге ФБР сумело взломать терминал с помощью сторонних специалистов.

Интернет вещей

Как мы уже видели в предыдущих отчетах, Интернет вещей имеет высокие шансы стать жертвой атак. Некоторые производители в курсе данной проблемы. General Motors внедрила новую программу вознаграждения для хакеров, кто сможет найти уязвимости в их машинах. Это вполне нормальная практика среди технологических компаний (Microsoft, Google, Facebook и другие уже несколько лет имеют подобные программы), но это что-то новенькое среди традиционных компаний, например, автопроизводителей. Это замечательно, что General Motors проявил подобную инициативу.

Японский автопроизводитель Nissan отключил приложение, которое позволяет владельцам электрокаров Nissan LEAF управлять системой отопления и кондиционирования воздуха.

Исследователь из Австралии обнаружил, что он может контролировать эти параметры в любом Nissan LEAF, просто используя VIN-номер.

Постепенно мы вводим новые "умные" устройства в наш дом. Компания Ring имеет дверной звонок с камерой, датчиком движения и встроенным Wi-Fi подключением. Pen Test Partners Company, изучая одно из таких устройств, обнаружила, что получив доступ к кнопке установки устройства, можно получить регистрационные данные той Wi-Fi сети, к которой оно подключено. Производитель оперативно отреагировал на это, выпустив новую прошивку, которая устраняет данную проблему.

Кибер-войны

Российские исследователи из Industrial Controls Systems Supervisory Control and Data Acquisition (ICS / SCADA) опубликовали список промышленного оборудования, которое поступает с одинаковыми паролями по умолчанию, чтобы заставить производителей внедрить более эффективный контроль безопасности. Список уже окрестили “SCADAPass”, и он содержит регистрационные данные по умолчанию более чем 100 продуктов от таких производителей как Allen-Bradley, Schneider Electric и Siemens.

Эти продукты в основном используются в критических инфраструктурах. В конце 2015 года на Украине была осуществлена кибер-атака на инфраструктуру электроснабжения. Примерно 225 000 жителей некоторых областей Украины остались без электричества (посередине зимы!) в результате этой кибер-атаки. Данная атака была связана с группой российских кибер-преступников, известной как “Sandworm”.

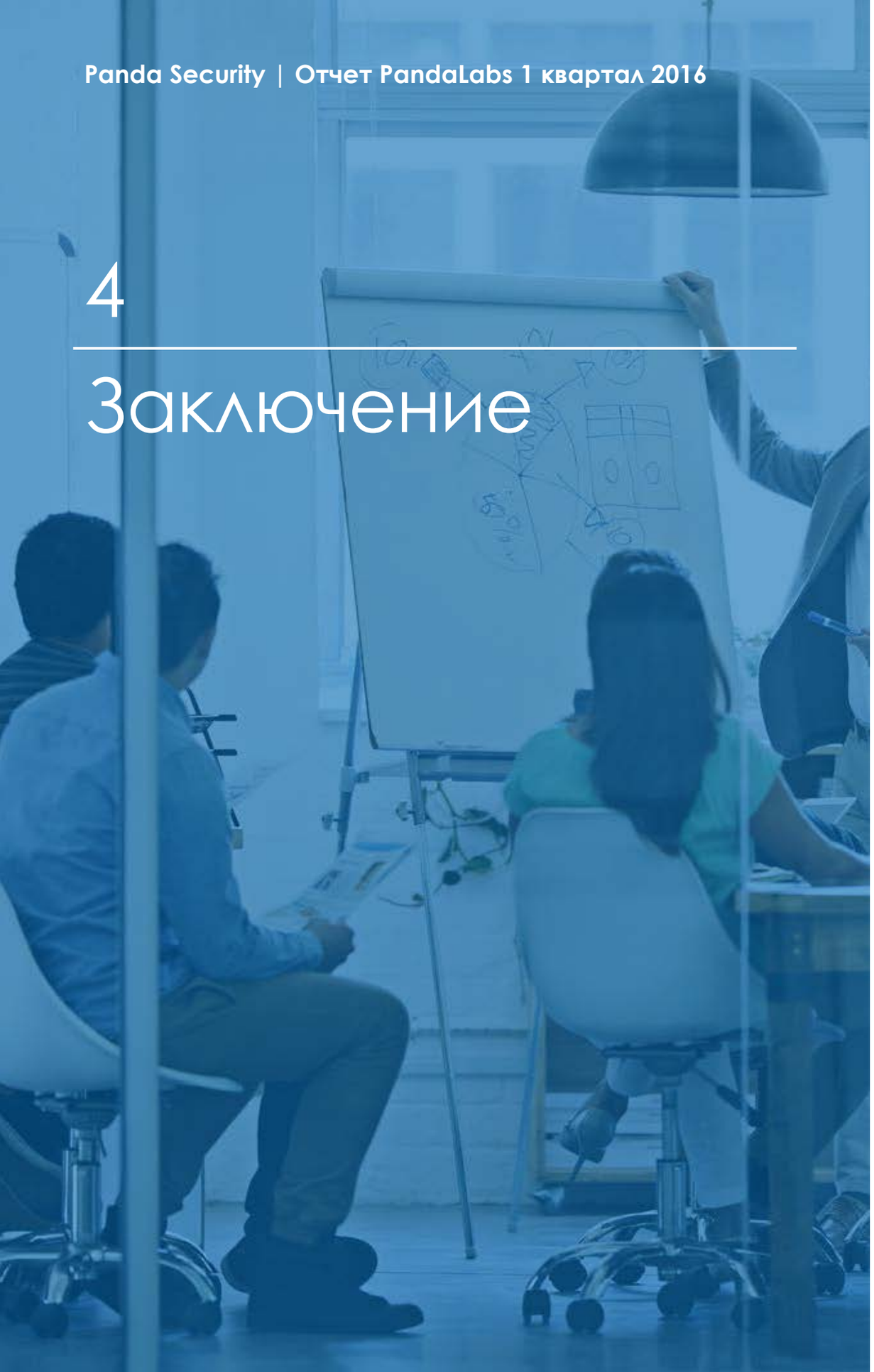
Министерство обороны США запустило специальную программу вознаграждения под названием "Взломай Пентагон". Хакерам предлагается вознаграждение за то, что они найдут уязвимости в веб-приложениях и сетях, связанных с Пентагоном.

Каждый может оказаться жертвой кражи информации, включая террористические группы, подобные ИГИЛ. Дезертир прихватил "флэшку" с данные о 22 000 членах ИГИЛ (перед вступлением в ИГИЛ кандидаты обязаны заполнить анкету со всей этой ниформацией).

Три группы латиноамериканских хакеров смогли взломать серверы, принадлежащие армии Боливии, после чего скачали и опубликовали электронные письма. Они сумели легко получить доступ к информации с помощью старой дыры безопасности в сервисе VMWare Zimbra, которая не была закрыта службами безопасности армии.

В марте разведывательная служба Южной Кореи призналась, что стала жертвой атаки, в которой были скомпрометированы мобильные телефоны 40 агентов безопасности в стране, обвинив в нападении Северную Корею. Спустя несколько дней правительство Северной Кореи сообщило о своей непричастности к этой атаке.

4. ЗАКЛЮЧЕНИЕ



4 Заключение

Как видите, год начался достаточно напряженно. Мы будем внимательно следить за развитием шифровальщиков, потому как нам придется жить с ними еще долгое время. Кроме этого, нам следует быть очень внимательными к Интернету вещей и многочисленным проблемам безопасности, окружающим данные устройства.

Мы надеемся, что настоящий отчет был для Вас полезным и интересным.
Мы продолжим информировать Вас о последних новостях IT-безопасности в будущих отчетах, а также 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

5. О PANDALABS

5

О PandaLabs

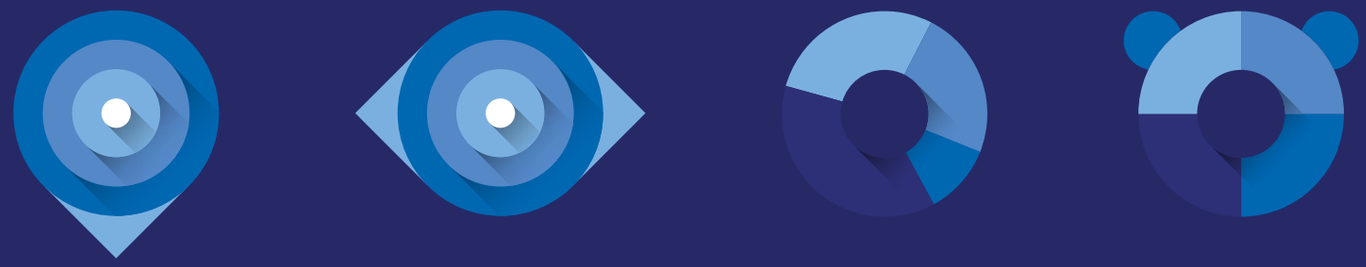
PandaLabs - это антивирусная лаборатория компании Panda Security, представляющая собой своего рода нервный центр компании по лечению вредоносных программ:

- PandaLabs непрерывно в режиме реального времени создает на глобальном уровне контрмеры, необходимые для защиты клиентов Panda Security от всех видов вредоносных программ.
- PandaLabs ответственна за выполнение тщательных сканирований с целью поиска всех видов вредоносных программ для повышения уровня защиты, предлагаемой клиентам Panda Security, а также за информирование 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