
ΟΤΥΧΕΤ PANDALABS 1 ΚΒΑΡΤΑΛ 2017



1. Введение

2. Анализ атак

3. Эволюция угроз

4. Взгляд на квартал

Шифровальщики
Кибер-преступления
Мобильные угрозы
Интернет вещей
Роботы и
персональные
помощники
Кибер-войны

5. Заключение

6. О PandaLabs

1. ВВЕДЕНИЕ

1

Введение

Интернет, почти по определению, - мать всех сетей, огромная машина децентрализованного хранения информации и обмена данными. Огромное разнообразие его возможностей выходит далеко за рамки любого явления, с которым мы уже знакомы. И все же, несмотря на свои многочисленные преимущества, Интернет в значительной степени не управляем, и он может стать источником неожиданных проблем для домашних пользователей, предприятий и организаций.

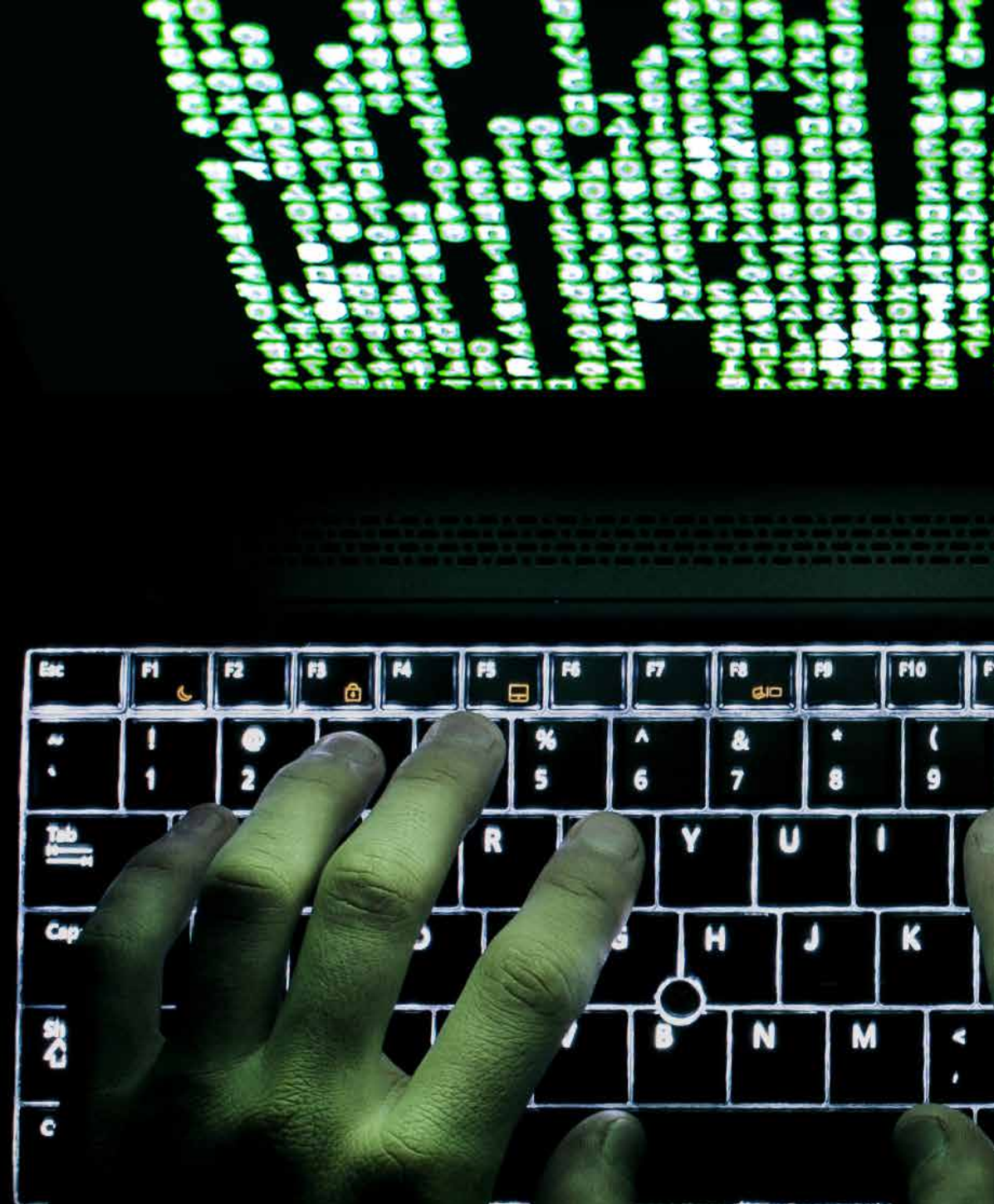
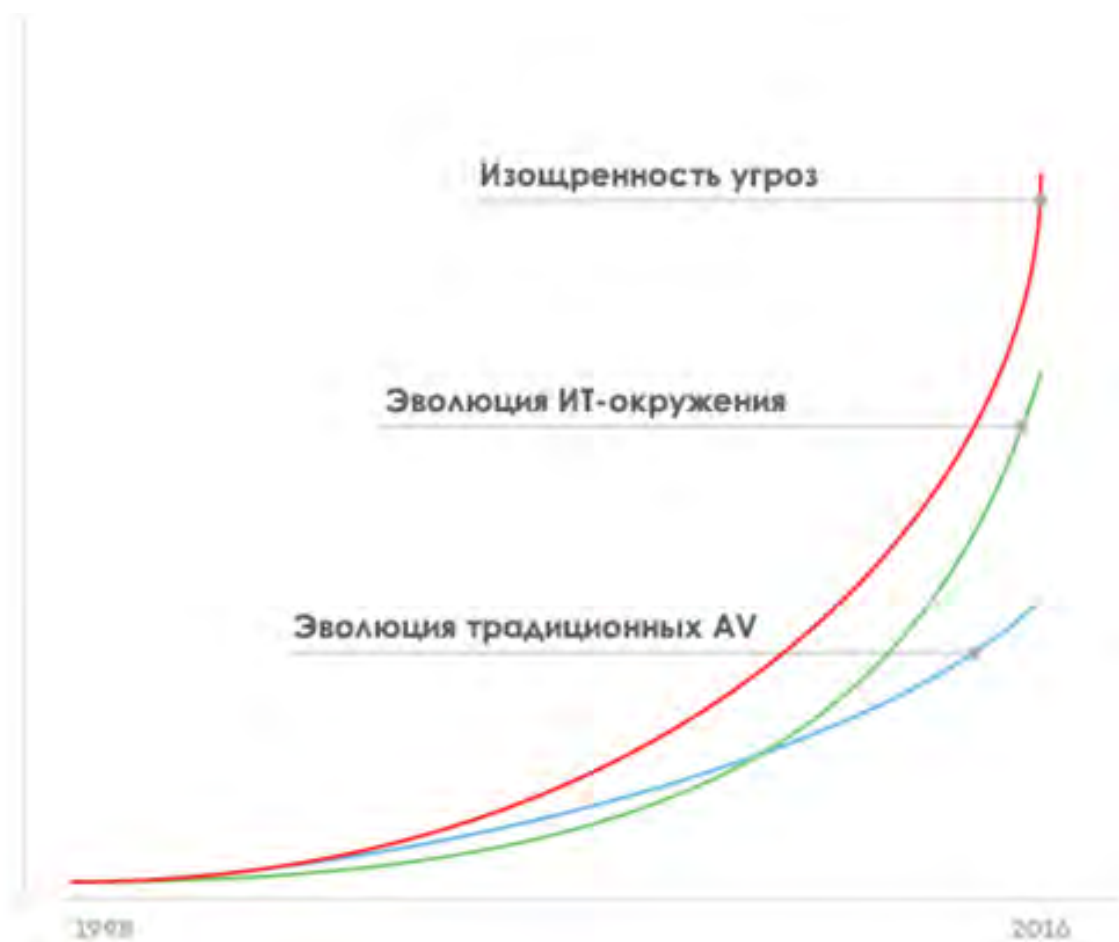
В первом квартале 2017 года мы наблюдали некоторые последствия той ситуации, когда мир все в большей степени зависит от Интернета, с помощью которого контролируются приборы и технологические процессы реального мира. Многие из них являются незащищенными.

Наблюдается заметное увеличение числа кибер-атак, происходящих ежедневно, при этом они становятся все более сложными, чем раньше. Из-за их постоянного развития теперь необходимо оставаться на шаг впереди угроз. Учитывая статистику, полученную за первые месяцы этого года, мы выделили три главных фактора успеха кибер-атак:

- Более изощренные угрозы, новые векторы атак, и большее количество атак.
- Более сложное IT-окружение с огромным количеством устройств, систем и подключений.
- Традиционные антивирусы развиваются по такому же пути, как и атаки, но не с такой скоростью.

Если бы нам пришлось выделить одну тенденцию, которая выделяется на фоне других, то стоит отметить атаки, которые становятся все более целенаправленными или "сделанными на заказ" в соответствии с выбранной жертвой. Теперь хакеры взаимодействуют с сетью жертвы и ее системами защиты в реальном времени, адаптируясь к ним для достижения поставленных целей.

В первые месяцы текущего года Интернет вещей (IoT) преподнес небольшой сюрприз, когда смарт-ТВ были атакованы шифровальщиком. Телевизоры LG под управлением Android стали первыми жертвами, показав, что "умные" телевизоры могут быть удаленно скомпрометированы с помощью DTT-сигналов.



2. АНАЛИЗ АТАК

2

Анализ атак

В наших отчетах, как и в отчетах других производителей решений безопасности, мы часто видим примерно одинаковую статистику угроз: количество новых угроз за определенный период времени, типы угроз и т.д. Хотя эти цифры интересны и могут стать ярким заголовком новостей, мы спросили себя в PandaLabs, что мы могли бы показать для оценки реальных рисков заражения, с которыми пользователи сталкиваются дома и на работе. Нам нужны данные, представляющие реальную ценность.

Для их получения мы сфокусировались на инцидентах, с которыми должны сталкиваться все пользователи. Во-первых, мы решили не считать угрозы, обнаруживаемые сигнатурами (их количество может достигать сотен миллионов), т.к. это известное вредоносное ПО, от которого в той или иной степени защищен каждый пользователь с базовым антивирусом. С другой стороны, мы также решили не включать эвристическое обнаружение, которое способно обнаруживать ранее неизвестные угрозы.

Это связано с тем, что профессиональные хакеры проводят минимальное тестирование антивирусов для проверки того, остаются ли незамеченными их "творения", а эти антивирусы включают сигнатурное и эвристическое обнаружение. Другими словами, мы можем отбросить эти цифры, словно пользователи всегда были защищены и никогда не было реального риска заражения. Но если мы не говорим о том, что мы обнаруживаем... тогда какие данные мы можем представить по данному вопросу?

Мы в Panda Security всегда были привержены защите клиентов, а потому несколько лет назад наша лаборатория создала новый уровень защиты, который мы решили добавить ко всем нашим продуктам. Он вступает в игру только тогда, когда другие уровни защиты не помогают.

Т.е. все, что останавливает этот уровень защиты, - это совершенно новые атаки.

С помощью этой системы мы не только считаем атаки, использующие вредоносное ПО, но и безфайловые атаки, а также и те, что злоупотребляют легитимными ПО и утилитами, что все чаще наблюдается в корпоративной среде.

Этот экстра-уровень позволяет нам постоянно показывать отличные уровни обнаружения в тестах, проведенных по методикам, имитирующим атаки в реальном мире. В тестах AV-Comparatives за первый квартал 2017 года мы показали 100% уровень обнаружения в двух тестах [Real-World Test](#), а в [Malware Protection Test](#) мы показали наилучший результат с 99,89% обнаружений и только 1 ложным срабатыванием, опередив всех наших конкурентов.

Из всех устройств, защищенных решением Panda, [2,25%](#) из них испытали атаки с абсолютно неизвестными угрозами.

Если посмотреть на тип клиентов, то среди домашних пользователей таких устройств [2,19%](#), а среди компаний - [2,45%](#). Хотя это может показаться нелогичным, ведь в компаниях гораздо более сложные системы защиты, чем на домашних ПК, но мы должны понимать, что компании сталкиваются с гораздо более профессиональными атаками. Компании обладают гораздо более ценной информацией, чем домашние ПК.

Среди наших корпоративных клиентов есть такие, кто используют традиционные решения, а есть и такие, кто уже выбрал наше EDR-решение (Adaptive Defense), которое выходит за рамки антивируса и предлагает дополнительные возможности, расширенные уровни защиты, мониторинг и

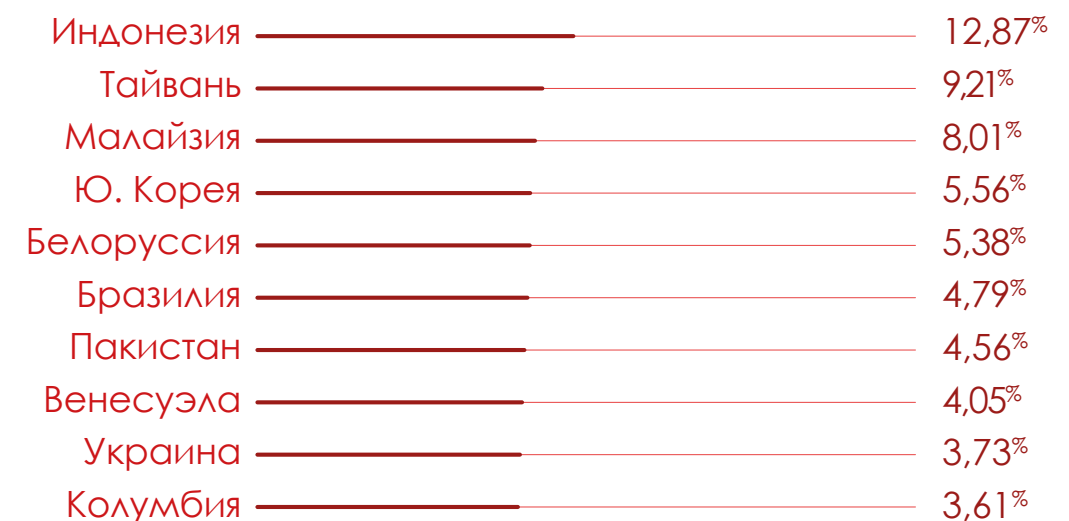
классификацию в реальном времени всех активных процессов на серверах и рабочих станциях в сети предприятия, экспертный анализ и пр.

Неудивительно, что количество атак, которые не удалось остановить всеми уровнями защиты в Adaptive Defense, намного меньше, чем у традиционных технологий. Кажется, логично, но так ли это на самом деле?

Итак, [2,83%](#) устройств, защищенных традиционными решениями, столкнулись с атаками неизвестных угроз. А среди устройств, защищенных нашим решением следующего поколения, таких устройств всего [0,83%](#).

Если говорить про географию подобных неизвестных атак, то мы посчитали процент атакованных устройств для каждой страны. Чем выше процент, тем выше вероятность быть атакованным с использованием неизвестных угроз в соответствующей стране:

СТРАНЫ С НАИБОЛЬШИМИ УРОВНЯМИ ЗАРАЖЕНИЯ



Азия и Латинская Америка - это регионы с самыми высокими уровнями инфекций.

Россия в этом "рейтинге" заняла 11-е место с показателем в 3,58%.

Ниже вы можете увидеть десятку стран с наименьшим уровнем заражения:

СТРАНЫ С НАИМЕНЬШИМИ УРОВНЯМИ ЗАРАЖЕНИЯ

Бельгия	1,04%
Словения	1,01%
Франция	0,98%
Греция	0,95%
Ирландия	0,85%
Швеция	0,85%
Нидерланды	0,66%
Дания	0,65%
Чехия	0,55%
Финляндия	0,34%

Другие страны, уровень заражения которых ниже среднемирового значения, но при этом они не попали в первую десятку: Канада (1,12%), Латвия (1,19%), Германия (1,20%), Испания (1,27%), Великобритания (1,29%), Австралия (1,30%) и Словакия (1,31%).



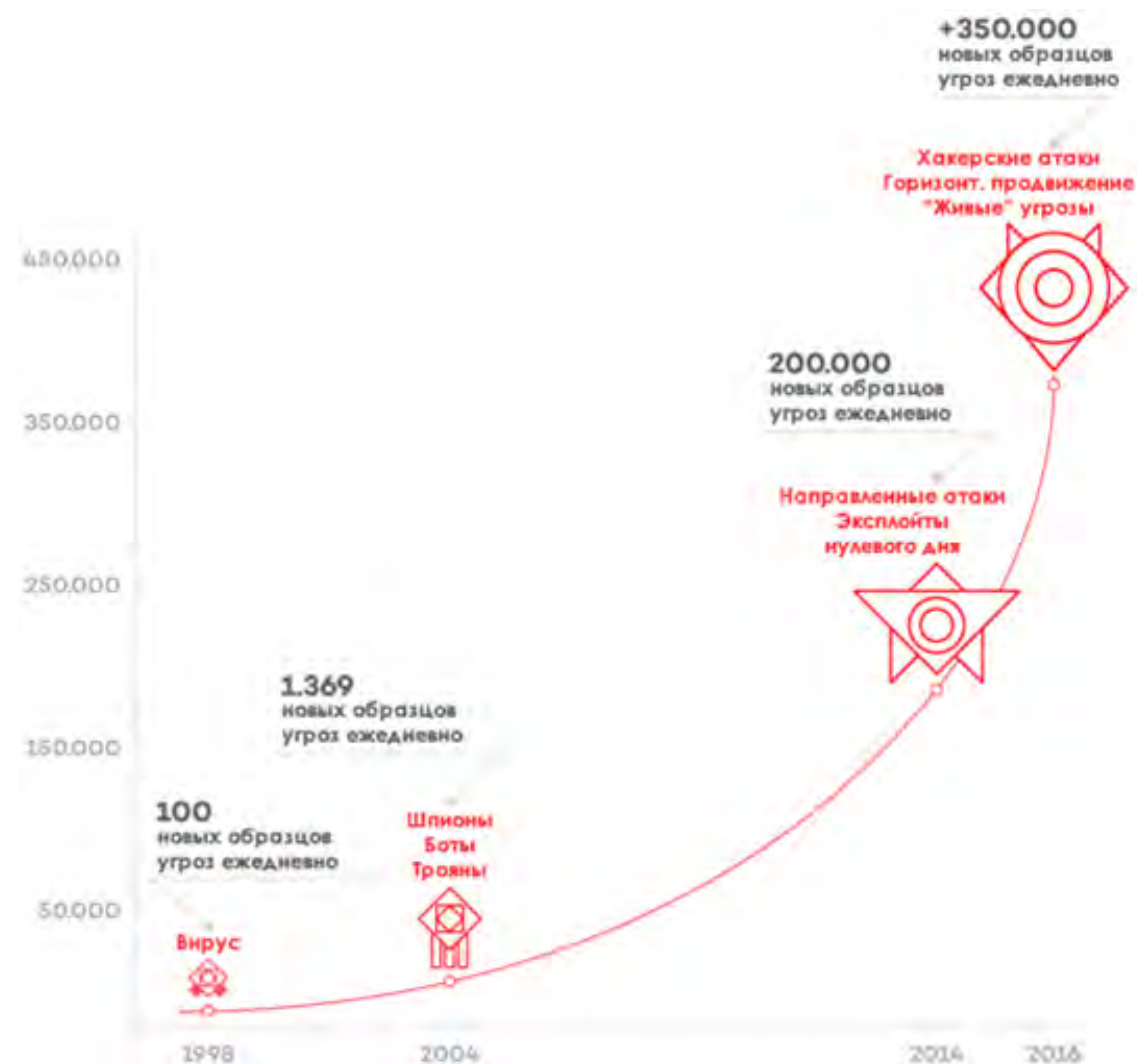
3. ЭВОЛЮЦИЯ УГРОЗ

3

ЭВОЛЮЦИЯ УГРОЗ

Мы живем во время революции кибер-угроз? Кажется, что так. Вредоносные программы становятся все более и более изощренными, а техники атак постоянно совершенствуются. Сейчас цель уже не выбирается случайно: атаки все чаще становятся направленными и скоординированными, использующими различные направления заражения.

И не надо забывать про мотив злоумышленников: они теперь не ищут славы, т.к. ими движут исключительно финансовые выгоды.



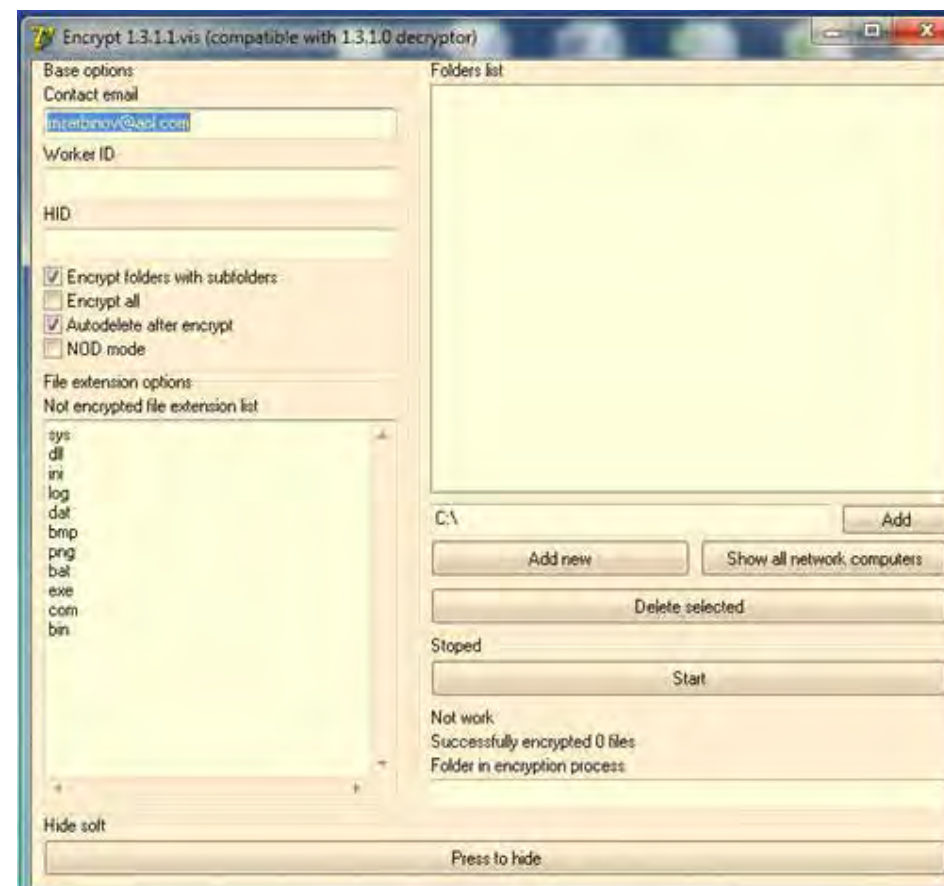
4. ВЗГЛЯД НА КВАРТАЛ

Шифровальщики

Атаки шифровальщиков все еще на подъеме, и эта тенденция сохранится до тех пор, пока жертвы платят выкуп. Существуют [оценки](#), что в 2016 году группы киберпреступников, которые специализируются на шифровальщиках, заработали 1 миллиард долларов США. Проблема актуальна во всем мире, а потому во многих странах совершенствуется законодательство для более эффективной борьбы с такими видами преступлений. Например, в Калифорнии считается [преступлением внедрение шифровальщиков](#).

Впрочем, новых законов недостаточно, чтобы сдерживать постоянные атаки и создание новых семейств шифровальщиков. Одно из таких семейств ([Spora](#)) начало распространяться в начале этого года, преимущественно в России.

Частота атак на компании продолжает расти. В дополнение к очень известным семействам шифровальщиков (Locky, Cerber, etc.), сейчас наблюдается более персонализированные виды атак, адаптированных под своих жертв. Одна из них была обнаружена лабораторией PandaLabs в 1 квартале: шифровальщик со своим собственным интерфейсом ([WYSIWYE](#)), который позволял злоумышленнику выбирать различные папки, чье содержимое будет зашифровано, и атакуемые компьютеры в сети, активировать функцию автоудаления, указывать адрес почты, куда следует обращаться жертве для оплаты выкупа и пр.:



Один из наиболее популярных и относительно простых методов проникновения в корпоративную сеть, - это атаки типа brute-force с использованием RDP-протокола (подключение к удаленному рабочему столу в Windows). Злоумышленники ищут в Интернете компьютеры, где активирована эта функция, а после нахождения потенциальной жертвы они запускают против нее атаку типа brute force до тех пор, пока не подберут учетные данные. Оказавшись внутри системы, они имеют полную свободу поступать так, как им заблагорассудится.

В 1 квартале 2017 года мы видели достаточно случаев атак русских хакеров. Все они имеют сходные закономерности: получив доступ к ПК через RDP, они устанавливали ПО для майнинга биткоинов с целью получения дополнительных доходов, а затем либо шифровали файлы, либо блокировали доступ к ПК. Причем они не всегда использовали вредоносное ПО: например, в [одном из проанализированных случаев](#) они использовали коммерческое приложение “Desktop Lock Express 2” для блокировки компьютера:



Мы также стали свидетелями особо коварного шифровальщика, известного как [Popcorn Time](#). Его новизна заключается в ужасном способе распространения, т.к. жертвы вынуждены сотрудничать с кибер-преступниками для заражения новых пользователей. Наряду с требованием выплаты 1 биткоина (примерно 800 евро) для восстановления доступа к зашифрованным файлам, он предлагает возможность бесплатного восстановления, если жертва

будет его распространять среди своих контактов.

Моментальные последствия атаки шифровальщиков очевидны: вы теряете доступ к своим файлам. Однако были случаи далеко за рамками этого, что подтвердили клиенты [отеля в Австрии](#). Кибер-преступники смогли удаленно заблокировать в отеле все ридеры электронных ключей, из-за чего постояльцы не могли попасть в свои номера. Это произошло со 180 клиентами в первую неделю сезона. Руководство отеля решило заплатить выкуп в 1500 евро, чтобы восстановить контроль над своими системами.

Кибер-преступления

Кибер-преступность становится все более профессиональной, а это означает, что для разных работ существуют высокоспециализированные группы: создание вредоносного ПО и эксплойтов, их распространение, кража информации, отмывание денег и пр. Наглядный пример тому - атака [RDPatcher](#), обнаруженная лабораторией PandaLabs. Ее цель - подготовить ПК жертвы для "сдачи в аренду" в теневом Интернете. После проникновения на ПК, хакеры приступали к созданию его полноценного профиля, собирая все типы данных о "железе", установленном ПО, решении безопасности, скорости соединения, посещенных сайтах и пр. Все это затем выкладывается на черном рынке для продажи и подключения к ботсети.

Кажется, изобретательности кибер-преступников нет конца. В одном случае, обнаруженным лабораторией PandaLabs, [мы видели, как хакеры избежали обнаружения, используя "goodware" для совершения своих атак](#). После входа в систему компьютера, они оставляли бэкдор с

помощью функции залипания клавиш, так что для входа в систему не требовалось устанавливать вредоносное ПО.

DDoS-атаки также заслуживают упоминания. Во второй половине 2016 года было несколько громких атак этого типа, а в этом квартале мы видели еще больше таких атак, хотя они не были столь жестокими по своей природе. В начале года, например, **клиенты Lloyds** имели проблемы с доступом к своим счетам в результате DDoS-атаки. В январе итальянская полиция разогнала группу кибер-шпионов под названием **Eye Pyramid**, созданную двумя родственниками для взлома госорганов, профессиональных студий, предпринимателей и политиков. Они получали доступ к конфиденциальной информации своих жертв, устанавливая вирус на их ПК, и осуществляли кражу финансовых данных и параметров национальных и муниципальных систем безопасности. Среди пострадавших оказались премьер-министры Италии Маттео Ренци и Марио Монти, президент Европейского Центробанка Марио Драги, а также руководители регионов, экономисты, бизнесмены и полицейские комиссары.

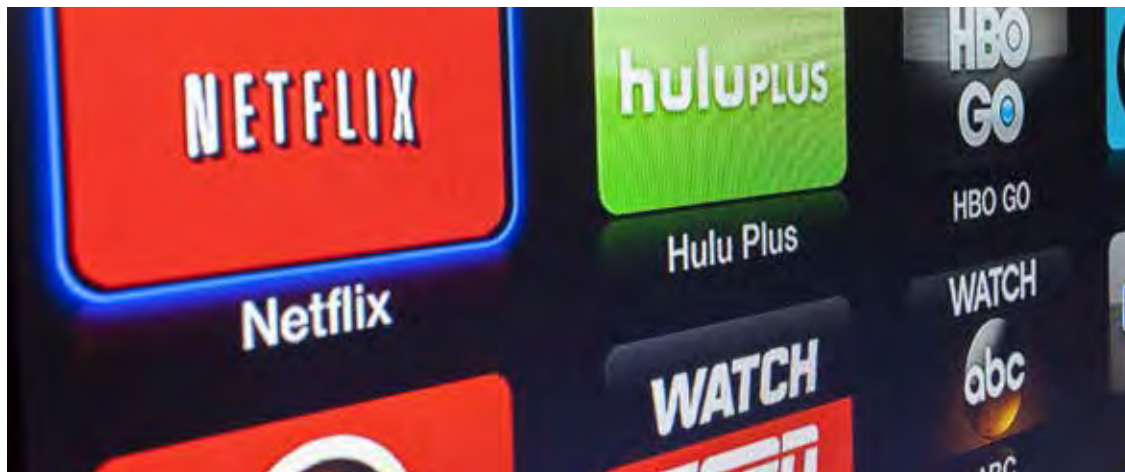
Взлом аккаунтов в соцсетях стал привычным явлением. Один из самых поразительных случаев в 1 квартале произошел в январе, когда был взломан официальный аккаунт New York Times в Twitter. Как только контроль был восстановлен, они удалили посты, размещенные хакерами:



Пример одного из твитов, который был опубликован на взломанном аккаунте. В нем утверждается, что Россия собирается начать атаку против США:



Эта группа хакеров известна тем, что взламывала аккаунты других компаний, например, Netflix и Marvel.



Кража данных также занимает особое место в последние месяцы. У компании Sangio, которой принадлежит "Hello Kitty", украли персональные данные 3,3 миллионов ее клиентов, включая такую информацию, как ФИО клиентов, дата рождения, вопросы безопасности для восстановления паролей и т.д.

Мы анализировали и некоторые ироничные случаи, как с израильской компанией Cellebrite, которая облегчала взлом телефонов (вернее, извлечение информации с них), но сама пострадала от взлома и кражи 900ГБ данных о клиентах, БД, а также технической информации о продуктах компании.

Даже Apple в начале этого года стал объектом кибератаки. Группа кибер-преступников под названием "Turkish Crime Family" шантажировала компанию, требуя выкуп и обещая в противном случае удаленно стереть данные с iPhone, iPad и Mac устройств 250 миллионов

пользователей. Эта группа заявляла, что она располагает действующими регистрационными данными пользователей, хотя Apple отрицал, что они были взломаны, предполагая, что эти данные могли быть получены со сторонних сайтов или в результате повторного использования паролей. Конечно, технологический гигант не стал поддаваться на попытку шантажа.



Мобильные устройства

Хотя количество новых вредоносных программ, созданных для мобильных устройств, все еще намного меньше, чем то, что создается для ПК, но тенденции примерно одинаковые. Например, шифровальщики - это техника, которая отлично переносится на мобильные устройства и гарантирует злоумышленникам отличные результаты. Новая угроза под Android, известная как "Charger", осуществляет кражу контактов и SMS-сообщений перед блокировкой терминала, угрожая продать часть вашей информации на "черном" рынке каждые 30 минут, если требуемый выкуп (0,2 биткоина) не будет заплачен.

Интернет вещей (IoT)

В течение некоторого периода времени многие здания были оснащены "умными" счетчиками для регистрации потребления электричества. Если не считать возможное влияние таких счетчиков на счет за электроэнергию (некоторые ассоциации потребителей уже сообщили о возможных махинациях с ними), то их широкое применение может повлечь за собой проявление других, менее известных рисков безопасности.

Как объяснил исследователь Нетанель Рубин на последнем Chaos Communications Congress в Гамбурге (Германия), смарт-счетчики представляют опасность по некоторым направлениям. Во-первых, поскольку все данные по потреблению электричества дома и в офисе записываются и отправляются в электрокомпанию, то хакер, контролирующий устройство, может просматривать информацию и использовать ее во вредоносных целях. Например, грабителю будет очень полезно знать, в какое время суток дом или офис пустой. Он также может удаленно узнать, какие устройства находятся в помещении, т.к. каждое электронное устройство оставляет свой уникальный "отпечаток" в электросети.

Другое распространенное устройство - это смарт-ТВ. На некоторых из них в качестве операционной системы стоит Android, который помимо преимуществ имеет и свои недостатки, что было показано американским программистом Дарреном Коутоном, когда он опубликовал в Twitter пост о том, что телевизор его семьи стал жертвой атаки. По словам Коутона, все случилось после того, как кто-то из его семьи установил (видимо, со стороннего сайта) приложение для просмотра фильмов в Интернете.

Его телевизор LG был произведен в 2014 году, работал под Google TV - специальной версией Android для смарт-телевизоров. После того как ТВ был заражен, вредоносное ПО потребовало 500 долларов США за код разблокировки экрана. Это требование было оформлено в виде уведомления от Министерства юстиции США.



Впрочем, есть гораздо более опасные атаки, которые показывают нам, что ждать в будущем. В феврале во время семинара по кибер-безопасности Европейского вещательного союза был показан [эксплойт](#), созданный консультантом по безопасности Рафаэлем Шилем, который позволил ему [получить контроль над смарт-ТВ без физического доступа к нему](#), отправив атаку через DTT-сигнал.

Роботы и персональные помощники

“Четвертая промышленная революция” уже на подходе. Недавний отчет Всемирного экономического форума привел некоторую статистику на сегодняшний день и прогноз на 2020 год. Так вот в развитых странах за это время закроется 7,1 миллиона рабочих мест, а создано будет

только 2,1 миллиона. Другими словами, будет потеряно 5 миллионов рабочих мест.

В другом недавнем отчете Организации экономического сотрудничества и развития (ОЭСР) Испания, Австрия и Германия были выделены как страны, которые окажут наибольшее влияние на революцию роботов. В частности, в этих странах 12% рабочих будет замещено роботами, причем в остальных странах-членах ОЭСР средний показатель замещения составит 9%.



На основе этих данных, Европарламент разработал набор правил для урегулирования взаимоотношений между роботами, гражданами и предприятиями. Предлагаемое законодательство сейчас обсуждается в Еврокомиссии, которая примет окончательное решение о границах внедрения роботов в общество. Цель - свести к минимуму возможные негативные последствия этого.

В феврале на всей территории США внезапно были активированы виртуальные помощники Google Home из-за того, что голос в рекламе Супербоула (финальная игра Национальной футбольной лиги США) сказал волшебные

слова "OK, Google." Т.е. получается, что возможности Google Home слушать разговоры людей, терпеливо дожидаясь голосовой команды, делают его идеальным устройством для подслушивания. Эти навыки виртуального помощника в сочетании с его возможностями хранения аудиофайлов, могут даже использоваться в расследовании преступлений. Например, полиция одного американского городка запросила у Amazon доступ к данным с Amazon Echo, т.к. он мог хранить полезную информацию для расследования преступления.

Кибер-войны

Сейчас более чем когда-либо ранее переплелись кибер-атаки и политика. В результате прошлогодних выборов в США мы наблюдаем огромное количество обвинений в адрес России. Перед тем как покинуть свой пост, Барак Обама обвинил россиян в проведении кибер-атак, которые нанесли ущерб предвыборной кампании Хиллари Клинтон в пользу Дональда Трампа. В результате этого из США были выдворены 35 российских дипломатов.

Вся эта история повлияла и на другие страны мира. Например, во Франции отказались от электронного голосования граждан, проживающих за рубежом, из-за очень высокого риска кибер-атак. В Нидерландах пошли еще дальше и объявили о том, что будут вручную подсчитывать бюллетени в ночь после выборов и сообщать результаты по телефону, чтобы избежать рисков возможных кибер-атак. Это заявление последовало после того, как эксперты по безопасности предупредили о возможных уязвимостях в ПО на избирательных участках.

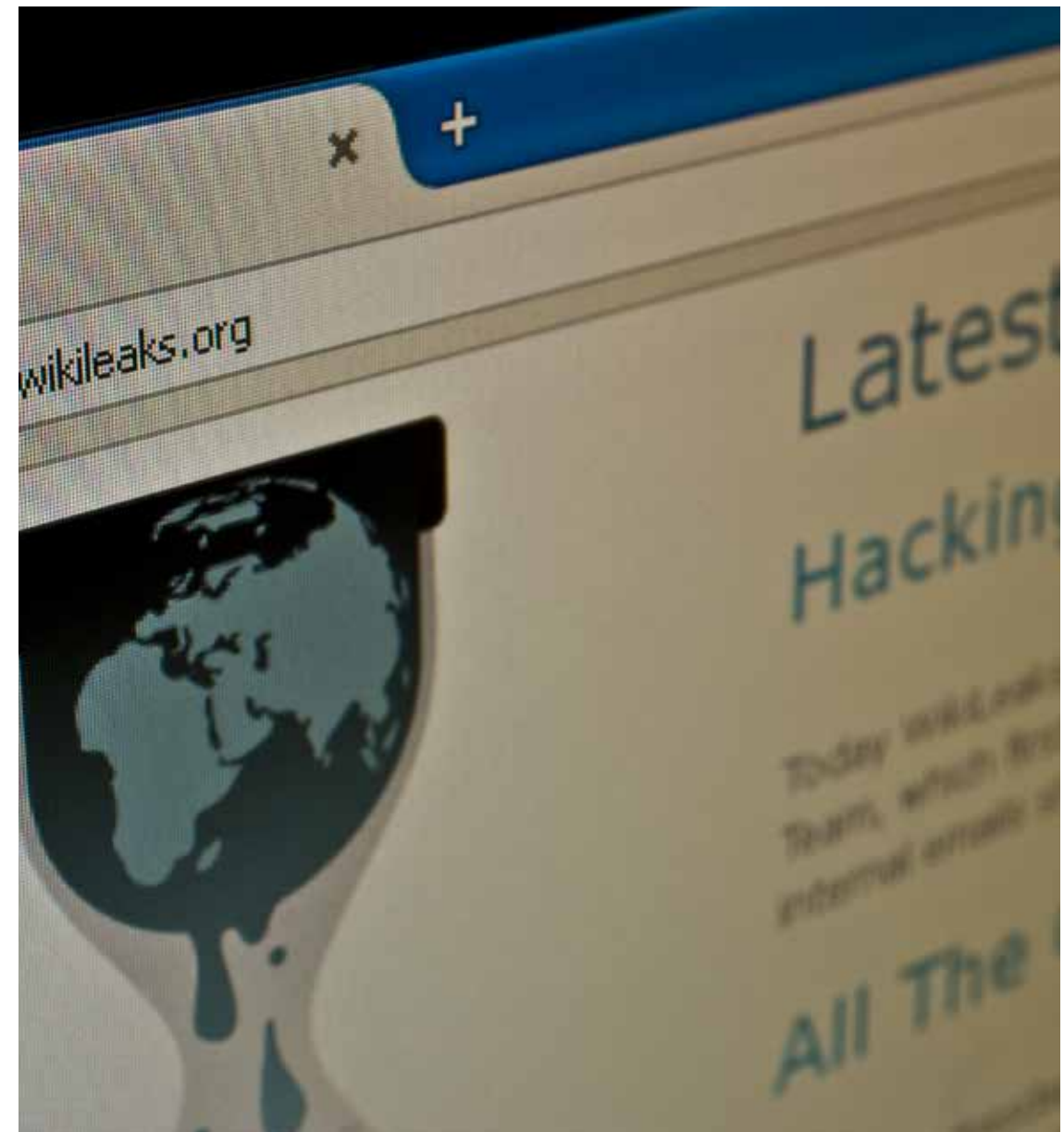
В феврале Нидерланды направили в НАТО предложение по созданию международного альянса по кибер-обороне для борьбы с растущими угрозами кибер-атак. Данный альянс должен будет иметь все возможности для обороны, правоохранительной деятельности и реагирования на атаки.

В марте канцлер Германии Ангела Меркель заявила, что защита инфраструктуры в Германии от кибер-атаки является одним из ее основных приоритетов в вопросах безопасности. Вскоре после этого стало известно, что немецкая армия сформировала собственный кибер-командный центр для усиления своей онлайн-обороны. Новый центр будет иметь 260 сотрудников, но теоретически это количество вырастет до 14500 к 2021 году.

Но если среди всех событий в мире кибер-войн и кибер-шпионажа следовало бы выделить одно, то им бы стал случай с ЦРУ/Wikileaks. 7 марта Wikileaks начала публикацию серии документов под названием "Vault 7", содержащих технические подробности и описания инструментария, используемого ЦРУ для взлома смартфонов, компьютеров и даже смарт-ТВ.

Wikileaks все еще продолжает публикацию документов на одном из [разделов своего веб-сайта](#). Поражает огромное количество инструментов и техник. Документы не оставляют сомнений в том, что ЦРУ имеет в своем распоряжении обширный арсенал кибер-средств для шпионажа, а потому может шпионить практически за любым человеком. Также верно и то, что сейчас ЦРУ потеряло полный контроль над указанными средствами. Хорошая новость заключается в том, что эти знания могут

быть использованы для усиления своей собственной защиты от подобного рода атак. Плохие новости: любой другой злоумышленник может воспользоваться опубликованной информацией в своих собственных вредоносных целях, изучив тактики, разработанные в ЦРУ, для нарушения конфиденциальности личной жизни обычных граждан.



4. ЗАКЛЮЧЕНИЕ

4

Заключение

Wikileaks продолжит публикацию информации о Vault 7, и мы сможем проанализировать новые "находки" в наших следующих отчетах.

Мы должны быть начеку по поводу эволюции Интернета вещей, т.к. эти устройства с точки зрения безопасности оставляют желать лучшего.

Атаки шифровальщиков по-прежнему будут в лидерах по их количеству, и эта тенденция будет продолжаться так долго, пока будет оставаться существенный процент жертв, готовых платить выкуп, а силовые структуры будут не способны отслеживать денежные операции с биткоинами.

Мы продолжим следить за атаками на предприятия, а также за тем, как с целью проникновения в корпоративные сети и кражи информации кибер-преступники все чаще используют (и злоупотребляют) легитимные и невредоносные программные средства, чтобы оставаться незамеченными со стороны систем защиты.

Работая в тесном сотрудничестве с антивирусной лабораторией PandaLabs, мы обязательно будем держать Вас в курсе происходящих событий и новостей из мира информационной безопасности через наш Медиа-центр, а через три месяца мы представим Вам новый анализ событий, произошедших в течение 2 квартала 2017 года.

<http://www.pandasecurity.com/mediacenter/>

<https://www.facebook.com/PandaCloudRus>

<http://www.vk.com/PandaCloudRus>



<http://twitter.com/#!/PandaCloudRus>

5.0 PANDALABS

5

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.



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 2017. Все права защищены.

