Декабрь, 2018

PandaLabs Годовой отчет 2018

panda

pandalabs

Введение:
Состояние информационной безопасности

Введение: состояние информационной безопасности

2017 был тем годом, когда слово *ransomware (шифровальщик)* перестало быть термином исключительно экспертов по ИБ и ИТ-сотрудников. Огромное внимание СМИ к таким атакам как WannaCry и Petya/GoldenEye превратило этот тип угрозы в одну из ключевых тенденций прошлого года. Однако, как известно специалистам, широко освещаемые события никогда не должны служить индикатором риска и не должны влиять на любые решения, связанные с безопасностью.

В рамках данного годового отчета мы, антивирусная лаборатория PandaLabs компании Panda Security, рассмотрели данные по угрозам, собранные в лаборатории из наших источников и сенсоров. Мы включили в него данные от решений безопасности конечных устройств, установленных на устройствах наших клиентов, тенденции, наблюдаемые нашими аналитиками при классификации файлов и поиске угроз (threat hunting), а также наиболее актуальные инциденты информационной безопасности, о которых сообщалось во всем мире.

Информация, полученная в 2018 году, продолжает отражать распространенность вредоносных атак: 9 миллионов вредоносных URL и 2,4 миллиона атак, заблокированных на каждый миллион конечных устройств в месяц. В течение анализируемого периода 20,7% изученных компьютеров подверглись хотя бы одной вредоносной атаке.

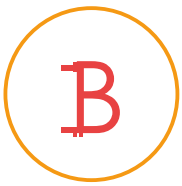
Впрочем, несмотря на постоянную лавину атак такого рода, которые по большей части носят авантюрный характер, PandaLabs может сделать вывод о том, что искоренение инфекций, вызванных атаками на основе файлов, почти завершено, и в настоящее время имеются лишь остаточные уровни. Это связано с развитием модели 100% классификации всех исполняемых файлов в системах, способной блокировать запуск любой программы, неизвестной для Panda Security, до тех пор, пока она не будет классифицирована. В свою очередь, кибер-преступники развивают тактики более коварных атак, которые используют существующие программные решения для проникновения в сеть жертвы и/или после этого. Это наводит нас на мысль о том, что подобный тип атак будет активно развиваться в будущем.

Еще раз было подтверждено, что методы безопасности на основе сигнатур хотя и экономически оправданы, но становятся все менее эффективными против такого рода атак, учитывая невозможность охвата всего широкого спектра особенностей, присущих этим безфайловым атакам на протяжении 2018 года.

Самые успешные типы атак против компаний в 2018 году

Широко распространенные вредоносные атаки

Атаки с использованием RDP



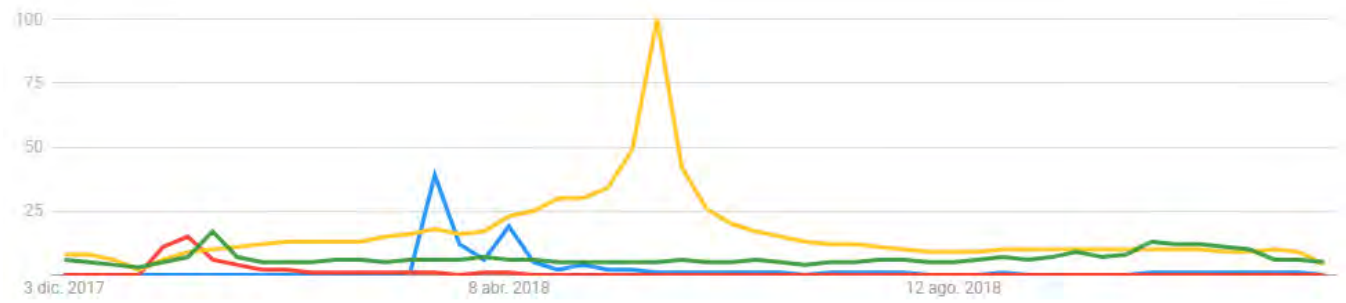
Бум криптоджекинга и шифровальщиков как услуги

Пока традиционные техники (фишинг, шифровальщики, компрометация корпоративной почты BEC) выглядят как никогда плодотворными, бум атак с использованием **RDP** в сочетании с другими техниками социальной инженерии, формируют у злоумышленников новый вектор проникновения. Если мы добавим к этому еще и бум **криптоджекинга и шифровальщиков как услуги (Ransomware as a Service), которые мы наблюдали в этом году, то мы имеем три основных типа атак, которые успешно взламывали корпоративные сети в 2018 году**.

Основной целью для кибер-преступников все еще являются конечные устройства. Именно на них хранится основной объем конфиденциальной информации, именно там они могут злоупотреблять регистрационными данными жертвы, что позволяет им перемещаться внутри сети от одной системы к другой. **Однако бюджет безопасности на защиту конечных устройств составляет примерно одну треть от того, что выделяется на безопасность сети в целом.**

Поэтому неудивительно, что учитывая такие эти бюджетные ограничения, многие корпоративные конечные устройства все еще защищены "традиционными" технологиями, которые не подходят для решения современных задач информационной безопасности.

Неудивительно и то, насколько успешны многие злоумышленники, учитывая, что в среднем для компрометации систем им требуется намного меньше времени, чем то время, которое необходимо предприятиям для их обнаружения. Эта несбалансированность наряду с хронической нехваткой специалистов в данной сфере по-прежнему будут представлять собой для предприятий основные проблемы, связанные с информационной безопасностью.



Поисковые запросы в Google:

- GDPR
- Cambridge Analytica
- Meltdown и Spectre

Данный график подтверждает, что, вероятнее всего, GDPR вызвал наибольший интерес с точки зрения объема поисковых запросов.

PandaLabs:

Данные об угрозах в 2018 г.

PandaLabs: Данные об угрозах в 2018 году

Решения Panda Security для защиты конечных устройств интегрируют многочисленные уровни технологий и сервисов, разработанных для защиты от вредоносных программ различных типов (основанных на файлах), а также от атак в памяти, через эксплойты или с помощью безфайловых техник. Многие атаки сочетают в себе различные техники, чтобы максимально повысить свои шансы на успех и в то же время сократить до минимума расходы кибер-преступника.

В этом отчете мы представим Вам данные об угрозах, соответствующих наиболее важным уровням защиты, о которых мы получили сведения с установленных корпоративных продуктов для конечных устройств: сигнатуры (специфические и общие), эвристика, поведенческий и контекстный анализ, защита от эксплойтов в памяти и сервисы. Эти уровни защиты предоставляются локально с помощью агента, установленного на конечном устройстве, и из облака, как представлено на рисунке 1 ниже.

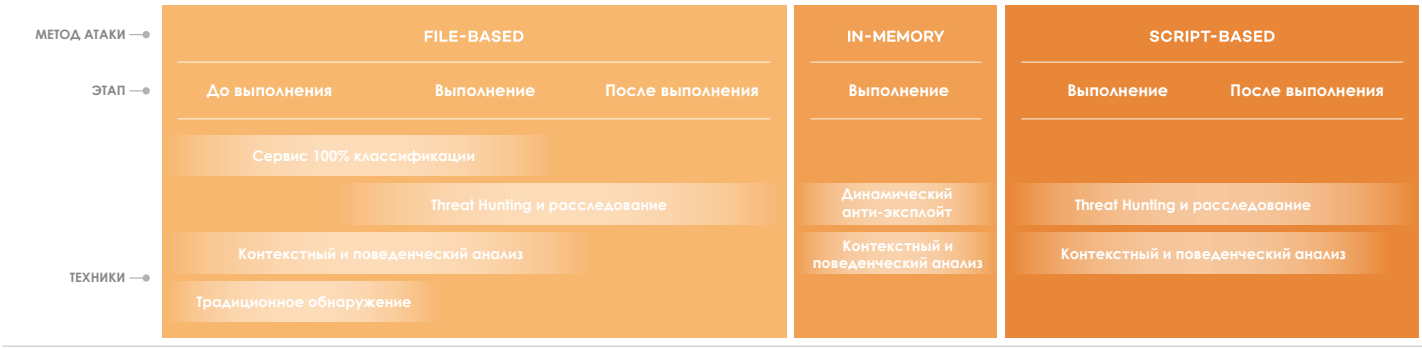


Рис. 1. Технологии защиты, методы и этапы атаки.

Обнаружения до выполнения угроз

Большинство вредоносных программ, обнаруженных на защищаемых конечных устройствах в компаниях, идентифицируется с помощью сигнатур и эвристики. Однако большинство вредоносных программ не запускаются на конечном устройстве из-за блокировки фишинговых писем и URL, связанных с вредоносными программами. В то время как **общее количество вредоносных файлов, поступающих на конечные устройства, постоянно растет (более 60% в течение рассматриваемого периода), для наших клиентов риск от файловых угроз существенно сократился** до предельных значений. Это связано с эффективностью интегрированных сервисов (предоставляемых через продукты и услуги), в частности, благодаря применяемому в Panda Security **подходу "100% классификации", который по умолчанию предотвращает выполнение неизвестных исполняемых файлов до тех пор, пока они не будут классифицированы в PandaLabs.**

В среднем, **на каждый миллион конечных устройств в месяц было обнаружено свыше 2,4 миллионов вредоносных файлов и заблокировано свыше 9 миллионов вредоносных URL.** Большинство из них мы видели только один раз.

Анализируя вредоносное ПО, векторы атак и вредоносные коды в 2018 году, мы можем видеть, что распространенность категорий вредоносных программ, обнаруженных на этом этапе, не сильно изменилась за последний год. **Трояны и шифровальщики составляют большинство этих угроз.** Однако **блокировка вредоносных URL** (через прямое обращение или через встроенные URL в письмах) происходит **более чем в 3,7 раз чаще,** чем обнаружения вредоносных файлов, **представляя собой более популярный вектор проникновения угроз на конечное устройство**, вместе с атаками типа brute-force против RDP - о развитии этого вектора атаки мы прогнозировали в начале года

2,4 МЛН. Вредоносных файлов

Вредоносных URL, блокируемых ежемесячно на миллион конечных устройств **9 МЛН.**

Мы считаем, что **доступное из Интернета RDP-подключение представляет в наши дни все более серьезный риск** для многих организаций, которые не знают о своей незащищенности. Стать жертвой данной техники атак означает постоянное сканирование со стороны кибер-преступников в поиске легких возможностей проникновения в сеть компании. Данные PandaLabs подтверждают тот факт, что **70% наших клиентов среди средних и крупных предприятий ежемесячно подвергаются такого рода RDP-атакам.**

Что касается наиболее распространенных векторов входа и вредоносных кодов в этом году, **то электронная почта продолжает оставаться наиболее популярным вектором атаки**, хотя многие из них в конечном итоге оказывались в спамовых папках до того, как попасть на конечное устройство. Пользователи, особенно при использовании мобильных устройств, в большей степени подвержены риску со стороны вредоносных URL или зараженных сайтов.

В связи с этим, сайты, зараженные кодом Coinhive, становятся более распространенной угрозой, будучи менее агрессивной формой **криптомайнинга.** Coinhive, изначально разработанный для того, чтобы позволять владельцам сайтов зарабатывать дополнительный доход без запуска рекламных объявлений, стал ведущей угрозой этого года, а потому его код устанавливается на взломанные сайты без ведома их владельцев. Такая незаконная служба криптомайнинга истощает ресурсы процессора и заряда батарей на устройствах в то время, пока пользователь находится на зараженном сайте. Фактически, **криптомайнинг вырос в 3,5 раза по сравнению с аналогичным периодом прошлого года**, в то время как шифровальщики выросли в 2,5 раза за тот же период. В 2018 году майнеры Monero составили почти 70% от общего числа идентифицированных криптомайнеров.

Классификации до выполнения угроз

Т.к. новые типы вредоносных программ создаются и публикуются намного быстрее, чем добавляются возможности их обнаружения, то всегда существует разрыв в обнаружении. Это приводит к **неизбежным инфекциям ряда пользователей, у которых нет более надежной и комплексной защиты.**

Чтобы устранить этот разрыв и свести к минимуму риск инфекции для клиентов, в 2015 году компания Panda Security представила "Сервис 100% классификации", который гарантирует, что все PE-файлы, пытающиеся запуститься на конечных устройствах, должны быть классифицированы PandaLabs в качестве надежных файлов прежде, чем им будет разрешен запуск. Этот сервис безопасности работает в качестве последней линии обороны против вредоносных программ на основе файлов.

За период с января по ноябрь на миллион конечных устройств ежемесячно наблюдалось примерно 5,8 миллионов различных исполняемых файлов. В то время как большинство файлов повторяются из месяца в месяц, каждый месяц примерно 20% из них были ненадежными или неизвестными. Из них в среднем 1,3% в конечном итоге классифицировались как вредоносные.

Pandalabs обнаружила

5,8 МИЛЛИОНОВ в месяц

Исполняемых файлов

На миллион конечных устройств

Обнаружение атак через поведенческий анализ

Модуль поведенческого анализа, который блокирует действия на основе их контекста выполнения, может распознавать сотни различных комбинаций процессов, их взаимосвязей, действий и пр., которые свидетельствуют о ранних этапах атак различных типов (шифровальщики, майнеры, атаки на базе скриптов и пр.). Как это ни странно, но из-за раннего предотвращения угрозы мы не можем определить окончательную природу угрозы, учитывая, что **хакеры также могут использовать комбинацию техник внутри одной атаки**. Для наших клиентов внедрение этих превентивных техник было огромным успехом в борьбе с опасными угрозами, например, шифровальщиками.

За наблюдаемый период времени **модуль поведенческого анализа предотвратил свыше 15 тысяч вредоносных действий** (например, последовательность событий, свидетельствующих о начальных этапах атаки) **на миллион конечных устройств в месяц. Злоупотребления PowerShell** для закрепления в системе занимают первое место, и на их долю приходится почти 26% этих блокировок.

Обнаружение эксплойтов в памяти

Атаки в памяти, которые эксплуатируют уязвимости в запущенных приложениях, обнаруживаются с использованием интегрированного динамического **модуля защиты от эксплойтов**. Данный модуль **обнаруживает в среднем свыше 8100 попыток эксплуатации на миллион конечных устройств в месяц. Internet Explorer и Outlook - эти приложения пострадали от большинства атак.**

Pandalabs обнаружила

8 100
ПОПЫТОК ЭКСПЛОЙТОВ В МЕСЯЦ

На миллион конечных устройств

Pandalabs обнаружила

15
тыс./месяц

Вредоносных действий

На миллион конечных устройств

Threat Hunting

Атаки со злоупотреблением законными программами и утилитами, присутствующими в среде, с хакерами, пытающимися спрятаться за нормальной активностью пользователей и систем, **представляет собой в наши дни одну из самых больших проблем**. Растущие возможности кибер-преступных групп или государств, использующих новые техники взлома и техники без использования вредоносных программ, а также сложность (вернее, невозможность) обнаружения таких заражений обычными методами ведут нас к уверенности к тому, что такие атаки станут самым серьезным вызовом для департаментов ИТ-безопасности.

Эта проблема усугубляется острой нехваткой квалифицированных специалистов по вопросам безопасности. По некоторым оценкам, к 2021 году возникнет дефицит в 3,5 миллиона человек. Мы считаем, что в наши дни это самая важная задача в сфере информационной безопасности.

Threat Hunting и сервис расследований компании Panda Security, будучи интегрированным компонентом решений **Panda Adaptive Defense**, **предназначены для выявления таких атак.** Сервис, предоставляемый командой экспертов **PandaLabs**, основан на собственных инструментах для создания и ретроспективного тестирования и проверки гипотез в отношении всех активностей, мониторинг которых осуществляется на всех конечных устройствах, для расследования потенциальных инцидентов и оказания помощи нашим клиентам по реагированию на подтвержденные инциденты.

За анализируемый период было подтверждено и расследовано порядка **90 типов инцидентов**.

Примеры случаев, расследованных в PandaLabs

Случай #1. Крупная сервисная компания

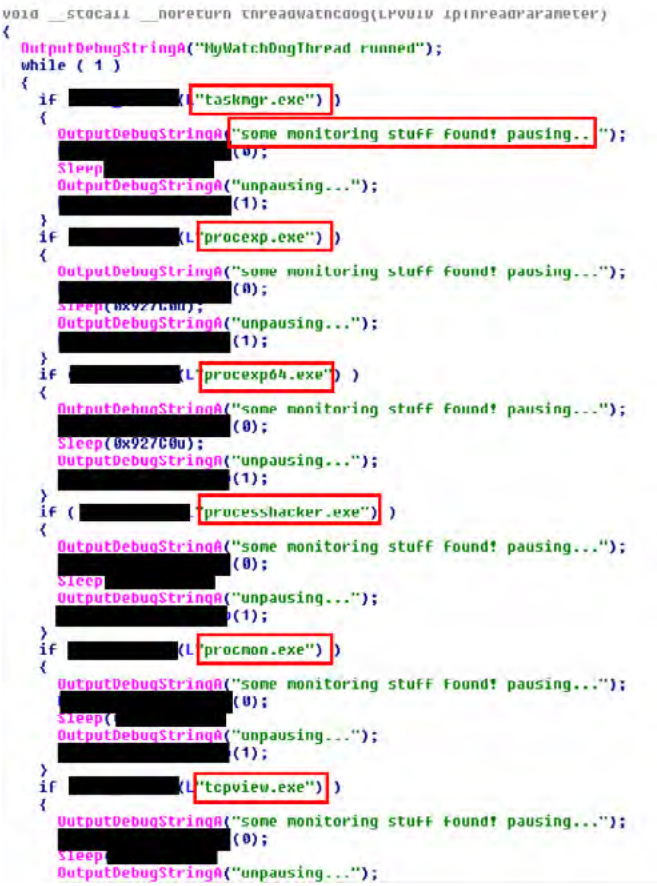
В системе, на которой не стояла защита Panda, при использовании телеметрии с защищенных систем были обнаружены подозрительные исходящие соединения с Китаем. Расследование привело к нейтрализации трояна, специально разработанного для извлечения из компании конфиденциальных данных. Троян "самокомпилировался" свыше 100 раз, безуспешно пытаясь уйти от блокировок путем создания различных вариантов самого себя.

Случай #2. Несколько клиентов

Пользователь получил по электронной почте письмо с документом Word, который использовался для запуска скрипта. Это, в свою очередь, привело к тому, что PowerShell скачал легитимную утилиту для сетевого подключения (socat.exe) и Tor. Обнаружение поведенческого анализа обратило внимание наших экспертов по threat hunting. Утилита подключения использовалась для создания ретранслятора с Tor, используя локальные порты для скрытия от инструментов сетевого мониторинга. Об этой технике уже сообщалось ранее в связи с банковскими троянами, но окончательный замысел злоумышленников в нашем случае остался неизвестным.

Случай #3. Предприятие средних размеров

Уязвимость EternalBlue использовалась для запуска файла прямо в памяти, включая код для подключения к серверу управления C&C и сбора системной информации (версия операционной системы, установленные продукты безопасности и пр.), а также кражи паролей пользователей. Чтобы избежать обнаружения, направленный бот также пытался добавить свое местоположение в исключения у Windows Defender, и включил свое собственное внедрение протокола Tor. В одном случае бот скачал и установил драйвер, руткит “Necurs” с функционалом для отключения различных продуктов безопасности, а также искал наличие утилит для мониторинга процессов и останавливал их работу во избежание обнаружения. В этом случае бот также скачивал и запускал модифицированный XMRIG криптомайнер в качестве службы без использования диска.



Драйвер обнаруживает присутствие программ безопасности и утилит мониторинга процессов, чтобы остановить их работу.

Вредоносные инциденты, попавшие в PandaLabs

Миссия Panda Security заключается в том, чтобы защитить своих клиентов от угроз безопасности. Вся представленная выше информация об угрозах, техниках, технологиях и сервисах была бы бессмысленной, если бы в конечном итоге наши клиенты не смогли бы защитить свои ИТ-системы и информацию, становясь жертвами злоумышленников. Таким образом, в качестве критического показателя для измерения нашего успеха в борьбе с кибер-атаками мы включили статистику по количеству инцидентов, попавших в PandaLabs от наших клиентов, и их динамике за последние 4 года. Цифры ниже показывают еженедельное количество зарегистрированных инцидентов за 2015, 2016, 2017 и 2018 годы по всем корпоративным и домашним продуктам.

Как мы видим, **в 2018 году количество зарегистрированных вредоносных инцидентов упало практически до нулевых значений**. Классификация всех исполняемых файлов, видимость всех запущенных программ и их активности, эффективность поведенческого анализа в реальном времени при выполнении авторизованных приложений, и также непрерывные сервисы поиска угроз (threat hunting), предоставляемые экспертами лаборатории, способствовали той ситуации, при которой можно говорить об остаточных уровнях вредоносных инцидентов среди наши клиентов. В 2018 году общее количество вредоносных инцидентов, попавших к нам от клиентов с Panda Adaptive Defense 360 или Panda Adaptive Defense, составило всего 10 штук, 8 из которых стали результатом ошибок или проблем с подключением.

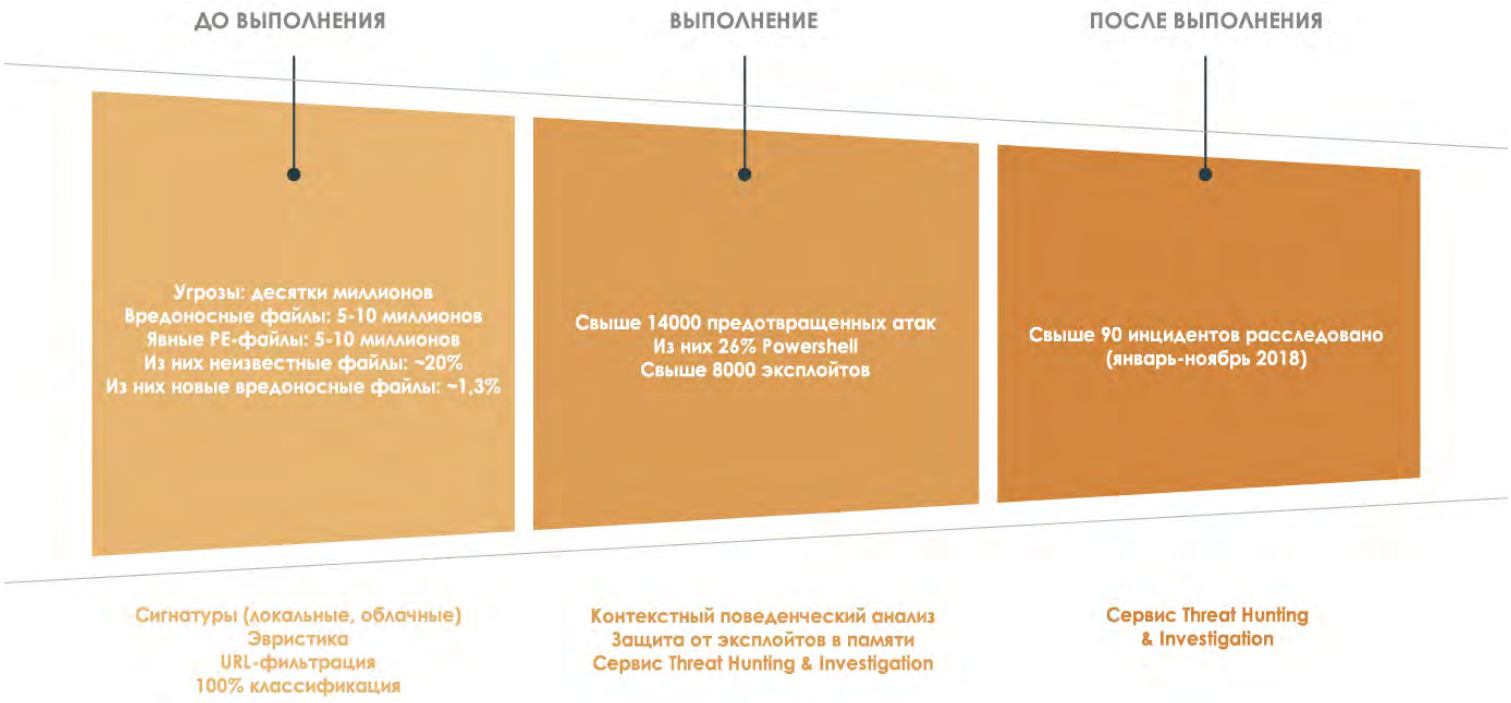
"Воронка смягчения угроз"

Угрозы, нацеленные на конечное устройство, можно охарактеризовать по их категории или типу (шифровальщик, криптомайнер, троян, безфайловая угроза и т.д., хотя многие атаки используют сочетание различных техник), а также в зависимости от уровня их сложности или кастомизации атаки. **Защита от очень сложных или кастомизированных атак требует высокого уровня зрелости у возможностей защиты конечного устройства.** Несмотря на то, что единственной и наиболее эффективной мерой смягчения угроз, которая может быть предпринята в компаниях, является патчинг, мы не ожидаем значительных изменений в значениях средней скорости, с которой компании внедряют даже самые критические патчи. Это связано с ограничениями по времени и ресурсам, а также из-за неудобств для пользователей и сопротивления с их стороны. Тем не менее, **в наши дни можно существенно снизить риск со стороны угроз, используя средства защиты конечных устройств следующего поколения**.

Данные показывают, что используя "запрет по умолчанию" для неизвестных и ненадежных приложений, достигающих конечных устройств, вместе с управляемым сервисом, который быстро осуществляет классификацию, способно понизить уровень риска со стороны вредоносных программ на основе файлов до предельно низких значений, с полной прозрачностью и удобством для администраторов и пользователей.

График ниже показывает смягчение угроз, наблюдаемые на выборке анализируемых конечных устройств, т.к. технологический и сервисный уровни отфильтровывают угрозы в зависимости от их уровня сложности или кастомизации.

«Воронка смягчения угроз»



Кибер-новости 2018:

От месяца к месяцу

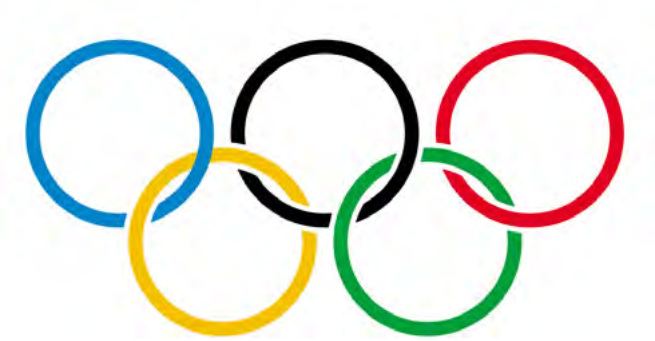
Январь

Уязвимости Meltdown и Spectre

Год начался с большой паники: анонс "катастрофических" уязвимостей **Meltdown и Spectre** (CVE-2017-5754), затронувших большинство современных процессоров. Мы не будем вдаваться здесь в технические подробности, т.к. доступно много информации. Мы просто отметим, что мы можем вздохнуть с облегчением, т.к. до сих пор мы не видели никаких реальных атак, а их последствия были ограничены небольшими проблемами производительности, которые Вы можете посмотреть **здесь**. Есть **ряд бесплатных утилит** для пользователей, чтобы проверить, защищены ли их системы от этих уязвимостей.

Кибер-атака на Зимние Олимпийские игры

Во время церемонии открытия Зимних Олимпийских игр в Южной Корее **кибер-атака** затронула Интернет-подключения, телевидение, а также сайт Игр. Хотя изначально в этой атаке была обвинена КНДР, спецслужбы США позже **приписали эту атаку российским агентам**.



Февраль

Срыв Форума злоумышленников “Infraud”

Министерство юстиции США предъявило обвинения 36 людям и арестовала 13 человек в результате срыва форума кибер-преступников “**Infraud**”. Эта группа нанесла пользователям ущерб в размере свыше 530 миллионов долларов США. Под лозунгом "Мы верим в Мошенничество" эта группа организовала незаконный бизнес-форум для своих 11000 участников, продавая украденные онлайн-личности, взломанные дебетовые и кредитные банковские карты, персонально идентифицируемую информацию, финансовую и банковскую информацию, вредоносное ПО для компьютеров и другую контрабанду. Вы можете найти подробности **здесь**.

Март

Создатели вредоносных программ “Cobalt” и “Carbanak” арестованы в Испании

В марте особое значение имел арест в Испании гражданина Украины. По **сообщениям**, он считается "мозгом" известных вредоносных программ Carbanak и Cobalt. По данным правоохранительных органов, проводивших арест, кибер-преступник и его сообщники заразили свыше 100 банков вредоносной программой, которая использовалась для удаленного взлома банкоматов, украв свыше 1 миллиарда долларов США менее чем за 1 год.

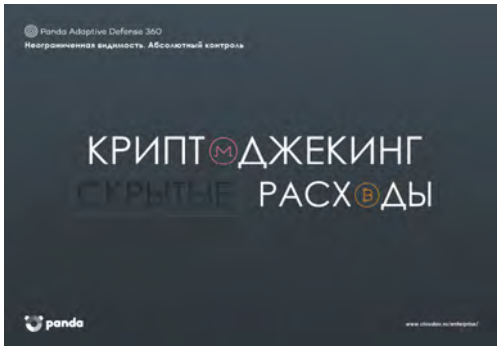
Обнаруженные в системах бэкдоры использовались правительством Великобритании

В марте исследователи **обнаружили несколько бэкдоров** в системах поставщика правительства Великобритании, разработанных для кражи правительственных и военных данных. Эта атака была связана с группой APT15, и есть подозрение, что утилита Mimikatz использовалась для сбора регистрационных данных системных администраторов.

Апрель

Coinhive становится главной угрозой

Cryptojacking - это несанкционированное использование устройства пользователя для майнинга криптовалют. Проще говоря, злоумышленники используют вредоносную программу, чтобы "захватить" эти компьютеры, планшеты или смартфоны и эксплуатировать часть их вычислительных мощностей для скрытого майнинга криптовалют. Одна из наиболее распространенных техник включает в себя **"захват" процессора жертвы или его GPU, когда он посещает сайт, зараженный специальной вредоносной программой для криптомайнинга**, как недавно случилось на YouTube. В этом случае рекламная платформа **DoubleClick** стала жертвой атаки, которая прятала код Coinhive для криптоджекинга в рекламе на YouTube. Да, Coinhive - это наиболее часто используемый скрипт для такого рода атак. **Исследование эксперта по безопасности Троя Мурша** выявило **50 000 сайтов, зараженных скриптом для криптоджекинга**, 80% из которых использовали Coinhive.



Май

VPNFilter – спонсируемая государством атака на SOHO-роутеры

ФБР и Министерство юстиции США объявили о "**действиях**" по вскрытию ботнета VPNFilter, который поразил сотни тысяч домашних роутеров ряда производителей. Предполагается, что ботнет контролировался группой лиц, спонсируемых одним из государств. Позже было обнаружено, что вредоносная программа может доставлять эксплойты на конечные устройства с помощью функции man-in-the-middle. Подробнее Вы можете прочитать **здесь**.

GDPR и некоторые непредвиденные обстоятельства

В мае вступило в силу общеевропейское законодательство о защите персональных данных (**GDPR**). Возможно, самым заметным результатом для пользователей стал поток сообщений на получение согласия на хранение их данных, что было использовано преступниками, которые запустили **фишинговые кампании**.

Еще одним непредвиденным последствием нового европейского регламента стало ограничение исследований в области ИБ для тех, кто использует **WHOIS** - систему для получения регистрационных данных доменов и диапазонов IP-адресов. ICANN, которая осуществляет надзор и управление системой доменных имен, предложила исключить ряд ключевой информации из публичных данных для соответствия требованиям GDPR, тем самым ограничив возможности исследователей по ИБ. В июне ICANN опубликовала предложение о предоставлении доступа к полным данным WHOIS в законных целях (со стороны правоохранительных органов), а также о надлежащей защите ПД в соответствии с GDPR. Сейчас ICANN собирает отзывы на свое предложение.

Нарушения бизнес-процессов в Мексике и Чили

В мае несколько финансовых учреждений Мексики и Чили подверглись кибер-атакам. В Мексике кибер-преступники атаковали приложения и инфраструктуру, используемые рядом банков для подключения к электронной системе межбанковских платежей SPEI. Они смогли незаконно перевести 400 миллионов песо (примерно 18 миллионов евро). Несколько дней спустя кибер-преступники запустили две атаки на Banco de Chile. Первая, как предполагается, служила для отвлечения внимания, и была атакой шифровальщика, который атаковал тысячи ПК и банкоматов, а также воздействовал на многие сторонние системы. А вот вторая атака, которая была "реальной" атакой, была направлена против системы SWIFT у этого банка. В этом случае хакеры смогли перевести примерно 10 миллионов долларов США с операционных счетов банка на счета в Гонконге. Нет никаких подробностей о методах, использованных злоумышленниками.

Июнь

Продукты, запрещенные в учреждениях ЕС

Следом за США, Великобританией и Нидерландами, 13 июня **Европарламент утвердил резолюцию о кибер-защите**, которая среди прочих рекомендаций призвала ЕС "…провести тщательный обзор ПО, ИТ и коммуникационного оборудования и инфраструктуры, используемых в учреждениях, с тем чтобы исключить потенциально опасные программы и устройства, и запретить те, что были признаны вредоносными, такие как Kaspersky Lab". Сразу после этого, Kaspersky приостановил сотрудничество с Европолом и проектом NoMoreRansom.

Этот шаг ЕС привлечет еще больше внимания к геополитическим рискам безопасности, которые должны учитываться организациями при принятии решений о покупке.

Кибер-атака на спутники

В июне была обнаружена **кибер-атака**, которая, по словам заметивших ее экспертов, была запущена с компьютеров в Китае и направлена на спутники США и Юго-Восточной Азии. Эти спутники принадлежали оборонным предприятиям и телекоммуникационным операторам. Цель атаки очевидна: шпионаж, в частности, перехват военных и гражданских сообщений. Исследователи заявили, что хакеры смогли заразить компьютеры, которые управляли спутниками, а теоретически это могло означать, что они могли изменить свою орбиту.

Июль

Поддельные сообщения WhatsApp вызвали убийства в Индии

Как объяснил репортер, "фейковые новости обвиняют в том, что они вводят в заблуждение избирателей и, возможно, влияют на выборы на Западе. Но в Индии они убивают людей". По крайней мере, 5 человек были избиты до смерти после того, как ложные слухи о похищении людей были распространены через WhatsApp. Поступали также сообщения о нескольких других случаях избиений в стране. Проблема заставила полицию Индии начать кампанию против фейковых новостей, а правительство страны потребовало, чтобы приложение заблокировало эти сообщения. Компания даже представила в стране новую функцию, чтобы запретить пользователям отправлять сообщения более чем пяти людям или группам одновременно.

Русские шпионы обвиняются во взломе DNC

13 июля Министерство юстиции США предъявило обвинения 12 русским шпионам за **хакерские преступления**, связанные с президентскими выборами 2016 года. Был предоставлен подробный доклад об использовавшейся тактик и выполненных операциях командой агентов, которые, судя по докладу, были сотрудниками ГРУ. Использовался фишинг для кражи регистрационных данных ряда лиц, содержимого писем, взлома их компьютеров и внедрения сотен файлов с вредоносным кодом. Для этого они **установили вредоносный X-Agent**, который способен записывать нажатия клавиш, красть файлы и делать скриншоты.

Sextortion

Испанская полиция предупредила о возобновлении кампаний по сексуальному вымогательству *sextortion*, в которых с 2014 года пострадало свыше 6000 человек. В кампаниях используются пароли, собранные в прошлом с помощью утечек данных, доступных на форумах по ИБ, которые все еще могут использоваться жертвами. Затем жертву заставляют поверить, что хакер мог взломать их систему и использовать веб-камеру для записи видео при просмотре жертвой порнографии. После идет угроза о том, что если не будет выплачен выкуп, то это видео будет опубликовано. По данным полиции Испании, выкуп варьируется от 50 до 6000 евро (в биткоинах).

Facebook оштрафовали за скандал с Cambridge Analytica

Комиссар по вопросам информации, контролирующий конфиденциальность в Великобритании, **оштрафовал Facebook на 500 тысяч фунтов стерлингов**, а это максимально возможный штраф, за два нарушения Закона о защите данных. Многие считают этот штраф легкой пощечиной для компании с годовым оборотом свыше 40 миллиардов долларов США в 2017 году. В соответствии с новыми правилами GDPR, вероятно, что штраф был бы гораздо более существенным.

Морские пути в опасности

В информационной безопасности 50 000 судов, находящихся в море, были выявлены многие уязвимости. Было обнаружено, что многие из них все еще используют устаревшие системы (некоторые из них еще имеют Windows NT с 1993 года) вместе с открытыми терминалами спутниковой связи, пользовательскими интерфейсами, доступными через небезопасные протоколы, а также регистрационными данными по умолчанию, которые никогда не менялись.

Пробелы в безопасности судов могут нанести существенный ущерб как национальной промышленности, так и морской среде, включая порты, каналы и доки. Аналитики предположили, что заполучив доступ к ECDIS (электронная система отображения карт и информации, используемая судами для навигации), также возможно получить доступ к системам, которые предупреждают капитана о возможных сценариях столкновения. Управляя этими сигналами о столкновениях, хакеры могут остановить такие важные маршруты как Ла-Манш, поставив под угрозу импорт и экспорт всей страны.

Август

Манипуляция мнением

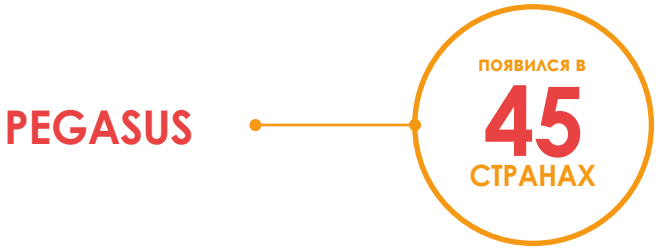
Действуя по наводке от компании FireEye, работающей в сфере ИБ, 21 августа Facebook объявил об удалении с Facebook и Instagram 652 страниц, групп и аккаунтов (некоторые из них из России и Ирана), которые занимались "скоординированным недостойным поведением". Эти страницы использовались для введения в заблуждение других людей о том, кем они были и что они делали.

В тот же день Microsoft **объявила**, что компания сорвала планы атаковать промежуточные выборы в США в ноябре. По данным от технологического гиганта, хакеры из группы Fancy Bear создали шесть доменов, которые выглядели так, словно это сайты Международного Республиканского Института, и которые должны были использоваться в фишинговых кампаниях.

Сентябрь

Шпион достиг 45 стран

18 сентября было выявлено, что опасный **шпион под названием Pegasus** распространился в 45 странах, из которых 6 стран ранее использовали шпиона для нарушения прав человека. Разработанный израильской компанией NSO Group, шпион направлен против устройств iPhone и Android, получая доступ к ним с помощью фишинга для запуска серии атак нулевого дня с обходом механизмов безопасности. Он используется для чтения сообщений, отслеживания звонков, сбора паролей, отслеживания местоположения и компиляции данных.



Обвинения за WannaCry

В сентябре министерство юстиции США предприняло необычный шаг: **официально обвинило** хакера из КНДР в совершении атак WannaCry, в причастности к взлому Sony Pictures в 2014 году и за кражу в Центральном банке Бангладеш в 2016 году.

Октябрь

Кибер-атака на Нидерланды

4 октября голландское правительство сообщило, что голландские и британские официальные службы прервали **кибер-атаку против Организации по запрещению химического оружия (ОЗХО)** в Гааге. Считается, что эта организация была атакована из-за непрекращающегося расследования о применении Россией химического оружия в Сирии и Великобритании. В этом деле были обвинены 4 российских агента, которые, вероятно, являются членами команды кибер-воинов ГРУ. Как утверждается, они прибыли в Нидерланды с дипломатическими паспортами. Они хотели взломать сеть организации, используя оборудование, спрятанное в машине, припаркованной рядом со штаб-квартирой, и нарушить работу ее компьютеров.

8 октября Google объявил о **закрытии своей социальной сети Google Plus** из-за дыры безопасности, которая привела к раскрытию персональных данных не менее 500 000 пользователей. Компания заверила своих пользователей, что ни один хакер не смог получить доступ к этим данным.

Ноябрь

Новая версия Stuxnet

Червь Stuxnet впервые был обнаружен в 2010 году в Иране. Считается, что он был разработан специально для атаки на иранские АЭС. 2 ноября Голамреза Джалали, Начальник гражданской обороны Ирана, заявил, что они обнаружили, как считается, **новую версию** данной атаки при попытке получить доступ к стратегическим сетям страны и объектам критической инфраструктуры.

Утечка данных в "черную пятницу" на Amazon

Всего за несколько часов до "Черной пятницы" **Amazon информировал ряд своих клиентов о "технической ошибке"** на своем сайте, которая раскрывала ФИО и адрес электронной почты лица, зарегистрированного в аккаунте. Гигант электронной коммерции подтвердил, что подозрительно выглядящее письмо, отправленное этим пользователям, на самом деле было реальным, и объяснил, что была исправлена ошибка, о чем позже были проинформированы пострадавшие пользователи. В отличие от этой утечки, месяцем ранее Amazon уже пострадал от другой утечки из-за сотрудника, продавшего клиентские данные и впоследствии уволенного. Несмотря на заверения Amazon в обратном, всегда лучше заменить свой пароль после инцидента с безопасностью.

Нарушения данных

Год GDPR

25 мая во всем Евросоюзе вступил в силу **GDPR** - **новый регламент по защите персональных данных**. Хотя компании имели два года на подготовку, в итоге в большинстве случаев в последние дни началась борьба за внедрение новых правил.

Многие компании обоснованно нервничали и опасались, если учесть, что **последствия нарушений положений GDPR достаточно суровы**: **штрафы на 10 миллионов евро** или 2% годового оборота (Уровень 1) или 20 миллионов евро или 4% годового оборота (Уровень 2).

Одним из явных последствий стали попытки поспешного соблюдения новых правил в последнюю минуту. Почта была заполнена письмами от компаний, которые просили разрешения пользователей на хранение их данных в файле. Однако многие эксперты отметили, что в них не было необходимости, т.к. компании уже имели эти разрешения от пользователей. В итоге многие компании потеряли ощутимую часть своих контактов.

Несмотря на наличие достаточного времени для подготовки, многие организации , видимо, были застигнуты врасплох. Это стало ясно из того факта, что спустя месяц после внедрения GDPR ряд органов по защите данных **сообщили** о значительном увеличении числа жалоб и уведомлений о нарушениях данных.

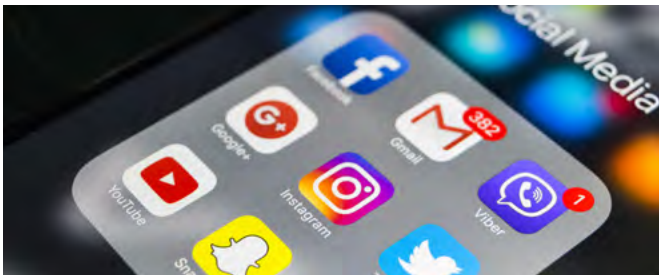
А последствия не заставили себя долго ждать. Первая экономическая санкция в рамках нового регламента была наложена в конце октября, когда **Hospital do Barreiro** в Португалии был оштрафован на 400 000 евро за два нарушения правил.

Штрафы УРОВЕНЬ 1
10 000 000 €
2% **общего годового оборота**

Штрафы УРОВЕНЬ 2
20.000.000 €
4% **общего годового оборота**

Социальные сети: Facebook

В этом году самая популярная соцсеть в мире столкнулась с рядом проблем, связанных с защитой данных и конфиденциальностью пользователей.



Первым инцидентом, обнаруженным в марте, стал **скандал с Cambridge Analytica**. Ряд газет опубликовали подробную информацию о том, как личные данные не менее 87 миллионов пользователей были использованы без разрешения для того, чтобы повлиять на президентские выборы в США. В результате, Марк Цукерберг был вынужден предстать перед Сенатом США.

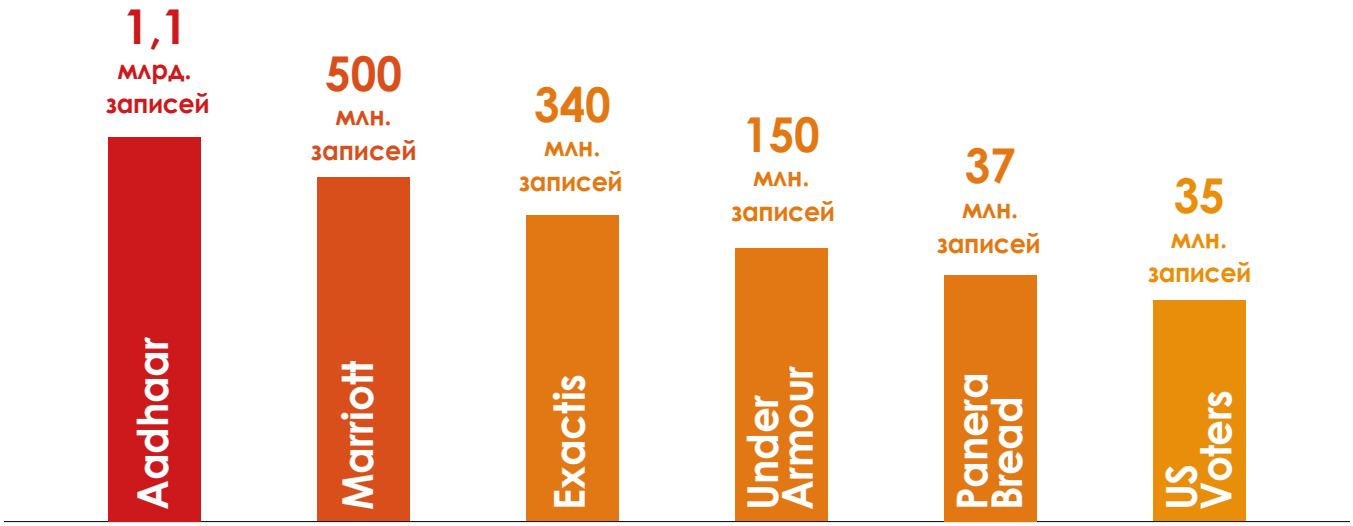
Комиссар по вопросам информации в Великобритании отреагировал **наложением штрафа в 500 000 фунтов стерлингов**, максимально возможного штрафа в рамках о законе по защите ПД до вступления в силу GDPR.

Затем в сентябре примерно **50 миллионов аккаунтов были раскрыты** после кибер-атаки на соцсеть. Хакеры использовали уязвимость, которая позволяла им красть токены доступа пользователей. В этом случае процесс уведомления и последствия заметно отличались.

Следуя правилам, установленным в GDPR, Facebook уведомил Комиссию по защите данных в Ирландии, где находится штаб-квартира компании. Однако еще не ясно, будет ли наложен штраф, который может достичь **1,4 миллиардов евро**.

И именно тогда, когда казалось, что ничего плохого уже не будет, в ноябре был **обнаружен** сайт, продающий сообщения не менее 81 000 взломанных аккаунтов. По словам владельца сайта, у них были данные 120 миллионов аккаунтов, которые они хотели продать. Однако Facebook быстро защитил себя, заявив, что его безопасность не была взломана, и что хакеры, вероятно, использовали вредоносные расширения для браузера, чтобы получить доступ к этим аккаунтам.

К сожалению, истории про нарушения данных постоянно продолжают появляться в СМИ. Ниже мы приводим **рейтинг шести самых серьезных** случаев с января по ноябрь 2018 г. в зависимости от количества пострадавших записей (или потенциально пострадавших).



1. Aadhaar (Индия)

Потенциально 1,1 млрд. записей

Индийская национальная идентификационная база данных Aadhaar содержит записи о 1,1 млрд. граждан Индии, включая их биометрические данные. В январе журналисты одной национальной газеты сообщили, что они смогли **получить любую запись о любом зарегистрированном в Aadhaar человеке за 500 рупий** (примерно 6 евро) из группы в WhatsApp. Они также получили ПО для печати Aadhaar за дополнительные 300 рупий. Агентство UIDAI, управляющее этой базой данных, решительно отвергло все претензии в свой адрес по поводу нарушения данных. Затем в июне один из экспертов по безопасности сообщил, что утечка данных в уязвимой системе позволила любому человеку скачать личную информацию по всем пользователям Aadhaar, включая их ФИО, уникальные 12-значные идентификационные номера, а также дополнительные сведения: банковские данные и другая персональная информация. UIDAI также отвергла обвинения в своей адрес и заявило, что база данных остается “безопасной и надежной”.

2. Сеть отелей Marriott

Пострадало 500 млн. пользователей

30 ноября Marriott International обнаружила, что система бронирования номеров во многих из принадлежащих ей сетей отелей была взломана, в результате чего персональные данные до 500 миллионов ее клиентов были раскрыты, что стало одним из крупнейших случаев нарушения данных за всю историю. Потенциальная ценность раскрытой информации настолько велика, что это привело к предположениям о причастности какого-либо государства к данной атаке, которая была призвана осуществлять шпионаж за передвижениями дипломатов, шпионов, военных представителей и руководителей высокого ранга. Несанкционированный доступ к системе бронирования Starwood Hotels, в которую также входят такие сети как St. Regis, Westin, Sheraton, Aloft, Le Méridien, Four Points и W Hotels, начался еще в 2014 году.

3. Exactis (США)

Примерно 340 млн. записей

В июне эксперт по безопасности Винни Троя обнаружил, что **Exactis, брокер данных из США**, раскрыл записи примерно 340 миллионов человек на общедоступном сервере. По словам Трои, каждая запись содержала до 150 полей информации, описывающей человека, включая ФИО, домашний адрес и номер телефона. Более того, примерно половина записей содержала адреса электронной почты.

Многие скомпрометированные записи также содержали такие данные как число детей в доме, их возраст, тип используемой платежной карт, примерная стоимость дома, наличие акций, увлечения, ипотечная компания, этническая группа, религия и многое другое. Хотя эти записи не содержат номера соц. страховок или банковские данные, все же они могут быть очень полезны для проведения мошеннических и фишинговых атак.

В этом случае, как и во многих других наиболее важных случаях этого года, нам еще предстоит увидеть окончательные последствия. Фактически, Джованни Буттарелли, европейский супервайзер по защите данных, **недавно прокомментировал**, что первые штрафы мы увидим только в конце года.

4. Under Armour (США)

Примерно 150 млн. записей

В марте **Under Armour стал главным героем одного из крупнейших нарушений ПД в истории**. Компания объявила, что произошла утечка данных 150 миллионов пользователей ее популярного приложения для питания и диеты MyFitnessPal после того как были взломаны ее приложение и сайт. Компания обнаружила, что в феврале неизвестное лицо получило доступ к именам пользователей, адресам электронной почты и хэшам паролей пользователей приложения.

5. Panera Bread (США)

До 37 млн. записей (или больше)

В апреле, после контактов с исследователем по безопасности Диланом Хулиханом, Брайан Кребс сообщил, что **сайт сети ресторанов Panera Bread** оставил открытыми записи о миллионах своих клиентов, включая ФИО, адрес электронной почты, почтовый адрес, день рождения и последние 4 цифры номера банковской карты клиента. По словам исследователя, данные оставались открытыми в течение 8 месяцев, несмотря на неоднократные уведомления в компанию после того, как утечка была обнаружена впервые.

6. Избиратели в США

До 35 млн. записей

В октябре, всего за несколько недель до промежуточных выборов в США 6 ноября, **на популярном хакерском сайте на продажу было выставлено до 35 миллионов записей об избирателях.** Высказывались опасения, что эти записи могли быть использованы для оказания влияния на выборы, включая манипуляцию со списками избирателей на избирательных участках, с тем, чтобы помешать людям голосовать. 19 штатов пострадали от этой утечки.

Другие нарушения данных в 2018 году:

British Airways

В сентябре британская авиакомпания сообщила, что с 21 августа до 5 сентября **кибер-преступники могли осуществлять кражу персональных и финансовых данных более 380 000 клиентов**. За атакой стояла группа MageCart, заразившая сайт авиакомпании вредоносным кодом, который позволял им собирать персональную информацию о клиентах British Airways. Последние данные по эту инциденту, опубликованные в октябре, свидетельствует о том, что пострадало 185 000 человек.

Orbitz

В марте сайт по бронированию билетов Orbitz сообщил о том, что **информация о более чем 880 000 платежных карт была украдена,** и вполне вероятно, что хакеры также получили доступ к персональной и конфиденциальной информации пострадавших.

Ticketmaster

В июне сайт по продаже билетов Ticketmaster **сообщил о нарушении данных,** от которого пострадало до 40 000 клиентов в Великобритании и других странах. Были украдены сведения по платежным картам, домашним адресам и номерам телефонов. По данным Ticketmaster, причиной данного инцидента стала вредоносная программа, встроенная в один из своих продуктов для поддержки клиентов.

Adidas

В июне бренд спортивной одежды Adidas **заявил,** что клиенты его сайта в США могли пострадать от нарушения данных. Хотя компания не раскрыла технические детали, этот инцидент потенциально мог затронуть миллионы людей.

T-Mobile

В августе телекоммуникационная компания T-Mobile стала жертвой кибер-атаки, в которой **были украдены** персональные данные порядка 2 миллионов людей (ФИО, номера телефонов, номера аккаунтов и т.д.).

SingHealth (Сингапур)

В июле Сингапур пострадал от **"самого серьезного" нарушения данных** в истории страны, когда были украдены **персональные данные 1,5 миллионов пациентов SingHealth**, самой крупной медицинской компании в стране. **Среди украденных данных оказались персональные данные премьер-министра страны Ли Сянь Луна**. По данным правительства Сингапура, атака "не была работой случайных хакеров или преступных группировок". Нападавшие "специально и неоднократно" охотились за персональными данными мистера Ли.

Timehop

В июле **приложение Timehop заявило,** что оно столкнулось с нарушением данных, затронувшим **21 миллион их пользователей**. Были украдены номера телефонов, ФИО и адреса электронной почты. Хакеры также могли даже получить доступ к аккаунтам пострадавших. По данным Timehop, нарушение стало возможным благодаря недостатку предпринимаемых мер безопасности на их облачном аккаунте.

Не будьте следующей жертвой

Никто не хочет, чтобы их компания появилась в новостях как новая жертва инцидента с нарушением безопасности, т.к. будут негативные последствия для репутации компании, ее бизнеса и ее пользователей. С момента вступления в силу GDPR это стало как никогда актуально. Основная цель данного регламента - это защита данных граждан Евросоюза и контроль над тем, как компании обрабатывают, хранят и используют эти данные, гарантируя безопасность, отслеживаемость и корректное управление. Также появилось право на забвение. Халатность в любом из этих процессов теперь влечет за собой **ряд дополнительных последствий**, таких как штраф до 20 миллионов евро или 4% от общего оборота компании.

Чтобы избежать такого исхода, сперва необходимо осознать важность осуществления эффективных мер и политики в области безопасности. Для организаций, которые обрабатывают данные, профилактика является ключевым аспектом регулирования. Важно работать с перспективой и предвидением, которые являются конкурентным преимуществом в вашей бизнес-стратегии.

Такие решения как **Panda Data Control** способны обнаруживать, осуществлять аудит и мониторинг неструктурированных персональных и конфиденциальных данных на конечных устройствах: от данных в покое до используемых данных и перемещаемых данных. Таким образом, можно избежать нежелательного доступа к конфиденциальным данным вашей компании, гарантируя, что все персональные данные зарегистрированы и отслеживаются, и что вы соблюдаете такие правила как GDPR и PCI-DSS.

Контроль персональных данных, предлагаемый решением **Panda Data Control**, важен еще и для того, чтобы продемонстрировать руководителям, DPO и органам власти, что ваша компания осуществляет строгий контроль на обработкой персональных данных на своих конечных устройствах и серверах. Необходимый инструмент для обоснования любых действий, которые вам необходимо осуществлять с этими данными: изменение, подтверждение или отмена.

Прогнозы ИБ на 2019 год

1. "Живой" взлом

Хотя "традиционные" типы вредоносных программ (черви или трояны), все еще остаются наиболее часто используемыми среди хакеров, однако новые методы атак (например, атаки без использования вредоносных программ) будут развиваться более быстрыми темпами. Это связано с тем, что их все сложнее обнаруживать, а также с возросшим в мире потенциалом осуществления кибер-атак со стороны государств и криминальных группировок.

2. В 2019 году концепция цифрового суверенитета также распространиться на безопасность

В 2018 году геополитика сыграла значительную роль в цифровой сфере как следствие более протекционистских позиций стран западного мира (США и Великобритания), реакции других держав (преимущественно России и Китая) и усиления взаимного недоверия между ними. Такие страны как Франция предпринимают меры для защиты своего цифрового суверенитета. **Мы считаем, что данная тенденция будет только нарастать в 2019 году, особенно в Европе (она будет двигаться к европейскому цифровому суверенитету)**, которая станет четвертым блоком наряду с США, Китаем и Россией. Это будет иметь важное значение с точки зрения стратегий и политики информационной безопасности, а также решений о закупках продуктов этой сферы.

3. Рост атак на цепочки поставок

Этот тип атаки, возможно, один из самых опасных: атаки на цепочки поставок влечет проникновение в процесс разработки в компаниях или законных программных проектах, куда хакеры встраивают вредоносный код. Этот код затем распространяется среди пользователей вместе с обновлениями этого ПО. Случай такого рода был недавно обнаружен в проекте с открытым исходным кодом GitHub, но это только один из многих обнаруженных инцидентов в этом году. Вероятнее всего, в 2019 году мы сможем увидеть еще больше таких инцидентов, учитывая их эффективность, огромное влияние, которое они могут оказать (т.к. они могут быстро распространиться на миллионы систем), и тот факт, что атака "прикрыта" доверием к законному ПО, что затрудняет ее предотвращение.

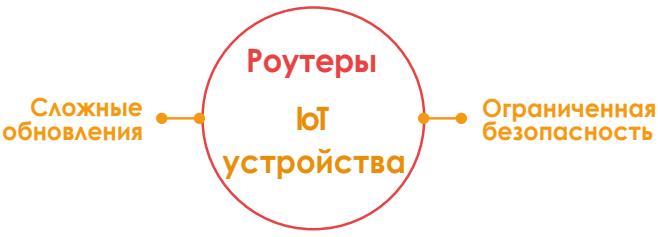
4. Искусственный интеллект станет чаще использоваться злоумышленниками

Те же инструменты и знания, которые используются для анализа огромных объемов данных и производства интеллектуальных алгоритмов, будут все чаще использоваться злоумышленниками со злым умыслом. Это можно объяснить демократизацией данных инструментов и их доступностью, а также наличием информации о продуктах безопасности - все это позволит разрабатывать алгоритмы, которые смогут автоматически обнаруживать новые способы атаки.

5. Будут обнаружены новые катастрофические уязвимости, подобные тем, что были обнаружены годом ранее (Meltdown и Spectre). В середине ноября команда исследователей обнаружила **семь новых атак** на процессоры. Две из них были модификациями атаки Meltdown, а остальные пять - вариациями Spectre. Мы считаем, что чем выше уровень внимания к таким уязвимостям со стороны исследователей, учитывая их влияние и то, что до сих пор проведено достаточно мало исследований по сравнению с уязвимостями в приложениях (значит, еще много чего будет обнаружено!), тем выше вероятность того, что будет поступать все больше новостей об этом, а также выше риск того, что будут изобретены функциональные эксплойты, которые в конечном итоге могут оказаться в руках кибер-преступников.

6. Больше атак на роутеры и IoT-устройства

Учитывая вышесказанное и продолжающуюся тенденцию таких атак как **VPNFilter** (поразил примерно полмиллиона роутеров различных производителей), то в 2019 году мы, вероятно, увидим рост числа атак не только на роутеры, но и в целом на IoT-устройства. **Для этого существует две главные причины: с одной стороны, безопасность этих устройств по умолчанию оставляет желать лучшего**: простые пароли по умолчанию или вообще их отсутствие. С другой стороны, **эти устройства сложнее обновлять**, и многие пользователи даже не знают, как это делать. Таким образом, их уровень защиты намного ниже, чем у других устройств (ПК, ноутбуки). Это означает, что они могут стать легкой добычей в руках кибер-преступников для выполнения DDoS-атак или распространения тех же криптомайнеров, предлагая хакерам низкие расходы и низкие риски, особенно сейчас, когда стоимость криптовалют резко упала и законные майнинговые операции стали менее прибыльными.



7. Нарушение данных, фейковые новости

В марте 2018 года разгорелся скандал с Cambridge Analytica. По оценкам, это привело к тому, что данные примерно 87 миллионов пользователей Facebook использовались в политических целях без их согласия. Массовый анализ данных с помощью доступных инструментов Больших данных позволяет извлекать подробные профили личных предпочтений во многих сферах, не только в политике. Подобно тому как фейковые новости стремятся повлиять на мнение людей и их политическое поведение, распространяемая через различные соцсети (Facebook, Twitter, LinkedIn и т.д.) персональная информация, правильно проанализированная и сопоставленная, может позволить разрабатывать крайне сложные и персонализированные атаки с использованием техник социальной инженерии. Например, используя извлеченную таким образом информацию, можно более эффективно выдавать себя за кого-то другого (или другую компанию), а потому обманом заставить жертву выполнять требуемые действия или вести себя нежелательным образом (например, осуществлять денежные переводы на банковский счет хакера). Эти виды атак (фишинг, компрометация корпоративной почты BEC), которые активно развивались в 2018 году, будут расти и в 2019 году, учитывая их эффективность (по оценкам, в среднем 4% получателей писем, которых стремятся обмануть, нажимают на нужные ссылки в них) и сложность в обнаружении.

На самом деле, безопасность, необходимая для защиты от этих прогнозируемых тенденций 2019 года и любых других видов незаконных действий, лежит в концепции модели Panda Adaptive Defense: решение способно контролировать и классифицировать каждый активный процесс (100%) на всех рабочих станциях в корпоративной сети, включая и те инструменты, которые, видимо, законны, но могут иметь подозрительное поведение или становиться векторами проникновения в сеть (например, RDP).

Panda Adaptive Defense - это не продукт: скорее, пакет информационной безопасности, который сочетает в себе решения для защиты конечных устройств (EPP, Endpoint Protection) и обнаружения атак на конечные устройства и реагирования на них EDR, Endpoint Detection & Response) с сервисами 100% классификации и Threat Hunting & Investigation. Это идеальное сочетание решений и сервисов для обеспечения детальной видимости всей активности на всех конечных устройствах, контроля над всеми запущенными в сети процессами и сокращения поверхности атаки.

Panda Adaptive Defense автоматически классифицирует 99,985% процессов, а оставшиеся 0,015% требуют внимания со стороны аналитиков. Квалифицированные аналитики PandaLabs, которые благодаря сервису 100% классификации, ликвидировали разрыв в обнаружении, обеспечивая надежность всех запускаемых процессов. Все это позволяет им действовать с точки зрения предотвращения, обнаружения и реагирования на известные и неизвестные вредоносные программы. Они также могут реагировать на атаки, которые не следуют традиционным шаблонам, такие как безфайловые атаки или атаки в памяти. Более того, сервис Threat Hunting & Investigation также служит для совершенствования нашей системы машинного обучения, предоставляя оповещения об аномальных действиях и поведении со стороны пользователей, приложений и устройств.

Предотвращение, обнаружение и реагирование на атаки с вредоносными программами или без них, с помощью единого агента

Видимость в реальном времени и ретроспективе всей активности на всех конечных устройствах в корпоративной сети

Классификация 100% процессов: 99,98% автоматически с помощью машинного обучения, оставшиеся 0,02% - аналитиками Panda

Threat Hunting и Экспертный анализ: глубокий анализ и расследование атак экспертами Panda и нашими партнерами (MSSP)

Библиография

2. PandaLabs: Данные об угрозах в 2018 году

https://www.cloudav.ru/mediacenter/news/no-kidnapping-no-ransom/

https://www.pandasecurity.com/mediacenter/security/evolution-cyberattacks-2017/

https://www.cloudav.ru/mediacenter/news/what-is-cryptojacking/

https://www.cloudav.ru/mediacenter/malware/boom-fileless-malware-attacks/

3. Кибер-новости 2018: от месяца к месяцу

https://www.cloudav.ru/mediacenter/security/meltdown-and-spectre-security-hole/

https://arstechnica.com/gadgets/2018/01/heres-how-and-why-the-spectre-and-meltdown-patches-will-hurt-performance/

https://www.grc.com/inspectre.htm

https://www.cloudav.ru/mediacenter/security/cyber-sabotage-winter-olympics/

https://www.theverge.com/2018/2/25/17050868/winter-olympics-2018-russia-north-korea-cyberattack-opening-ceremonies

https://en.wikipedia.org/wiki/Infraud_Organization

https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

https://threatpost.com/china-linked-apt15-used-myriad-of-new-tools-to-hack-uk-government-contractor/130376/

https://thenextweb.com/hardfork/2018/03/07/wordpress-cryptocurrency-mining-malware/

https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

https://www.pandasecurity.com/mediacenter/panda-security/1980-2018-gdpr/

https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/

https://www.cloudav.ru/mediacenter/news/whois-protocol-gdpr/

https://www.cloudav.ru/mediacenter/news/the-european-parliament-calls-for-reinforced-cyberdefense-in-europe/

https://www.roalddahl.com/shop/books/my-year-exclusive-museum-edition

https://www.npr.org/2018/07/18/629731693/fake-news-turns-deadly-in-india?t=1536657722588

https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

https://www.bleepingcomputer.com/news/government/us-charges-12-russian-intelligence-officers-for-hacking-dnc-running-dcleaks/

https://www.cloudav.ru/mediacenter/security/gdrp-facebook-fine/

https://www.cloudav.ru/mediacenter/security/danger-shipping-industry/

https://www.zdnet.com/article/microsoft-weve-just-messed-up-russian-plans-to-attack-us- 2018-midterm-elections/

https://threatpost.com/dangerous-pegasus-spyware-has-spread-to-45-countries/137506/

https://www.cloudav.ru/mediacenter/news/korean-hacker-charged-wannacry/

https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body

https://www.cloudav.ru/mediacenter/news/cyber-security-glitch-google-plus/

https://www.infosecurity-magazine.com/news/stuxnet-returns-striking-iran-with/

https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-black-friday-2018-data-breach-a8645306.html

4. Нарушения данных

https://www.pandasecurity.com/mediacenter/security/gdpr-is-here-what-now/

https://www.cloudav.ru/mediacenter/security/gdpr/

https://www.theguardian.com/technology/2018/jun/26/european-regulators-report-harp-rise-in-complaints-after-gdpr

https://www.itpro.co.uk/data-protection/28029/latest-gdpr-news-uk

https://www.cloudav.ru/mediacenter/security/gdrp-facebook-fine/

https://www.cloudav.ru/mediacenter/news/facebook-minimize-risks-vulnerabilities/

https://www.bbc.com/news/technology-46065796

https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/

https://www.wired.com/story/exactis-database-leak-340-million-records

https://www.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUSKCN1MJ2AY

https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach. html

https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/

https://threatpost.com/up-to-35-million-2018-voter-records-for-sale-on-hacking-forum/138295/

https://www.cloudav.ru/mediacenter/news/british-airways-hacked/

https://www.cnet.com/news/possible-orbitz-data-security-breach-affects-880000-payment-cards/

5. Прогнозы ИБ на 2019 год

https://thehackernews.com/2018/06/ticketmaster-data-breach.html

https://www.bloomberg.com/news/articles/2018-06-28/adidas-says-millions-of-u-s-customers-being-alerted-of-breach

https://www.theverge.com/2018/8/24/17776836/tmobile-hack-data-breach-personal-information-two-million-customers

https://www.zdnet.com/article/singapore-suffers-most-serious-data-breach-affecting-1-5m-healthcare-patients-including-prime/

https://www.businessinsider.es/timehop-breach-21-million-users-2018-7?r=US&IR=T

https://www.wired.co.uk/article/google-france-silicon-valley

https://boingboing.net/2018/11/26/candy-from-strangers.html

https://www.zdnet.com/article/researchers-discover-seven-new-meltdown-and-spectre-attacks/

https://en.wikipedia.org/wiki/VPNFilter

panda

pandalabs