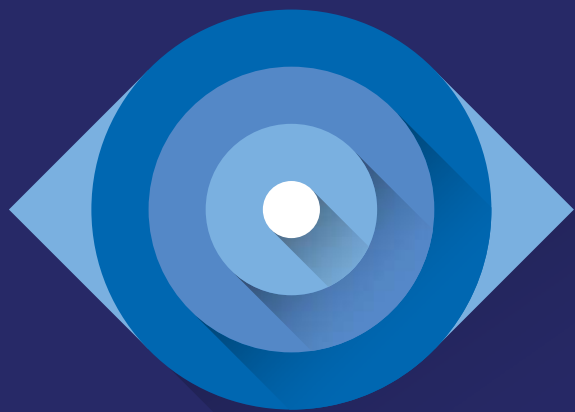

ОТЧЕТ PANDALABS 2 квартал 2017



1. Введение

2. Квартал
в цифрах

3. Взгляд на
квартал

Шифровальщики

Кибер-войны

Кибер-преступления

Мобильные устройства

Интернет вещей

4. Заключение

5. Рекомендации

6. О PandaLabs

1. ВВЕДЕНИЕ

1

Введение

С точки зрения информационной безопасности второй квартал 2017 года стал одним из самых ужасных за всю историю. Без преувеличения, атака WannaCry в мае и атака GoldenEye/Petya в июне были вне конкуренции, т.к. от них пострадали почти все страны мира и огромное множество компаний, ряд из которых восстанавливают свои системы до сих пор. По разным оценкам, общий ущерб от этих атак составил от 1 до 4 млрд. долларов.

Эти атаки тесно связаны с кибер-войнами и усилиями различных стран по борьбе с ними. Обе атаки воспользовались уязвимостью, обнаруженной АНБ, которая была украдена группой хакеров Shadow Brokers и опубликована в апреле. Существует ряд доказательств, которые указывают на КНДР как источника атаки WannaCry, в то время как, по мнению многих экспертов, атака GoldenEye/Petya была направлена на срыв работы компаний и учреждений на Украине за день до их Дня конституции, причем они предполагают, что за этой атакой стояла Россия.

Пока мы не можем официально сказать, что уже ведется глобальная кибер-война, однако тем или иным образом атаки, подобные WannaCry или Petya, затрагивают каждого из нас. На фоне шума об этих двух заметных атаках, **другие атаки спокойно проходят без должного внимания.** Но это не просто серьезные атаки, а, возможно, даже более опасные инциденты. **Дерзкие попытки повлиять на выборы в таких странах как Франция и США, используя тактики кибер-шпионажа** в пользу кандидатов, чьи политические взгляды совпадают с целями авторов атак (как это было в случае с Трампом в США и Ле Пен во Франции), - вот яркие примеры скрытых войн, которые осуществляются в кибер-пространстве и способны заметно повлиять на события в мире.

Между тем, рядовые граждане ежедневно сталкиваются с многочисленными кибер-преступлениями, в результате которых злоумышленники делают огромные прибыли за счет своих жертв.

2. КВАРТАЛ В ЦИФРАХ

2

Квартал в цифрах

В наших отчетах, как и в тех, что публикуют другие разработчики решений безопасности, мы всегда предоставляем схожие статистические данные по вредоносным программам: сколько новых угроз появилось в отчетном периоде времени, какие типы угроз и т.д. Хотя эти цифры интересны и могут стать ярким заголовком для новостей, в этом году мы в PandaLabs решили пойти дальше и показать данные, которые несут новый смысл и имеют реальную ценность.

Чтобы посчитать статистику, представленную ниже, мы решили не считать все угрозы, которые обнаруживаются 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.

Мы будем учитывать только данные по новым угрозам, не обнаруживаемым сигнатурами и эвристикой: вредоносные атаки, безфайловые атаки и другие атаки, выполненные с использованием легитимных системных инструментов, что становится все более распространенной практикой в корпоративных средах, как мы могли наблюдать в случаях с GoldenEye/Petya в июне.

Но как мы будем измерять то, что мы не можем обнаружить?

Дело в том, что фактически мы можем обнаруживать и останавливать такие атаки, даже если они никогда ранее не были замечены сигнатурами или эвристикой. Для этого мы используем набор собственных технологий, формирующий то, что мы называем "Контекстный интеллект", который позволяет нам выявлять вредоносные модели поведения и создавать улучшенные механизмы по кибер-защите от известных и неизвестных угроз.

Технология Контекстного интеллекта помогла нам достичь выдающихся уровней обнаружения в тестах, имитирующих атаки, происходящие в реальном мире. В тестах AV-Comparatives в первом полугодии 2017 года Panda Security показала наилучшие результаты в Real-World Protection Test, получив самую высокую награду "Advanced+" с помощью нашего Panda Free Antivirus - самого простого решения в нашей линейке решений информационной безопасности.

Далее, мы проанализировали полученные данные об атаках. Из всех машин, которые были защищены решениями Panda Security, **3,44%** из них были атакованы неизвестными угрозами, что выше почти на 40% по сравнению с предыдущим кварталом. Если мы посмотрим на тип клиента, то среди домашних пользователей и малых предприятий таких машин было порядка **3,81%**, в то время как среди средних и крупных предприятий - около **2,28%**.

Домашние пользователи имеют гораздо меньше средств защиты, в результате чего они более подвержены атакам. Многие атаки, которые успешно были реализованы дома, были легко предотвращены в корпоративных сетях прежде, чем они смогли оказать какое-то влияние.

Среди наших корпоративных клиентов есть те, кто используют традиционные решения, а также те, кто выбрал наше EDR-решение (Adaptive Defense), который далеко выходит за пределы антивируса и предлагает дополнительные функции, существенно

расширяя уровни защиты, классифицируя угрозы и осуществляя в реальном времени мониторинг всех процессов, запущенных на серверах и рабочих станциях, а также предоставляя экспертный анализ и пр. В результате этого количество атак, которые способны преодолеть все уровни защиты в EDR-решении Adaptive Defense, намного меньше соответствующего количества для только традиционных технологий безопасности.

2,67% устройств, защищенных традиционными решениями, столкнулись с неизвестными угрозами, в то время как таких устройств, защищенных с помощью Adaptive Defense, было всего **1,21%**, что показывает более высокие уровни предотвращения атак во времени.

Как же эти атаки распределены географически? Мы посчитали процент атакованных машин в каждой стране. Чем выше процент, тем выше вероятность быть атакованным с использованием неизвестных угроз в соответствующей стране.

Наиболее атакуемые страны

Сальвадор	10,85%
Бразилия	10,04%
Бангладеш	9,77%
Гондурас	9,44%
Россия	8,96%
Венесуэла	8,87%
Колумбия	8,29%
Пакистан	8,17%
Мексика	7,99%
Эквадор	7,67%

Менее атакуемые страны

Австрия	1,14%
Бельгия	1,06%
Германия	0,97%
Япония	0,90%
Нидерланды	0,87%
Дания	0,71%
Финляндия	0,64%
Словения	0,64%
Норвегия	0,47%
Швеция	0,42%

Полный список стран

Сальвадор	10,85%
Бразилия	10,04%
Бангладеш	9,77%
Гондурас	9,44%
Россия	8,96%
Венесуэла	8,87%
Колумбия	8,29%
Пакистан	8,17%
Мексика	7,99%
Эквадор	7,67%
Боливия	7,58%
Индонезия	7,57%
Тайвань	7,46%
Таиланд	7,30%
Иран	6,58%
Сингапур	6,30%

Перу	5,62%
Македония	5,59%
Турция	5,18%
Парагвай	5,11%
Гватемала	5,03%
Босния и Герцеговина	4,69%
Панама	4,62%
Латвия	4,40%
Аргентина	4,35%
Литва	4,18%
Сербия	4,10%
Болгария	4,03%
Чехия	4,00%
Уругвай	3,69%
Хорватия	3,65%
Гонконг	3,61%
Польша	3,61%
Чили	3,39%
Малайзия	3,39%
Италия	3,28%
Румыния	3,21%
Словакия	2,86%
Коста-Рика	2,25%
ЮАР	2,16%

США	1,99%
Канада	1,80%
Венгрия	1,71%
Греция	1,55%
Испания	1,50%
Франция	1,49%
Кипр	1,48%
Швейцария	1,44%
Португалия	1,41%
Великобритания	1,35%
Пуэрто-Рико	1,25%
Австрия	1,14%
Бельгия	1,06%
Германия	0,97%
Япония	0,90%
Нидерланды	0,87%
Дания	0,71%
Финляндия	0,64%
Словения	0,64%
Норвегия	0,47%
Швеция	0,42%

3. ВЗГЛЯД НА КВАРТАЛ

3

Взгляд на квартал

Этот квартал был четко отмечен двумя главными атаками. Первая атака WannaCry случилась в мае, и она устремилась во все корпоративные сети в каждом уголке нашей планеты.

WannaCry - одна из крупнейших атак в истории. Хотя в прошлом были атаки, когда количество жертв или скорость их распространения были выше (например, Blaster или SQL Slammer), но все же ущерб, вызванный теми атаками, остался в тени от их стремительного распространения. В случае же с WannaCry, мы говорим о шифровальщике с функциональностью червя, а это означает, что каждая зараженная сеть не смогла избежать шифрования. Учтите, что мы говорим о более чем 230 000 пораженных компьютеров, при этом ущерб составил от 1 до 4 миллиардов долларов США. Получается, средний ущерб составил от 4 300 до свыше 17 000 долларов в пересчете на каждый компьютер. Поэтому можно с уверенностью сказать, что это была самая разрушительная атака в истории.

Для получения подробного анализа того, что случилось, и необходимых рекомендаций, вы можете [посмотреть вебинар](#) про атаку WannaCry, который провел Технический директор PandaLabs Луис Корронс.

Вторая серьезная атака в этом квартале - это GoldenEye/Petya, своего рода остаточные толчки после землетрясения WannaCry. Несмотря на то, что большинство его жертв были сосредоточены в определенном регионе (особенно на Украине), тем не менее, **от нее пострадали компании из более чем 60 стран мира.**

Тщательно спланированная атака была проведена с использованием бухгалтерского ПО под названием MeDoc, очень популярного на Украине. Злоумышленники взломали сервер обновлений этой программы, а потому любой компьютер с установленной программой MeDoc, мог быть автоматически заражен при установке обновлений.

Эта атака была сложна и очень опасна. Здесь не только зашифрованные файлы, но также и главная загрузочная область в тех случаях, где подключенный пользователь имел права администратора. Сперва он показался таким же вымогателем, как и WannaCry, но после проведения тщательного анализа данной угрозы мы увидели, что авторы атаки не имели намерений разрешить восстановление зашифрованных данных.

Кажется очевидным, что в случае с GoldenEye/Petya мы столкнулись с направленной атакой, предназначенной для срыва работы компьютеров в компаниях и учреждениях Украины. Но как и в случае с оружием массового поражения, сопутствующий ущерб неизбежен. После проникновения GoldenEye/Petya в корпоративную сеть, он распространяется с использованием широкого набора эффективных техник. Иностранные компании с офисами на Украине также были заражены.

Через несколько дней после атаки правительство Украины открыто обвинило Россию в совершении нападения.

В презентации, которую Вы можете посмотреть [здесь](#), PandaLabs выполнила разбор ключевых моментов этой атаки и ее авторов.

Шифровальщики

WannaCry и GoldenEye/Petya отвлекли на себя все внимание общественности, **но была масса и других шифровальщиков**. Был атакован веб-хостинг Nayana в Южной Корее, где шифровальщики зашифровали данные на 153 серверах Linux.

Злоумышленники требовали выкуп в размере 1,62 млн. долларов США. Компания вела переговоры с преступниками и сократила эту цифру до 1 млн. долларов, выплатив ее в три платежа.

Кибер-войны

Две крупные атаки 2017 года породили подозрения, что за ними могут стоять правительства определенных стран (КНДР в случае с WannaCry и Россия в случае с GoldenEye/Petya). Но это только всего лишь два случая в море более или менее таинственных войн, которые происходят в кибер-пространстве.

Основные игроки в этой игре кибер-войн - это обычные подозреваемые: США, Россия, КНДР... но удивительно, что Китай за последние несколько месяцев как-то выпал из этого списка, т.к. он не был вовлечен во все эти скандалы. Единственным объяснением этому может быть соглашение о кибер-безопасности, подписанное между США и Китаем в 2015 году, хотя вполне возможно, что они продолжают свои атаки, которые попросту еще не были выявлены.

США явно обеспокоены атаками на американские компании и учреждения. Самуил Лайлс, Исполнительный директор Кибер-дивизиона в Министерстве внутренней безопасности (DHS), свидетельствовал перед Комитетом по разведке Сената США о том, что хакерские атаки, поддерживаемые российским правительством, направлены на системы, связанные с президентскими выборами в более чем 21 штате.

Комитет по разведке Конгресса США провел слушания, чтобы обсудить последствия российских хакерских атак на президентские выборы 2016 года. Джек Джонсон, бывший секретарь Министерства внутренней безопасности в администрации Обамы, напомнил, что Президент России Владимир Путин отдал приказ о нападении **с целью повлиять на исход президентских выборов в США**. Он также утверждал, что с помощью данных атак хакеры не смогли сфальсифицировать результаты выборов.

В июне правительство США выпустило предупреждение, обвинив правительство КНДР в серии кибер-атак, проведенных с 2009 года, и предупредив о том, что в будущем могут быть совершены новые удары. Предупреждение, которое поступило от Министерства внутренней безопасности и ФБР, относилось к группе хакеров "Hidden Cobra", которые помимо всего прочего атаковали СМИ, аэрокосмическую и финансовую отрасли, а также критическую инфраструктуру в США и других странах мира.



Название "Hidden Cobra" не так известно, но эта группа известна также под названием "Lazarus Group," и она была связана с такими атаками, как взлом Sony в 2014 году.

Анализируя все данные и улики по деятельности Hidden Cobra/Lazarus Group, вы сможете прямиком выйти на саму WannaCry, делая по пути остановки на атаки финансовых учреждений, таких как атака на ЦБ Бангладеша.

Во время саммита Gartner Security & Risk Management, который состоялся в июне в Вашингтоне, бывший директор ЦРУ Джон Бреннан сказал, что предполагаемый союз между российским правительством и кибер-преступниками, которые осуществили кражу аккаунтов в Yahoo, - это всего лишь вершина айсберга, и что будущие кибер-атаки, осуществляемые правительствами, будут использовать эту формулу, и они станут более частыми.

В том же выступлении он заявил, что российские спецслужбы, на

деле, не контролируются законом, в то время как в США все наоборот. Кто-то может найти эти высказывания странными, т.к. всем известно (благодаря WikiLeaks), что на протяжении многих лет ЦРУ взламывала роутеры домашних, корпоративных и публичных Wi-Fi сетей для осуществления тайной слежки.

В нашем последнем отчете мы говорили о том, как Франция отказалась от использования электронных методов голосования для граждан, проживающих за рубежом, в силу "чрезмерно высокого" уровня риска кибер-атак. Оказалось, что была как минимум одна кибер-атака, и всего за пару дней до выборов была опубликована приватная информация, а Эммануэль Макрон быстро распространил пресс-релиз о том, что они были взломаны.

Более поздние исследования связали взлом с группой "Fancy Bear", предположительно поддерживаемой правительством РФ.

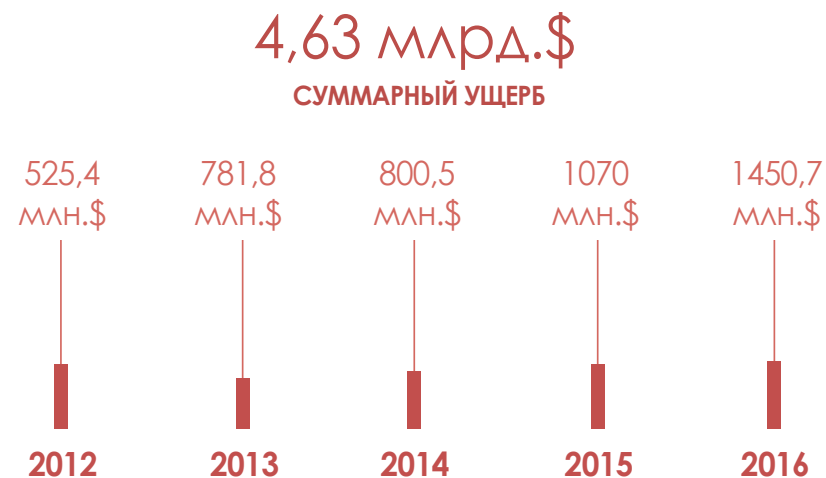
По информации от Financial Times, в отношении членов британского парламента были проведены попытки взлома их почтовых аккаунтов с помощью методов brute-force. В этой атаке также подозреваются хакеры, которые спонсировались иностранной державой.

Этот вихрь уловок и международных конфликтов затронул технологические компании. ФСБ России запросила у CISCO, SAP и IBM исходный код их решений безопасности, чтобы проверить возможные бэкдоры. Спустя несколько дней правительство США запретило всем федеральным ведомствам использовать решения Kaspersky из-за своей близости к российскому правительству и ФСБ.

Кибер-преступления

Согласно отчету 2016 Internet Crime Report, опубликованному IC3 (Центр обработки жалоб по Интернет-преступлениям, относится к ФБР США), **потери от кибер-преступлений выросли на 24% и превысили 1.3 млрд. долларов США.**

Мы должны иметь в виду, что IC3 учитывает только тот ущерб, о котором им было сообщено, но по их оценкам это всего лишь 15% от реальных суммарных потерь. Значит, в 2016 году только в США суммарный ущерб мог составить порядка 9 млрд. долларов.



Самые востребованные эксплойты используются для запуска атак "нулевого дня", которые по определению не известны производителю ПО и которые позволяют хакерам взламывать компьютеры, даже если их ПО обновлено. В апреле была обнаружена уязвимость, от которой пострадали различные версии Microsoft Word, и мы знаем, что она использовалась хакерами как

минимум с января. В том же апреле, Microsoft опубликовала соответствующее обновление для защиты пользователей Office.

Медицинские карты как минимум 7000 пациентов были скомпрометированы в результате нарушения безопасности в медицинском центре Bronx Lebanon Hospital Center в Нью-Йорке.

Были и другие инциденты безопасности, в которых злоумышленники не принимали непосредственного участия. В тех случаях, в результате технической ошибки или просто по неосторожности, данные, которые должны быть серьезно защищены, фактически стали доступны любому, кто хотел получить к ним доступ. Это случилось в **Автомобильной ассоциации Automobile Association (AA)**, которая в апреле на несколько дней оставила "в открытую" 13 ГБ данных, среди которых можно было найти свыше 100 000 адресов электронной почты, связанных с информацией по кредитным картам.

Похожий случай произошел в США на еще более высоком уровне. **Маркетинговые компании, которые были наняты Республиканской партией США, открыли публичный доступ к данным 198 миллионов избирателей** (всего в США чуть более 200 миллионов избирателей). Эти данные, которые были доступны пару дней, содержали подробную информацию о каждом избирателе: ФИО, дата рождения, адрес и пр.

В Китае незаконная торговля данными клиентов Apple закончилась арестом 22 человек. Все признаки указывают на инсайдеров, поскольку некоторые из задержанных работали в компаниях по субконтракту с Apple и имели доступ к данным, которые потом были проданы.

InterContinental Hotels Group (IHG) сообщила о том, что пала жертвой кражи данных, повлиявшей на ее клиентов. Хотя в феврале компания сообщила о том, что от атаки пострадало порядка десяти отелей, но теперь уже стало известно о заражении

POS-терминалов в более чем 1000 ее заведений. В своем заявлении компания подтвердила риски в отношении карт, которыми расплачивались в период с 29 сентября до 29 декабря 2016 года. В компании также пояснили, что не располагают информацией о несанкционированном доступе к платежной информации после 29 декабря, но и подтверждения о полном искоренении вредоносных программ не было до марта 2017 года. Среди различных пострадавших сетей отелей, которыми владеет данная группа компаний, оказались Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels и Crowne Plaza.

Сервис **OneLogin**, который предлагает пользователям единый вход на все платформы в облаке, обеспечивая более удобную и безопасную работу, по иронии судьбы также взломали. Компания сообщила в своем блоге, что она была атакована, а хакеры сумели проникнуть в их дата-центр в США, получив доступ к базам данных и оставив пользовательские информацию, приложения и пароли открытыми для хакеров.

Мобильные устройства

Начиная с 1 июня, Google стала предлагать более высокие вознаграждения тем, кто находит наиболее серьезные и ранее не обнаруженные уязвимости безопасности в их продуктах. Первое вознаграждение возросло с 50 000 до 200 000 долларов, а второе - с 30 000 до 150 000.

Уязвимость (CVE-2017-6975) в прошивке чипов Broadcom Wi-Fi HardMAC SoC, которая проявляется при переподключении к Wi-Fi сети, вынудила Apple выпустить обновление iOS (10.3.1).

Впрочем, эта уязвимость влияет не только на iPhone и iPad, но также и на другие мобильные устройства (например, Samsung или Google Nexus), которые получили в апреле новое обновление безопасности для решения этой проблемы безопасности.



Интернет вещей

Нам стало очень комфортно жить во взаимосвязанном мире. Но получаемые удобства - это всего лишь одна сторона медали. Другая сторона связана с различными опасностями, например, такими как атака WannaCry, которая благодаря высокому развитию Интернета и сетевых технологий оказала гораздо более серьезное влияние.

Смарт-города с гипервысокими уровнями сетевых соединений и состоящие из миллиона подключенных к Сети устройств являют собой наглядный пример внедрения технологий в нашу повседневную жизнь. Во всем мире города становятся все более "умными", и прогнозируется, что к 2020 году свыше 50 миллиардов устройств будет подключено к Интернету. Это значительно повысит риски безопасности, которые будут способны негативно отразиться на работе городской инфраструктуры, светофоров или городских систем водоснабжения. В июне WannaCry в Австралии заразил 55 камер, расположенных на светофорах и осуществляющих контроль скорости, после того как субподрядчик подключил зараженный компьютер к сети, в которой они были расположены. После этого инцидента полиция была вынуждена отменить 8000 выписанных штрафов.

7 апреля в 23:30 156 аварийных сирен одновременно зазвучали в Далласе (США, штат Техас). Официальным властям удалось их отключить только через 40 минут после перевода всей системы оповещения о чрезвычайных ситуациях в автономный режим работы (оффлайн). Следователи до сих пор не знают, кто стоял за данной атакой, которая привела к этому инциденту.

Недавно на свет появилась новая уязвимость, от которой пострадали автомобили Mazda. Впрочем, в отличие от других случаев, которые мы наблюдали в прошлом, чтобы взломать систему автомобиля, необходимо вставить "флэшку" во время работы двигателя в определенном режиме.



4. ЗАКЛЮЧЕНИЕ

4

Заключение

Группа хакеров "Shadow Brokers" планирует продолжить публикацию украденных в АНБ материалов, так что гонка кибер-армий будет только усиливаться. В связи с этим домашним и корпоративным пользователям необходимо будет предпринимать дополнительные меры безопасности.

Наибольший риск заражения существует у домашних пользователей и малых предприятий. Среди стран, которые в большей степени подвержены риску со стороны неизвестных угроз, - это Сальвадор, Бразилия, Бангладеш, Гондурас, Россия и Венесуэла.

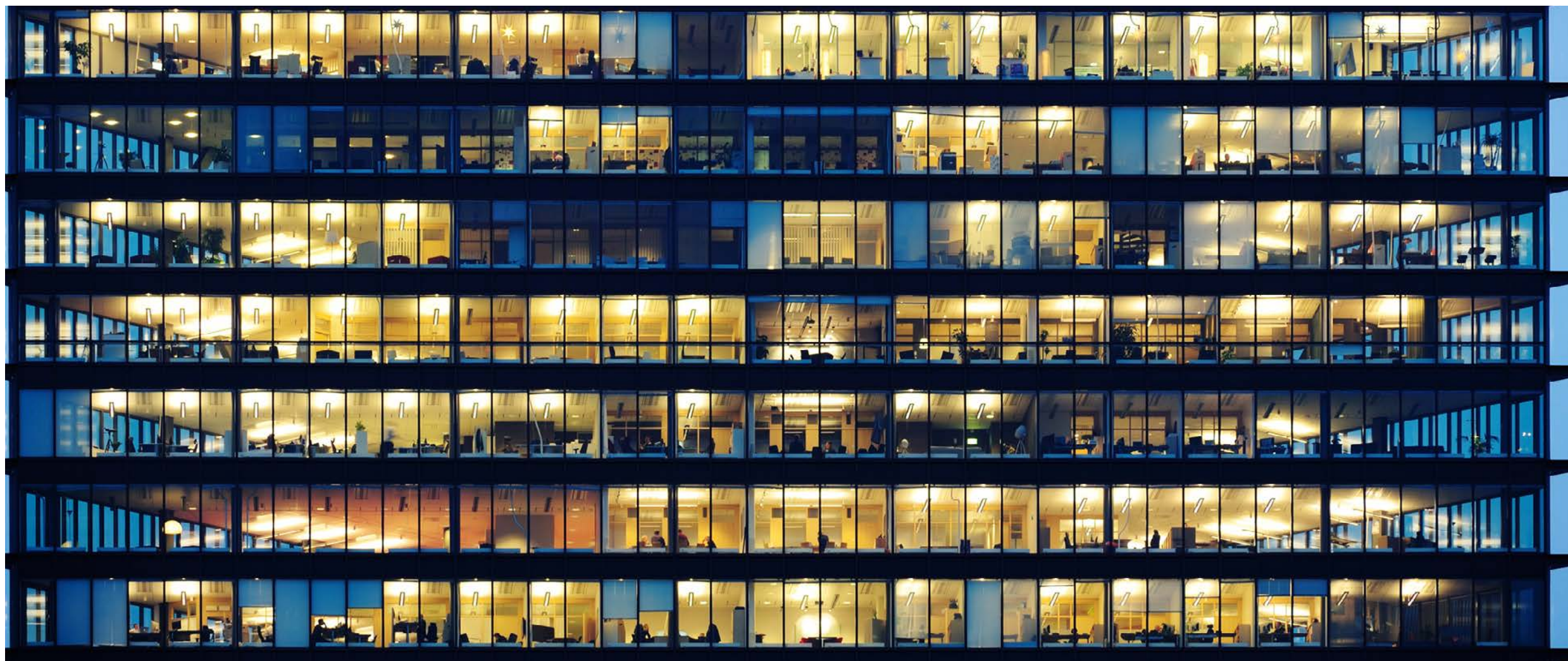
WannaCry и Petya показали нам, что правительства различных стран мира могут и не стесняться "нажимать на кнопку", когда необходимо запустить кибер-атаки. Каждый, кто пользуется Интернетом и подключенным к нему устройством, в конечном итоге может стать жертвой глобальной кибер-войны. Поэтому мы призываем все государства мира искать пути к заключению какого-то международного договора (некий аналог Женевской конвенции), чтобы ограничить возможности государств по совершению кибер-атак.

Атаки шифровальщиков по-прежнему на подъеме, и единственное этому объяснение заключается в том, что жертвы по-прежнему платят выкуп. Иначе атаки такого рода сошли бы на нет. От всех нас зависит, сможем ли мы положить конец этому безумию: с одной стороны, мы должны надежно защищать себя от угроз, чтобы не стать жертвой, а с другой стороны, - всегда иметь резервную копию наших данных, чтобы не пришлось платить выкуп.

Наиболее популярные эксплойты для запуска так называемых атак "нулевого дня" - это уязвимости, которые еще неизвестны производителям ПО. Инсайдерские атаки также представляют огромный риск для домашних и корпоративных пользователей, как и атаки на POS-терминалы.

Постоянный рост числа подключений к Интернету, начиная от мобильных устройств и заканчивая всеми типами устройств "Интернет вещей", значительно увеличивает количество атак до таких уровней, с которыми мы еще ни разу не сталкивались в прошлом.

Данная тенденция будет развиваться и далее, т.к. скоро уже десятки миллиардов устройств будут подключены к Интернету, причем это количество будет только увеличиваться.



05. РЕКОМЕНДАЦИИ

5

Рекомендации

Традиционные решения безопасности пока еще эффективны в защите от большинства вредоносных программ, но при этом они не способны бороться с атаками, которые используют невредоносные инструменты и другие передовые техники.

Надо использовать решения безопасности, адекватные уровню угроз, с которыми мы сталкиваемся. Такие EDR-решения (Endpoint Detection & Response, обнаружение атак на конечные устройства и реагирование на них), как Adaptive Defense, - это единственные решения, которые способны предоставить все необходимые инструменты для защиты от новых угроз и сложных атак.

Самая важная вещь при защите от атак - это наличие всей необходимой информации: что случилось, когда, как, была ли кража данных или нет и т.д. Используемое решение безопасности должно предоставлять все эти данные как в реальном времени, так и впоследствии, в результате чего можно выполнять тщательный анализ инцидентов. Это особенно важно и для соблюдения законодательства о защите персональных данных.

Также должен быть план действий на случай атаки. Рано или поздно, но каждый из нас может стать жертвой атаки, поэтому четкие действия могут значительно минимизировать ущерб.

Многие правительственные учреждения, частные компании и общественные организации в разных странах мира уже сделали ставку на предлагаемую нами стратегию, благодаря чему Adaptive Defense стал самым продаваемым решением безопасности в истории Panda Security. Крупные корпорации в различных секторах экономики (финансы, ИТ, вооружение, энергетика и пр.) защищают свои системы с помощью Adaptive Defense.

PandaLabs будет держать вас в курсе новостей из мира информационной безопасности в нашем Медиа-центре.

6. ○ PANDALABS

6

○ PandaLabs

PandaLabs - это антивирусная лаборатория и центр исследований и разработки компании Panda Security. Является мозговым центром компании относительно всего, что связано с вредоносными программами. Мы в PandaLabs:

- 🛡 Создаем автоматизированные системы, работающие в режиме реального времени, и постоянно предоставляем контрмеры, необходимые для защиты клиентов Panda Security во всем мире от всех типов вредоносного кода.
- 🔍 Отвечаем за выполнение тщательного анализа всех типов вредоносных программ с целью повышения уровня защиты, предлагаемой клиентам Panda Security, а также информируем общественность 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.

