Ноябрь, 2017

Отчет PandaLabs 2017 год

panda

pandalabs

Введение.

Луис Корронс
Технический директор антивирусной лаборатории PandaLabs

В самом сердце компании

В компании, которая занимается разработкой решений информационной безопасности, антивирусная лаборатория является ее мозгом. Именно отсюда координируется деятельность по исследованию угроз и техник по кибер-защите.

Мы несем на своих плечах весь груз ответственности по безопасности наших клиентов. Если кто-то из них будет заражен, то для нас это будет неудача. Хорошие новости заключаются в том, что **количество инцидентов с вредоносными программами, которые анализируются в PandaLabs, стремится к нулю**.

Один из способов оценки того, что мы действительно хорошо выполняем свою работу, - это анализ и оценка наших решений независимой тестовой лабораторией. В наши дни наиболее тщательное исследование, безусловно, осуществляется в рамках тестирования решений безопасности в реальных условиях (Real World Test) от компании AV-Comparatives. Этот тест присуждает самую высокую оценку за обнаружение угроз, и она была вручена нашим решениям:

В чем секрет?

В заключительной главе данного отчета я скажу об этом более подробно, но в целом секрет заключается в "забывании" о вредоносных программах. Если мы сфокусируемся на борьбе с вредоносными программами, то битва будет проиграна до ее начала.

Использование технологии Машинного обучения для защиты наших пользователей означает, что технические специалисты PandaLabs получают значительно больше времени и ресурсов для исследования непосредственно самих атак.

А это очень плохие новости для злоумышленников. Наша команда Threat Hunting анализирует и выслеживает аномальные шаблоны поведения, независимо от того, насколько невинными они могут показаться на первый взгляд. В результате мы смогли обнаружить огромное количество новых атак, о некоторых из которых мы расскажем в данном отчете.

Сочетание самых передовых технологий и управляемых сервисов позволяет нам классифицировать 100% активных процессов и четко знать, что происходит во время их выполнения. Неограниченная видимость и абсолютный контроль сводит степень воздействия любой угрозы до нуля.

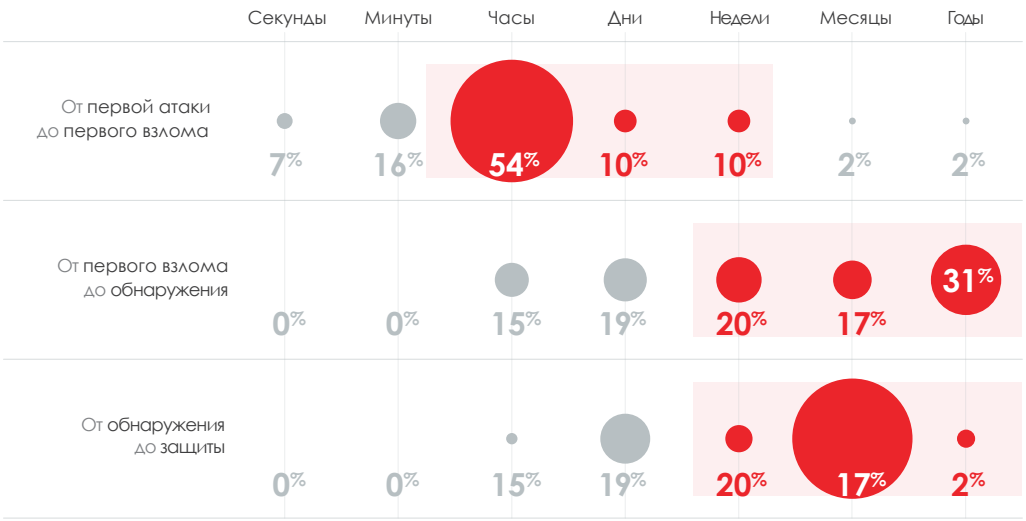
Эволюция атак.

В компаниях и банках произошло намного больше случаев ограблений, чем когда-либо в истории, но с той особенностью, что теперь злоумышленники могут находиться за тысячи километров от жертвы, никогда физически к ней не приближаясь.

Фактически, атакуемое устройство может и не иметь доступа к данным или ресурсам, интересующих кибер-преступников, потому что такое устройство может использоваться только лишь как точка запуска атаки.

Они будут использовать горизонтальное продвижение по корпоративной сети до тех пор, пока не найдут интересующие их данные или систему, которую они захотят вывести из строя.

Таким образом, эти новые техники для проникновения сквозь системы защиты и сокрытия вредоносных программ позволяют угрозам оставаться незамеченными в корпоративных сетях на протяжении долгих периодов времени.



Источник: DBIR 2016

Сейчас.

Кибер-преступность - это привлекательный и прибыльный бизнес. Злоумышленники используют все больше (и лучше) цифровых и финансовых ресурсов, что позволяет им разрабатывать все более изощренные атаки.

Почти каждый может запустить атаку благодаря более широкой доступности технологий, черному рынку и инструментам с открытым кодом. Как следствие, нам всем следует исходить из того, что любая компания может стать целью усовершенствованной атаки, для того чтобы начать работать над эффективными политиками и мерами безопасности. Наличие механизмов для обнаружения, блокировки и устранения любого типа современных угроз может защитить деньги вашей компании и ее репутацию.

Почти все эти преступления имеют экономическую основу: все это делается ради денег. Хакеров привлекают выгодные жертвы. Именно по этой причине мы должны предпринимать все возможные меры, чтобы усложнить им осуществление атаки и помешать им достичь своей цели, тем самым снизив их эффективность.

В большинстве случаев, когда атака становится сложной и злоумышленники не могут достичь своей финальной цели, им проще будет перейти к другой жертве, где они смогут быстрее и легче провести свою атаку и получить более высокий уровень окупаемости своих "инвестиций".

Чтобы дать Вам представление о сложности подобных атак, скажем, что техники взлома использовались в 62% случаев нарушений безопасности в компаниях. Фактически, **только в 51% случаев хакеры использовали вредоносные программы**. В остальных случаях они использовали другие инструменты, против которых большинство компаний не защищены.

В том случае, если ваша компания пала жертвой кибер-атаки, крайне важно иметь экспертную информацию о ней, чтобы знать, какие необходимо предпринимать соответствующие меры.

Также полезно знать, откуда началась атака, какие техники в ней использовались, какие продвижения были сделаны, как были преодолены средства защиты и пр.

Другие мотивирующие факторы.

В то время как большинство атак мотивированы финансово, все же существует небольшой процент атак, которые имеют совершенно другие цели.

В 2017 году мы видели атаку **Petya/GoldenEye**, направленную против украинских компаний. Мотив был политическим, а правительство Украины открыто обвинило российское правительство в том, что именно оно стояло за этими атаками.

Но это не единичный случай. Мы находимся в эпицентре гонки кибер-вооружений, при этом страны создают кибер-войска не только для ведения наступательных операций, но и в качестве ключевой инициативы по усилению защиты от внешних угроз.

Например, план по информационной безопасности, принятый при предыдущем Президенте США Бараке Обама, заставляет его преемника подготовить 100 000 новых экспертов по компьютерной безопасности к 2020 году. На самом деле, цель для 2018 года - иметь **133 команды для кибер-войск (Cyber Mission Force).**

Все страны считают приоритетной задачей включить кибер-войска в свои вооруженные силы в качестве еще одного оперативного подразделения. Действительно, такие подразделения зачастую имеют в своем распоряжении достаточно крупные бюджеты.

Глобальные инвестиции в кибер-войска

СТРАНА	ГОДОВОЙ БЮДЖЕТ, млн. $	ЧИСЛЕННОСТЬ КИБЕР-ВОЙСК
	7 000	9 000
	1 500	20 000
	450	2 000
	300	1 000
	250	1 000
	200	4 000

Источник: RBTH

Тенденции.

Зная своего врага.

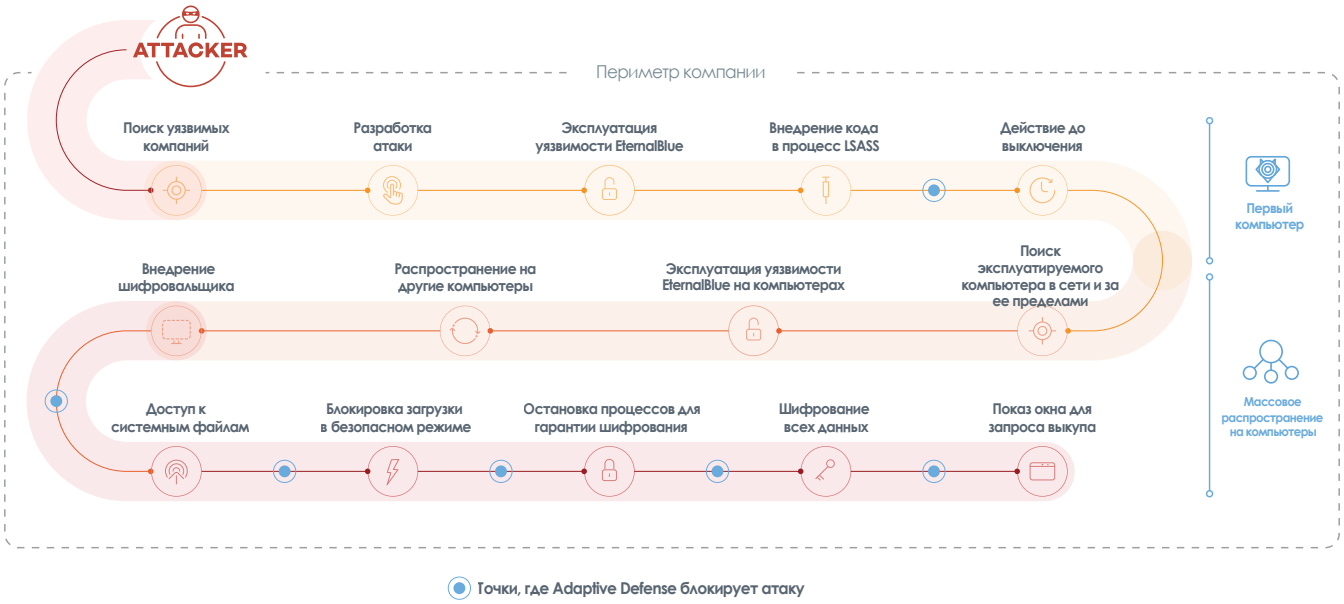
Новые векторы атаки помогают создавать все более сложные атаки. Кибер-преступники создают новые инструменты, чтобы использовать преимущества эксплойтов. Чтобы усложнить ситуацию, они больше не полагаются на взаимодействие с человеком для успеха своих атак.

Такой подход предполагает тщательное изучение своих жертв, их вооруженную реакцию на эксплуатацию весьма специфических дыр безопасности, а также подразумевает использование автоматического и стремительного распространения вредоносных программ без необходимости человеческого вмешательства.

Они в реальном времени взаимодействуют с сетью жертвы и ее решениями безопасности, адаптируясь к ее окружению для достижения своих целей.

Критически важно знать, с чем мы имеем дело.

Мы в Panda Security создали Cyber-Kill Chain, чтобы лучше визуализировать вещи с точки зрения злоумышленников, раскрывая различные шаги, которые они предпринимают с первого этапа и до момента достижения конечной цели:



Эта последовательность является отличным инструментом для понимания того, как компании могут значительно повысить свои возможности защиты, обнаруживая и блокируя угрозы на каждом этапе жизненного цикла атаки.

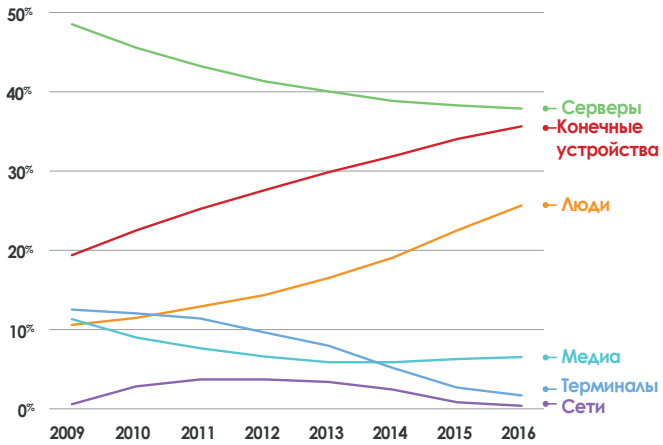
Cyber-Kill Chain показывает, что в то время как хакеры должны пройти полностью все эти фазы цепочки для достижения успеха, все, что нам необходимо сделать, - это "просто" остановить атаку на любом из этапов.

В данном **документе** мы предоставляем вам подробное объяснение каждого из разделов. Также вы можете посмотреть наше **видео**.

Цель - конечное устройство.

Стоит упомянуть один критический момент, если мы говорим об атаках. Во многих случаях поставщики решений безопасности тратят много времени, говоря о периметре сети, Интернете вещей и других векторах, которые необходимо защищать, но самое главное, что зачастую упускается из вида: само конечное устройство.

Почему это так важно? Если злоумышленники не могут добраться до конечного устройства, то они не смогут получить доступ к другим целям, извлечь информацию, собрать сетевые данные или развернуть новые атаки. Данная тенденция четко показана на следующем графике (доля инцидентов безопасности в зависимости от цели):



Источник: Verizon Data Breach Investigations Report.

Тем не менее, значительные средства в бюджетах компаний на безопасность выделяются на защиту периметра сети, **пренебрегая критически важной частью - конечным устройством**.

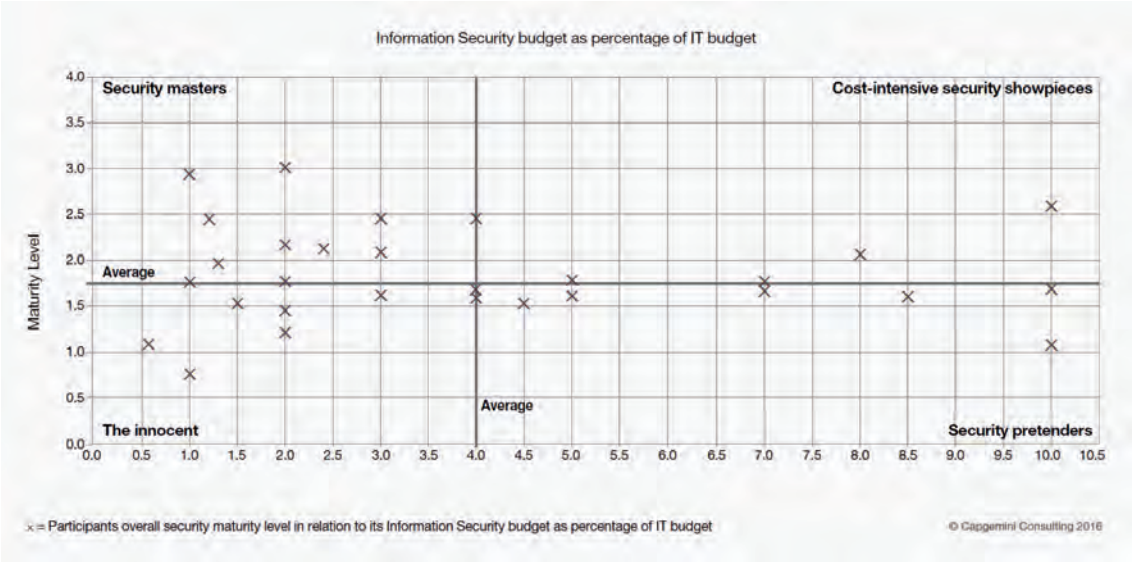
Это происходит не из-за невежества или небрежности. В прошлом фокусировка на периметре сети действительно имела смысл. Внутри корпоративной сети конечные устройства были в основном безопасными, поэтому приоритет был смещен на защиту от внешних атак, которые должны были преодолевать периметр.

ПРОДУКТЫ, млрд. $		СЕРВИСЫ, млрд. $	
Периметр	11,9	Консалтинг	21
Идентификация	4,6	Интеграция	20
Конечные устройства	3,8	SOC: • Профилактика • Обнаружение • Реагирование	20
Web	2,6		
Прочее	11,0		

Сегодня ситуация кардинально изменилась: периметр размыт, мобильность стала нормой в любой компании, а корпоративные сети подвергаются гораздо большему воздействию.

Злоумышленники чаще обращают свои взгляды на индивидуальные компьютеры, зная, что если они сумеют добраться хотя бы до одного из них, то вероятность того, что они смогут выполнить последующие действия до их обнаружения, становится очень высокой.

Таким образом, речь идет об установлении приоритетов, т.е. не о том, что требуется увеличить инвестирование, а о том, куда необходимо инвестировать. Это было продемонстрировано в исследовании Capgemini, в котором уровень инвестиций в безопасность сравнивался с уровнем фактической защиты корпоративных активов:



Цифры.

Одним из наиболее очевидных последствий профессионализации атак стал экспоненциальный рост количества вредоносных программ. По данным Verizon, только **число атак с участием шифровальщиков увеличилось почти на 50%**.

Это связано не только с тем, что выросло число атак (хотя это также верно). Преимущественно, это зависит от расширения набора техник, используемых кибер-преступниками.

Более 10 лет назад мы публиковали статью, где обсуждали данную тенденцию. В ретроспективном анализе мы посмотрели, что в 2002 году 10 наиболее распространенных угроз стали причиной 40% всех инфекций, а в 2006 году этот показатель уменьшился до 10%.

Какова ситуация в 2017 году?

Т.к. все наши решения взаимодействуют с нашим облаком, мы имеем все данные для анализа того, стала ли эта тенденция более ярко выраженной.

Чтобы рассчитать показатели, мы взяли все вредоносные программы (PE-файлы), которые мы не встречали до 1 января 2017 года. По состоянию на 20 сентября 2017 мы получили **15 107 232 различных вредоносных файлов**. И это только те, которые мы никогда ранее не встречали. Общее количество созданных вредоносных программ значительно выше, поскольку сюда надо добавить еще все типы файлов (скрипты, документы и пр.), а также и те, что хоть и были только что созданы, но еще ни разу не пытались заразить наших клиентов. Фактическое количество должно составлять порядка **75 285 000 новых образцов вредоносных программ**.

Ниже представлены 10 образцов вредоносных программ, которые чаще всего фигурировали в нашем облаке:

№.	ДАТА	ТИП	НАЗВАНИЕ
1	15.08.17	Trj/HackCCleaner.A	HackCCleaner
2	05.01.17	Trj/CerberCrypto.A	Cerber
3	15.05.17	Trj/RansomCrypt.I	WannaCry
4	15.08.17	Trj/HackCCleaner.A	HackCCleaner
5	17.05.17	Trj/Agent.SM	Downloader
6	24.02.17	Trj/Genetic.gen	Bot
7	15.05.17	Trj/RansomCrypt.I	WannaCry
8	12.05.17	Trj/RansomCrypt.K	WannaCry
9	15.05.17	Trj/Agent.PS	Downloader
10	12.05.17	Trj/RansomCrypt.K	WannaCry

Логично, что в этой "десятке" мы видим файлы, связанные с наиболее серьезными случаями, произошедшими в 2017 году: например, WannaCry (3, 7, 9 и 10 места) и "бэкдорная" версия CCleaner (1 и 4 места). Остальные - загрузчики (трояны, использующиеся в качестве посредника для установки всех типов вредоносного ПО) и бот.

Из всех 15 107 232 образцов вредоносных программ, сколько из них мы видели только один раз? **99,10%, т.е. 14 972 010 образца**.

Если мы посмотрим на цифры с другого конца, мы увидим, что широко распространена лишь незначительная часть от общего количества угроз. Мы видели всего **989 вредоносных файлов, которые присутствовали более чем на 1000 компьютерах, т.е. всего 0,01%**.

Это подтверждает то, что мы уже знаем: за некоторыми исключениями (например, WannaCry или HackCCleaner), большинство вредоносных программ меняется при каждом новом заражении, поэтому каждый образец имеет очень ограниченное распространение.

Группируя их по семействам или типам, неудивительно, что заметно выделяются шифровальщики (ransomware), т.к. это один из самых прибыльных типов атак, следовательно, наиболее популярный (с каждым годом эта популярность только возрастает).

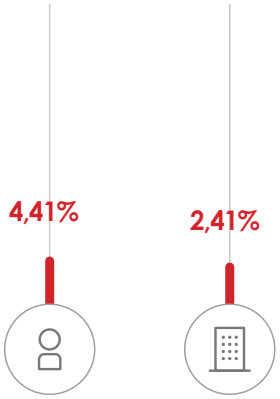
В любом случае, если мы хотим знать, с какими рисками заражения мы сталкиваемся, то общее количество новых образцов вредоносных программ является не настолько актуальным показателем в отличие от того, насколько часто мы можем сталкиваться с ними. Чтобы рассчитать этот показатель, мы измерили только те попытки заражения вредоносными программами, которые не обнаруживаются сигнатурами или эвристикой, включая вредоносные атаки, безфайловые атаки или такие атаки, в рамках которых используются вполне легитимные системные средства (это становится все более распространенным явлением в корпоративных средах, как мы видели это в случае с Goldeneye/Petya в июне).

Для измерений мы использовали данные, которые сбираются рядом наших собственных технологий, составляющие то, что мы называем "Контекстный интеллект". Он помогает нам выявлять закономерности вредоносного поведения и генерировать усовершенствованные действия по кибер-защите от известных и неизвестных угроз.

Затем мы приступили к анализу полученных данных по атакам.

Не все из нас имеют одинаковые средства защиты, т.к. домашние ПК или компьютеры в небольших компаниях чаще имеют базовый уровень защиты (подвержены большему риску), а средние и крупные компании имеют намного больше ресурсов, выделяемых для защиты данных.

В данном отчете мы будем учитывать только те атаки, которые прошли все уровни защиты, не были обнаружены и были остановлены в последний момент непосредственно перед компрометацией компьютера. Компании, которые выделяют больше средств на безопасность, должны иметь меньшее число таких атак - действительно, статистика эта подтверждает. **В то время как у домашних пользователей и малых компаний доля таких атак достигает 4,41%, в средних и крупных компаниях такой показатель падает до 2,41%.**



Хотя эти данные могут "успокоить" компании, мы же советуем не обманывать себя: чтобы причинить ущерб компании, злоумышленникам не обязательно атаковать все компьютеры в корпоративной сети. На самом деле, они будут атаковать небольшое число компьютеров, чтобы оставаться незамеченными, минимизировать риск обнаружения и достичь своих целей.

Географическое распределение атак.

Мы подсчитали процент машин, атакованных в каждой стране: чем выше процент, тем больше вероятность стать жертвой новых угроз при использовании компьютера в этой стране:

Иран	11,96%
Алжир	11,81%
Индия	10,96%
Египет	7,89%
Боливия	6,88%
Доминик. Респ.	6,88%
Пакистан	6,43%
ЮАР	6,30%
Малайзия	5,99%
Бангладеш	4,71%
Таиланд	4,59%
Индонезия	4,48%
Марокко	4,28%
Молдавия	4,22%
Бразилия	4,22%
Армения	4,14%
Сальвадор	3,98%
Парагвай	3,88%
Гондурас	3,82%
Казахстан	3,70%
Украина	3,63%
Венесуэла	3,55%
Уругвай	3,50%
Китай	3,42%
Тунис	3,42%
Гватемала	3,32%
Филлипины	3,29%
Сауд. Аравия	3,28%
Белоруссия	3,25%
ОАЭ	3,22%
Чили	2,98%
Колумбия	2,89%
Россия	2,86%
Вьетнам	2,82%
Эквадор	2,66%
Кипр	2,56%
Мексика	2,39%
Грузия	2,34%
Македония	2,14%
Бруней	2,14%
Тайвань	2,08%
Перу	2,07%
Сингапур	1,85%
Босния и Герцеговина	1,82%
Коста-Рико	1,82%
Болгария	1,81%
Турция	1,79%
Италия	1,71%
Панама	1,68%
Аргентина	1,63%
Португалия	1,58%
Ю. Корея	1,53%
Сербия	1,51%
Пуэрто-Рико	1,44%
Литва	1,42%
Латвия	1,39%
Великобритания	1,33%
Хорватия	1,30%
Ирландия	1,26%
Словакия	1,16%
Испания	1,14%
Эстония	1,09%
Германия	1,06%
Румыния	1,03%
Австрия	1,01%
Израиль	0,99%
США	0,99%
Норвегия	0,94%
Польша	0,94%
Франция	0,93%
Австралия	0,91%
Чехия	0,88%
Гонконг	0,86%
Венгрия	0,82%
Н. Зеландия	0,79%
Швейцария	0,78%
Мальта	0,77%
Швеция	0,75%
Дания	0,67%
Греция	0,64%
Япония	0,64%
Словения	0,62%
Канада	0,60%
Бельгия	0,54%
Нидерланды	0,53%
Финляндия	0,51%

Взгляд на 2017.

Отслеживание самых крупных атак 2017 года немного похоже на катание на американских горках: вы не можете видеть, что впереди, и вы не знаете, как высоко вы подниметесь или как сильно вы провалитесь, пока не проедете эти участки. Но несмотря на эту неопределенность, в одном можно быть точно уверенным: вы никогда не видели ничего подобного, и вы не сможете легко забыть об этом.

Equifax, CCleaner, Sabre, WPA2, Vault7, CIA, KRACK, NSA, Election Hacking... - вот лишь некоторые из них, которые мы проанализируем ниже. Они являются причиной массовых заражений, краж данных, атак шифровальщиков, взломанных приложений, кибер-войн, направленных атак против крупных корпораций, и уязвимостей, поразивших миллиарды устройств.

Но есть две атаки, которые сильно выделяются на фоне других за счет степени воздействия и уровня причиненного ущерба: WannaCry и GoldenEye/ Petya.

WannaCry появился в мае 2017 года, посеяв хаос в корпоративных сетях и распространившись по всему миру, став одной из самых серьезных атак за всю историю. Хотя по количеству жертв и скорости распространения мы видели в прошлом и более мощные атаки (например, Blaster или SQLSlammer), тем не менее, ущерб от предыдущих атак был вторичен по сравнению с уровнем их распространения. Однако в данном случае, будучи шифровальщиком с функциональностью сетевого червя, WannaCry блокировал и шифровал данные на каждом зараженном компьютере.

Луис Корронс, Технический директор PandaLabs, проводил вебинар, на котором детально анализировал все произошедшее и рассматривал меры, которые должны быть предприняты для защиты от других атак этого типа. Вы можете прослушать вебинар здесь.

Goldeneye/NotPetya стал второй наиболее заметной атакой 2017 года, словно **толчок во время землетрясения WannaCry**. Хотя его жертвы первоначально ограничивались определенной географической территорией (Украина), все же в конечном итоге от этой атаки пострадали компании из 60 стран мира.

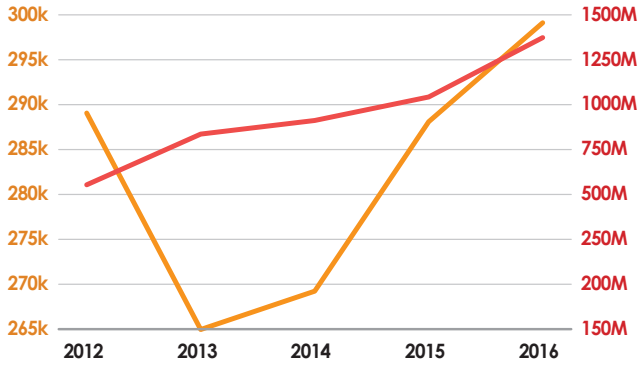
Тщательно спланированная атака была осуществлена через бухгалтерское приложение M.E.Doc, которое очень популярно среди компаний на Украине. Злоумышленники скомпрометировали сервер обновления этой программы, в результате чего все компьютеры, на которых была установлена программа M.E.Doc, автоматически могли быть заражены этим зловредом.

В дополнение к шифрованию файлов, если пользователь, под которым был запущен сеанс на компьютере, имеет права администратора, то зловред переходил в главную загрузочную область (MBR) жесткого диска. Сначала показалось, что это шифровальщик в стиле WannaCry, но после тщательного анализа стало ясно, что хакеры на самом деле и не планировали предоставлять возможность для восстановления файлов. Спустя несколько дней, правительство Украины открыто обвинило Россию в причастности к атаке.

Луис Корронс также рассказал об этой атаке и ее авторах на своем вебинаре, который вы можете прослушать здесь.

Кибер-преступления.

Согласно отчету об интернет-преступлениях "2016 Internet Crime Report", опубликованному Центром рассмотрения жалоб по фактам совершения преступлений в Интернете (известный как IC3), созданным ФБР США, **ущерб, причиненный кибер-преступлениями, вырос на 24%, достигнув отметки в 1,3 млрд. долларов США**. Следует отметить, что речь идет только о сумме, о которой сообщили в IC3 жертвы из США, что по оценке Центра составляет всего 15% от числа всех инцидентов. Так что реальный ущерб только в США может достигать **9 млпд. долларов США только в течение 2016 года**.



Самые привлекательные эксплойты для запуска атак - это известные как эксплойты "нулевого дня", т.к. они неизвестны производителям ПО и позволяют хакерам компрометировать пользователей, несмотря на то, что их ПО полностью обновлено.

В апреле 2017 года была обнаружена уязвимость нулевого дня, которая влияла на некоторые версии Microsoft Word, и тогда же стало известно, что она использовалась хакерами как минимум с января. В том же месяце Microsoft выпустила требуемое обновление для пользователей Office.

RDPPatcher демонстрирует возрастающий уровень профессионализма кибер-преступлений. Эта атака, обнаруженная лабораторией PandaLabs, готовит компьютер своей жертвы для "сдачи в аренду" на черном рынке.

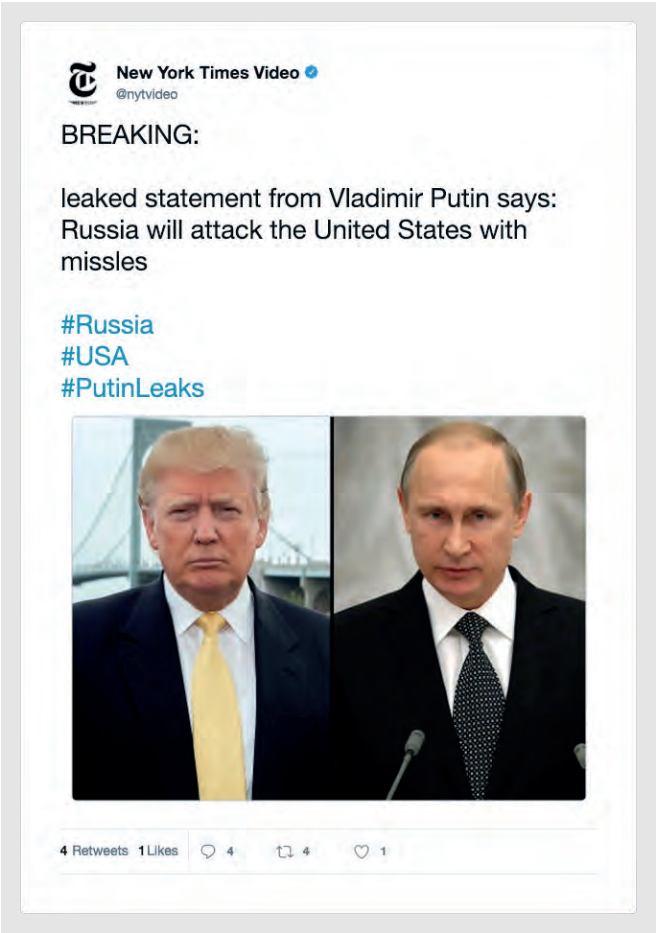
Кибер-преступники делают все возможное, чтобы избежать обнаружения, а самый эффективный метод для этого - не использовать вредоносное ПО. Поэтому атаки, не использующие вредоносные программы, стали весьма популярны. В случае, обнаруженном лабораторией PandaLabs, хакеры на компьютере оставили внедренный ими открытый backdoor, который позже они использовали для доступа к устройству без необходимости установки вредоносного ПО и с помощью опции **залипания клавиш**.

Во второй половине 2016 года мы видели несколько **DDoS-атак**, о которых много говорили в СМИ, а в 2017 году их стало еще больше, хотя они не были настолько мощными. Например, клиенты банка Lloyds имели проблемы с доступом к своему онлайн-банку в результате DDoS-атаки, от которой пострадали их серверы.

Итальянская полиция вскрыла кибер-шпионскую сеть, получившую название Eye Pyramid, организованную в январе 2017 года двумя гражданами Италии (они были родственниками) для шпионажа за учреждениями и органами власти, предприятиями, бизнесменами и политиками.

Взлом аккаунтов в соцсетях стал обычным явлением, и один из самых ярких случаев произошел в январе с официальным аккаунтом New York Times в Twitter, который был взломан. Как только они восстановили контроль над своим аккаунтом, они удалили твиты, размещенные хакерами:

Вот пример одного из твитов, который был опубликован на взломанном аккаунте. В нем утверждается, что Россия планирует запустить атаку против США:



Та же группа хакеров взломала аккаунты других компаний, таких как Netflix и Marvel.

Группа кибер-преступников, известная как "**Turkish Crime Family**", шантажировала Apple, требуя выкуп под угрозой уничтожения данных на устройствах iPhone, iPad и Mac, принадлежащих 250 миллионам пользователей. Apple не стала поддаваться на шантаж.

Кражи корпоративных данных.

В 2017 году инциденты с кражами данных также мелькали в новостных заголовках. Возможно, самая ироничная история года случилась с израильской компанией Cellebrite, которая предлагает сервисы по взлому телефонов, в частности, для извлечения данных с мобильных устройств. Так вот эта компания была взломана, в результате чего у нее было украдено 900 ГБ данных, включая клиентскую базу, базы данных, а также техническую информацию о продуктах компании.

Медицинские карты как минимум 7 000 людей были скомпрометированы в результате инцидента безопасности в медицинском центре Bronx Lebanon Hospital Center в Нью-Йорке (США).

Другой тип инцидентов безопасности, в которые не вовлечены злоумышленники, связан с ошибкой или небрежностью, в результате чего данные, которые должны быть надежно защищены, становятся достоянием общественности. Это случилось в США, когда маркетинговые компании, нанятые Республиканской партией, случайно оставили доступными для всех **данные 198 миллионов зарегистрированных избирателей** (почти все их зарегистрированные избиратели).

Dow Jones случайно разрешил доступ к данным 2 миллионов своих пользователей через облачный сервис Amazon в результате конфигурационной ошибки. В этих данных можно было найти имена пользователей, их адреса электронной почты, а также номера банковских карт.

22 были арестованы в Китае за торговлю данными клиентов Apple. Все доказательства указывали на факт инсайдерства, т.к. некоторые из задержанных работали в компаниях, являющимися партнерами Apple и имеющие доступ к этим данным.

В этом году HBO пал жертвой нескольких кибер-атак. В одной из них были взломаны серверы компании, после чего с них были украдены **эпизоды** еще не показанных серий, а также ряд внутренних корпоративных данных.

InterContinental Hotels Group (IHG) пала жертвой атаки, в результате которой были украдены данные их клиентов. Хотя компания заявила в феврале, что атака затронула только около десятка отелей, однако с тех пор стало известно, что были **заражены POS-терминалы в более чем 1000 принадлежащих им заведений**. В состав этой группы входят различные гостиничные бренды, такие как Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels и Crowne Plaza.

Sabre Corporation - это североамериканская компания, которая управляет бронированием номеров в 100 000 отелях и билетов у более чем 70 авиакомпаний во всем мире. Хакеры получили регистрационные данные для доступа к одной из систем бронирования данной компании, после чего им стала доступна платежная информация и данные по бронированию.

Данная конкретная система управляет бронированием номеров для частных лиц и туристических агентств в 35 000 отелей и прочих мест временного проживания. **В результате атаки были скомпрометированы данные за 7 месяцев с 10 августа 2016 года до 9 марта 2017 года**.

В результате атаки на Sabre пострадал целый ряд гостиничных сетей, включая Four Season Hotels & Resorts, Trump Hotels, Kimpton Hotels & Restaurants, Red Lion Hotels Corporation, Hard Rock Hotels и Loews Hotels.

Taringa, популярная в Латинской Америке социальная сеть, пострадала от нарушения безопасности, в результате которой **была украдена информация о более чем 28 миллионах пользователей**, включая имена пользователей, адреса электронной почты и MD5-хэши паролей.

Но самое крупное нарушение безопасности в 2017 году (и самое ужасное в истории) могло случиться немного позже, когда **был скомпрометирован гигант кредитной отчетности Equifax**. В связи с характером предоставляемых услуг, компания располагает огромным объемом высоко конфиденциальной информации о миллионах людей, включая номера социальных страховок.

Атака была осуществлена с помощью уязвимости в Apache Struts на одном из серверов компании. Уязвимость (наряду с соответствующим обновлением, ее устраняющей) была опубликована 6 марта. Спустя несколько дней хакеры атаковали сервер компании, который пребывал во взломанном состоянии до конца июля, когда была обнаружена данная атака. В течение данного срока **были скомпрометированы данные порядка 200 миллионов людей**, 70% из которых являются гражданами США, а остальные - Великобритании и Канады. Позже список пострадавших стран пополнился Аргентиной, Бразилией, Уругваем, Перу, Парагваем, Эквадором и Чили.

Что еще хуже, позже выяснилось, что три топ-менеджера компании воспользовались тем временем, когда была обнаружена атака, и когда она стала известна общественности, продав свои акции компании на сумму в 1,8 миллиона долларов США. Глава службы безопасности компании был уволен, и только спустя месяц Руководитель Equifax с 2005 года Ричард Смит заявил о том, что он уходит в отставку.

Трояны.

После Goldeneye/Petya с атакой столкнулась компания **Netsarang**, в результате которой в версии пяти ее программ (Xmanager Enterprise 5.0, Xmanager 5.0, Xshell 5.0, Xftp 5.0 и Xlpd 5.0) через бэкдор был внедрен файл. Он имел действующую цифровую подпись компании, что означало полное проникновение хакеров в компанию на каждом ее уровне. А ведь среди клиентов этой компании имеются банки и энергетические компании.

Самый громкий случай с бэкдорами в ПО в 2017 году, несомненно, произошел с **CCleaner**. Скомпрометированные версии программы были установлены более чем у 2 миллионов пользователей. Взломанное ПО ожидало получения команд, и, вероятно, никогда не выполняло никаких вредоносных действий.

Впрочем, исследователи Cisco обнаружили, что хакеры имели список компаний, чьи компьютеры они хотели скомпрометировать. В их число входило 20 известных и крупных компаний, среди которых Samsung, Cisco, Sony, Intel и Microsoft.

Эти три атаки свидетельствуют о том, что за ними стояла очень профессиональная организация, и можно поверить в то, что они поддерживались правительствами каких-то стран. Кстати, **NATO заявляло**, что за атакой GoldenEye/Petya также стояло правительство одной из стран.

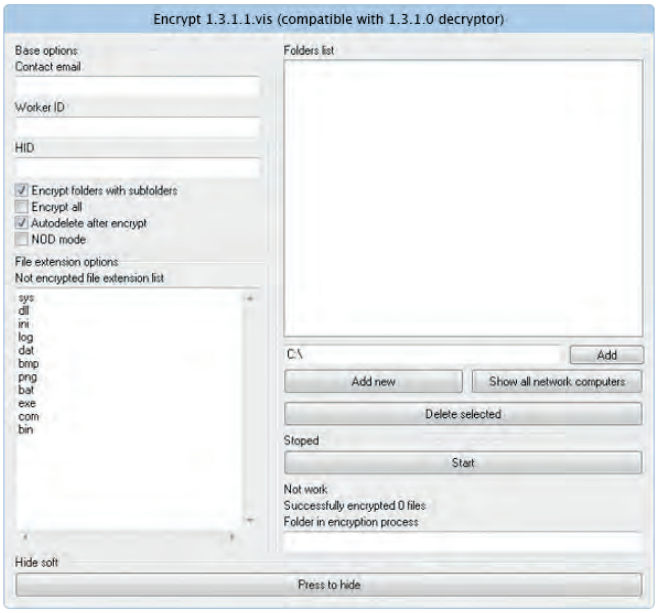
Глобальное влияние атак

Шифровальщики.

Число атак шифровальщиков по-прежнему растет, и это будет продолжаться до тех пор, пока компании готовы платить огромные выкупы за возвращение своих данных.

В дополнение к хорошо известным семействам шифровальщиков (Locky, Cerber и др.), есть специальные, более персонализированные версии для такого типа жертв, которые готовы платить.

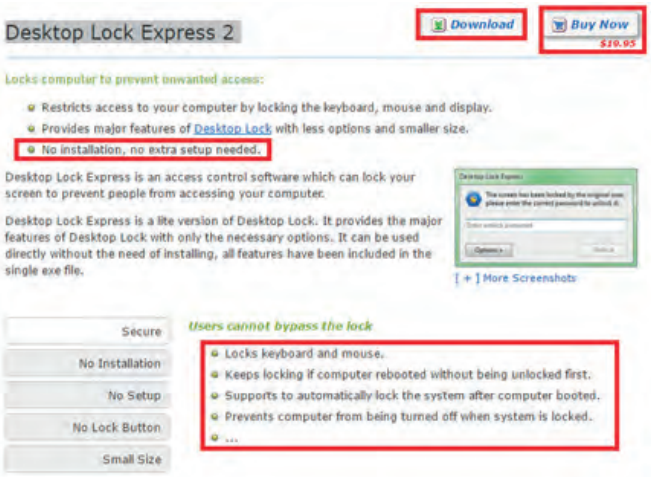
Один из них был обнаружен лабораторией PandaLabs - это шифровальщик со своим собственным "дружественным к пользователю" интерфейсом, получившим название WYSIWYE, который позволяет кибер-преступникам настраивать атаку перед ее запуском:



Один из самых популярных и наиболее простых методов проникновения в корпоративную сеть - это использование атаки типа brute-force через удаленный рабочий стол (RDP-протокол) в Windows. Злоумышленники сканируют Интернет, осуществляя поиск компьютеров, у которых активирован данный функционал, и после того как потенциальная жертва найдена, они запускают brute-force атаку до тех пор, пока не подберут правильные регистрационные данные.

В течение 2017 года мы видели многочисленные примеры атак такого типа, причем хакеры были преимущественно из России и действовали по аналогичной схеме: как только они получали доступ к компьютеру через RDP, они устанавливали ПО для майнинга биткоинов (как дополнение), а после этого шифровали файлы или блокировали доступ к компьютеру.

При этом они не всегда используют для этого вредоносные программы. Например, в одном из проанализированных нами случаев хакеры использовали коммерческое приложение "Desktop Lock Express 2" для блокировки компьютера:



Немедленные последствия атаки шифровальщика очевидны: вы теряете доступ к вашим файлам. Однако случаи цифрового "киднеппинга" могут выйти далеко за рамки этого. Как в одном случае с **отелем в Австрии**, где постояльцы отеля оказались запертыми в своих номерах после того как кибер-преступники отключили ПО для электронных замков.

Один шифровальщик зашифровал данные на 153 серверах Linux, принадлежащих веб-хостинговой компании Nayana из Южной Кореи. **Хакеры запросили выкуп размером 1,62 миллиона долларов США**. Компания договорилась с преступниками и снизила сумму до 1 миллиона, которые должны были быть выплачены в три платежа.

Интернет вещей (IoT).

В течение многих лет было много предупреждений об опасностях, связанных с устройствами Интернета вещей (IoT), в основном из-за того, что при создании многих таких устройств разработчики не уделяли должного внимания вопросам безопасности.

Также и потому, что эти устройства не имели Интернет-подключения, и, следовательно, не представляли особого риска, но после того как в них были реализованы опции подключения к Интернету, они стали уязвимы для атак.

Похоже, что к этим предупреждениям стали прислушиваться, а в США сенаторы от Демократической и Республиканской партий объединились, чтобы создать законы, которые частично исправляют эту ситуацию.

Идея состоит в том, чтобы среди прочих мер потребовать от производителей продуктов с опцией подключения к Интернету сделать их обновляемыми (для устранения дыр безопасности), запретить использование фиксированных паролей, а также предотвратить продажу продуктов с известными дырами безопасности.

Умные здания.

За последние годы многие здания претерпели изменения. Например, где-то были внедрены "**смарт-метры**" для контроля потребления энергии в домах и офисах. Помимо возможных негативных последствий со счетами за электроэнергию, о которых сообщают ассоциации по защите прав потребителей, существуют и другие, менее известные проблемы в сфере безопасности, связанные с широким распространением таких устройств.

Как объяснил исследователь Нетанел Рубин во время недавнего Chaos Communications Congress в Гамбурге (Германия), эти смарт-метры представляют угрозу на различных уровнях. Во-первых, т.к. они записывают все данные, связанные с потреблением энергии в домах и офисах, чтобы потом отправлять их в коммунальные службы, злоумышленник, который сумел получить контроль над таким устройством, сможет увидеть эту информацию и использовать ее в преступных целях.

Например, он мог бы увидеть, когда потребление минимально (т.е. помещения пусты), чтобы ограбить здание. Учитывая, что все электроприборы оставляют "след" в сети, он мог бы даже использовать эту информацию для обнаружения любых ценных приборов, которые можно было бы украсть.

Smart TV.

Еще более распространенное устройство - это Smart TV. Некоторые из них работают под управлением операционной системы Android, которая имеет свои плюсы и минусы. Об этом в Twitter писал Даррен Котон, ИТ-разработчик из США, после того как была совершена атака на телевизор его родственника. Как объяснил Котон, все это произошло после того как жертва установил со стороннего сайта приложение для просмотра фильмов в Интернете.

Телевизор представлял собой модель LG, выпущенную в 2014 году, которая работала на Google TV - специальная версия Android для телевизоров. Как только устройство было заражено, **вредоносное ПО запросило выкуп в размере 500 долларов за разблокировку экрана**. Причем требование было выполнено в виде уведомления от Министерства юстиции США.

Кроме того, наблюдаются и многие другие опасные атаки, которые могут указывать на происходящее в этой области. В феврале во время Семинара Европейского вещательного союза по вопросам информационной безопасности специалист по безопасности Рафаэль Шеель представил созданный им эксплойт. Он может позволить хакеру удаленно получить контроль над Smart TV, просто запустив атаку через TDT-сигнал.

Смарт-города.

В Австралии 55 видеокамер, установленных на светофорах и перекрестках, были взломаны после того, как субподрядчик подключил компьютер к сети, к которой они были подключены.

7 апреля в Далласе (Техас, США) 156 сирен оповещения о чрезвычайных ситуациях одновременно включились в 23:40. Чиновникам удалось их отключить примерно через 40 минут, но только после отключения всей системы оповещения. До сих пор неизвестно, кто был ответственен за атаку.

Автоиндустрия.

Поступали сообщения о новой уязвимости, влияющей на автомобили, особенно на Mazda. Тем не менее, в отличие от предыдущих случаев, чтобы скомпрометировать ИТ-систему автомобиля, хакер должен был бы вставить USB-устройство во время работы двигателя в определенном режиме.

Уже неудивительно, что автомобили и другие машины могут иметь Интернет-подключение и, соответственно, могут быть атакованы, существуют и другие цели в этом секторе. Например, автомойки. На конференции Black Hat в Лас-Вегасе (США) исследователи Билли Риос и Джонатан Баттс показали, как им удалось взломать автоматические автомойки, подключенные к Интернету. Они взломали систему таким образом, что могли бы физически атаковать автомобиль и его пассажиров.

Еще из автомобильного сектора: удаленно также могут быть взломаны сегвеи, в результате чего хакеры могут их контролировать удаленно. Исследователь IOActive Томас Килбрайд показал различные уязвимости и инциденты безопасности. Дело в том, что сегвеи не проверяют примененные обновления, а потому каждый мог бы в любое время обновить устройство вредоносной прошивкой, которая сделала бы все, что нужно хакеру.

Критическая инфраструктура.

Голландский исследователь Виллем Вестерхоф проанализировал трансформаторы, используемые в солнечных батареях для преобразования постоянного тока в переменный ток и для его поставки в сеть одной из лидирующих компаний данного сектора, SMA Solar Technologies.

Всего он раскрыл 21 уязвимость, которые могли бы позволить хакеру, скажем, контролировать объем электроэнергии, поставляемый в сеть. Такие уязвимости могут быть использованы удаленно через Интернет.

Злоумышленник, взломавший эти установки, мог бы нанести огромный ущерб. Более подробная информация доступна здесь.

Здравоохранение.

Взлом электросети, конечно, чрезвычайно серьезное преступление, которое может повлиять на жизнь многих людей, но это все же далеко до потенциальной опасности, когда хакер контролирует кардиостимулятор или медицинское оборудование в больнице, в результате чего, в худшем случае, он может удаленно убить людей, как показано в нашем отчете.

Управление по санитарному надзору за качеством пищевых продуктов и медикаментов при Министерстве здравоохранения и социальных служб США (FDA) предупредило почти полмиллиона пациентов, чтобы они посетили своего доктора для обновления прошивки различных моделей кардиостимуляторов Abbott.

Мобильные устройства.

Вредоносное ПО, разработанное специально для мобильных устройств, по-прежнему уступает вредоносному ПО, разработанному для ПК, но основные действия у него такие же.

Популярность шифровальщиков, которые дают кибер-преступникам прекрасные результаты, подтверждается еще и их нацеленностью на мобильные устройства.

Угрозы для мобильных устройств.

Charger, новая угроза для Android, - это хороший пример того, как развивается вредоносное ПО для мобильных устройств. **Charger крадет контактную информацию** и SMS-сообщения, блокирует терминал, запрашивая выкуп под угрозой продажи части вашей информации на черном рынке каждые 30 минут. Размер выкупа составляет 0,2 биткоина.

Большие компании озабочены этой проблемой, в результате чего появляются такие инициативы как Google Project Zero Contest, которые увеличивают награды для тех, кто найдет самые серьезные уязвимости нулевого дня (ранее не обнаруженные). Премия за первое место увеличилась с 50 000 до 200 000 долларов США, а второе - с 30 000 до 150 000 долларов США.

Уязвимости.

Уязвимость (CVE-2017-6975) в прошивке чипов Broadcom Wi-Fi HardMAC SoC заставила Apple срочно выпустить обновление iOS (10.3.1). Эта уязвимость, возникающая при повторном подключении к Wi-Fi, влияет не только на продукты Apple, но также и на мобильные устройства других производителей, таких как Samsung или Google, которые выпустили свои обновления в ответ на данную проблему в апреле 2017 г.

Но если существует уязвимость, которая серьезно выигрывает "битву", то ей должна стать KRACK, влияющая на протокол WPA2. Она относится не только к мобильным устройствам, т.к. она влияет на все типы устройств, где реализован WPA (ПК, роутеры и пр.), но все же стоит отметить, что в основном проблема касается пользователей мобильных устройств Android.

Проблема была обнаружена в 2016 году бельгийскими исследователями Мати Ванхофом и Франком Пессенсом, но она не была оглашена публично до октября 2017 года. Особенно уязвима для данной атаки одна из реализаций этого протокола с открытым кодом, "wpa_supplicant", используемая в Linux и Android.

После того как Google выпустит соответствующий патч безопасности для своей операционной системы, требуется, чтобы огромное количество производителей устройств внедрили новые обновления. Кроме того, в мире используются сотни миллионов устройств, которые уже не поддерживаются их производителями, и, следовательно, они никогда не получат требуемых обновлений. Эта проблема типична для данной экосистемы.

Кибер-войны.

Предположительно, две главные атаки года (WannaCry и **GoldenEye/Petya**) были совершены правительствами двух государств (КНДР в случае с WannaCry и Россия в случае с GoldenEye/Petya), хотя никаких доказательств тому нет. В любом случае, это всего лишь пара случаев в рамках ожесточенной и скрытно ведущейся кибер-войны.

Главные действующие лица все те же: США, Россия, КНДР, Китай и Иран, хотя в большинстве случаев невозможно быть уверенным в том, кто же на самом деле стоит за любой атакой, т.к. почти всегда злоумышленники проделывают качественную работу по "заметанию" всех своих следов, а иногда даже подставляют других преступников.

Кибер-атаки и политика сейчас переплетены больше, чем когда-либо ранее. После того, как мы "пережили" последние выборы Президента США, и перед уходом из Белого дома Обама обнародовал новые санкции против России, обвинив ее в том, что она организовала кибер-атаки против предвыборной кампании кандидата от Демпартии Хиллари Клинтон в пользу Дональда Трампа. В результате были высланы 35 российских дипломатов, а два принадлежащих России центра были закрыты.

Последствия этого ощущаются во всем мире. Франция отказалась от использования электронного голосования для граждан, проживающих за рубежом, по причине "чрезвычайно высокого риска" кибер-атак. В Нидерландах пошли еще дальше: они стали вручную проверять голоса в ночь после выборов и передавать результаты по телефону, чтобы избежать риска возможных кибер-атак.

В феврале Нидерланды также призвали создать международный альянс по кибер-защите в рамках НАТО, который будет иметь потенциал для обороны, контроля и осуществления мер реагирования на возрастающую угрозу кибер-атак.

Канцлер ФРГ Ангела Меркель в марте заявила, что защита национальной инфраструктуры от потенциальных кибер-атак станет одним из главных приоритетов Германии.

Вскоре после этого было сообщено о том, что **немецкая армия будет формировать свои кибер-войска** для усиления онлайн-обороны. Планируется набрать 260 сотрудников, причем это количество возрастет до 14 500 к 2021 году.

Никто кроме ЦРУ США не попал в центр внимания одного из самых новостных событий этого года в сфере кибер-шпионажа.

7 марта **WikiLeaks начал публиковать серию документов под названием “Vault 7”**, содержащих подробности техник и программных инструментов, используемых для проникновения на смартфоны, компьютеры и даже смарт-ТВ. WikiLeaks продолжает публиковать документы и посвятил утечкам отдельный раздел на своем **веб-сайте**.

Хорошие новости заключаются в том, что вы можете использовать эти обнародованные знания для своей более надежной защиты от таких угроз. Но проблема в том, что другие преступники могут изучить эти техники и использовать их для нарушения конфиденциальности граждан.

США явно обеспокоены атаками против американских учреждений. Комитет по разведке Конгресса США провел слушания о **последствиях атаки России на президентских выборах 2016**, где бывший секретарь Министерства внутренней безопасности США при администрации Обамы Джех Джонсон подтвердил, что Президент РФ Владимир Путин приказал атаковать с целью

повлиять на результаты выборов в США. Он также сказал, что Россия не смогла манипулировать голосами благодаря этим атакам.

В июне правительство США обвинило правительство КНДР в **серии кибер-атак, осуществленных с 2009 года**, и предупредило о высокой вероятности их продолжения.

Предупреждение от МВБ и ФБР относится к группе хакеров "Hidden Cobra", которые атаковали СМИ, аэрокосмический и финансовый секторы, а также критическую инфраструктуру в США и других странах. **Есть доказательства, связывающие недавнюю атаку WannaCry с этой группой** "Hidden Cobra", больше известной как "Lazarus Group".

Одним из возможных объяснений тому, что атаки приписываются КНДР, является расширение санкций против них со стороны ООН, заставляя их искать альтернативное финансирование.

Во время саммита Gartner Security and Risk Management, который прошел в Вашингтоне в июне 2017 года, бывший директор ЦРУ Джон Бреннан рассказал о предполагаемом **союзе между правительством России и кибер-преступниками** при краже данных с аккаунтов Yahoo. По словам Бреннана, это лишь верхушка айсберга. Он предупредил, что будущие кибер-атаки со стороны правительств ряда стран продолжат следовать этой формуле, а их периодичность будет лишь расти.

По данным Financial Times, аккаунты также были взломаны и у ряда членов британского парламента, которые также уверены в том, что эта атака была спонсирована из-за рубежа.

FINANCIAL TIMES

Cyber Warfare

British MPs targeted by hackers in co-ordinated attack

An armed police officer outside the Houses of Parliament © AFP

MAY 17, 2017 **Sam Jones**, Defence and Security Editor 5 comments

Этот вихрь политически мотивированных кибер-атак также влияет и на технологические компании. ФСБ России потребовала, чтобы такие компании как CISCO, SAP и IBM передали им исходный код своих решений безопасности для поиска возможных бэкдоров. Спустя несколько дней правительство США запретило всем федеральным ведомствам в стране использовать решения Kaspersky из-за близости к правительству России и ФСБ.

theguardian

US government bans agencies from using Kaspersky software over spying fears

Federal agencies have been barred from using cybersecurity software made by Kaspersky Lab over fears the firm has ties to state-sponsored spying programs

Хотя до сих пор не представлено каких-либо неоспоримых доказательств, подтверждающих злонамеренную деятельность со стороны Kaspersky, понятно, что в нынешней обстановке напряженности между двумя державами правительство США в любом случае было бы обеспокоено. США исходит из того, что данная компания расположена в стране, власть в которой они считают почти авторитарной. Они считают, что **правительство России может в любой момент дать Kaspersky задание использовать свое ПО для запуска атаки** или кражи информации в гипотетическом случае эскалации конфликта.

О системах Threat Hunting.

Инаки Урзай

Главный стратег по безопасности в Panda Security

Число экспертов по ИБ во всем мире растет в геометрической прогрессии. Рост, в основном, обусловлен действиями правительств разных стран, которым необходимо играть активную роль (по своей инициативе или в виде ответной реакции) в виртуальном конфликте, в котором никто не может оставаться в стороне. Правительства многих стран мира уже на протяжении некоторого времени создают специальные агентства по кибер-обороне: **в Германии недавно создан дивизион с более чем 13 000 кибер-солдат, свыше 100 000 агентов должно быть в США к 2020 году, в КНДР уже вроде бы их порядка 6 000**, а также подобные подразделения, по всей видимости, имеются в России, Китае, Великобритании, Франции, Испании, Израиле, Иране и других странах.

Кроме того, есть специалисты, работающие с производителями и поставщиками решений безопасности во всем мире. Все эти компании имеют экспертов по информационной безопасности во всех странах мира. И, наконец, существуют кибер-преступники, которые в результате бума роста числа экспертов по информационной безопасности и глобального интереса к этой сфере в состоянии гораздо проще и быстрее находить себе обученных специалистов.

Этот рост потенциала высококвалифицированных сотрудников создал среду, в которой возможно систематически обнаруживать уязвимости в ПО. Это также способствует развитию профессиональных инструментов для проведения атак (с улучшением их устойчивости и масштабируемости), не использующих вредоносные программы, осуществляемых преступниками и способных адаптироваться к среде жертвы с максимальной скоростью.

Как мы можем видеть с Panda Adaptive Defense, **атаки, основанные на вредоносных программах, могут прекрасно сдерживаться** с помощью решений, основанных на "строго позитивной" модели, созданной компанией Panda Security.

Когда все приложения, которые пытаются запуститься на компьютере, классифицированы, и разрешено запускаться только тем из них, которые действительно безопасны, **то исчезает "разрыв в обнаружении", характерный для традиционной антивирусной модели**. Вредоносные программы больше не могут прятаться в неизвестных файлах, которые игнорируются традиционными решениями безопасности.

Рынок уже не может позволить себе игнорировать способность этой модели безопасности предотвращать атаки, поэтому очевидно, что у этой модели будет расти доля рынка.

Поскольку этот подход заменяет традиционные антивирусные модели, злоумышленники будут адаптировать свои техники для его обхода. И в этом случае вполне возможно, что станут превалировать атаки, которые не основаны на использовании вредоносных программ.

Атаки, не использующие вредоносное ПО, характеризуются использованием инструментов, которые зачастую используются легитимными сетевыми администраторами: например, приложения для удаленной установки программ, резервного копирования данных и пр.

При таком подходе **хакеры выдают себя за администратора** после того, как они смогут получить его сетевые регистрационные данные, поэтому в глазах любого внешнего наблюдателя они будут выглядеть именно как законный сетевой администратор, выполняющий свою работу.

Т.к. не используется никакое вредоносное ПО, системы безопасности обязаны уметь идентифицировать такие типы атак на основе поведения сетевых пользователей. Технологии, способные решать такие задачи, подпадают под понятие **Threat Hunting**.

Платформы Threat Hunting должны быть способны, среди прочего, осуществлять мониторинг поведения компьютеров, запущенных на них приложений и, в особенной степени, их пользователей.

Для каждого из этих компонентов динамически должны быть определены типичные профили поведения, а затем, в режиме реального времени, они должны сопоставляться с тем, что происходит на самом деле, чтобы искоренить любое поведение, которое могло бы указывать на то, что кто-то украл регистрационные данные другого сотрудника и действует от его лица.

Говоря технически, процесс Threat Hunting основан на огромном пуле данных, описывающих все модели поведения контролируемых компонентов и обновляемом в реальном времени по мере возникновения новых событий. В этом контексте **используемая платформа должна быть способна исследовать этот огромный объем информации для разработки новых гипотез атак**, тестировать их в реальном времени на выборочных группах данных перед тем как активировать их в основном потоке данных, и генерировать модели, основанные на поиске аномалий профиля поведения. На этом этапе, **системы машинного обучения будут уделять повышенное внимание потенциальным инцидентам,** которые после срабатывания должны быть тщательно проанализированы с использованием удаленных инструментов экспертного анализа, интегрированных в платформу.

Такие инструменты позволят аналитикам запускать персонализированные проверки на пострадавших компьютерах, чтобы они могли "поставить" себя в любую точку времени в истории события на каждом компьютере или в активности каждого пользователя и реконструировать их шаги для подтверждения атаки.

В обозримом будущем **традиционные вредоносные программы в виде явно вредоносных специфических программ будут заменены операциями, выполняемыми без вредоносного ПО**, в которых злоумышленники узурпируют личность пользователей сети и будут выполнять требуемые им действия под видом, казалось бы, законных сетевых пользователей.

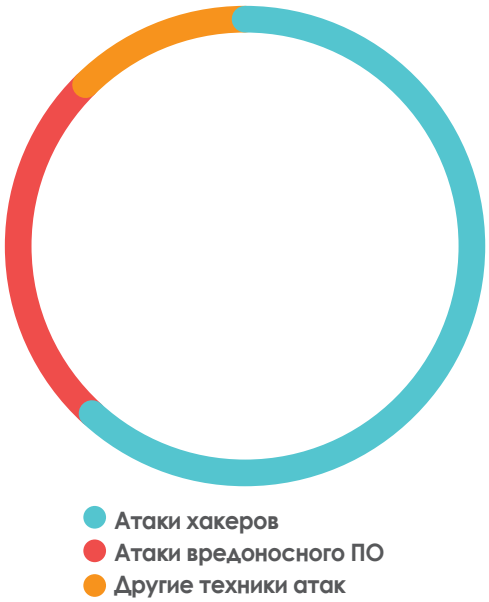
В этой связи крайне необходимо, чтобы решения безопасности, помимо предоставления возможностей по внедрению строго управляемых позитивных моделей, также предоставляли масштабируемые сервисы и платформы threat hunting.

Panda Adaptive Defense - это первое решение на рынке, которое сочетает в себе обе такие возможности: автоматизированный сервис Threat Hunting и инструменты в виде API и консолей, которые позволяют пользователям выполнять сканирование и рекогносцировку своих сетей с целью поиска хакеров, скрывающихся за учетными данными законных корпоративных пользователей.

Примеры атак.

Атаки стали более совершенными. Изменились цели. Техники стали изощренными, количество векторов атак увеличилось, а инструменты для их проведения стали более изысканными.

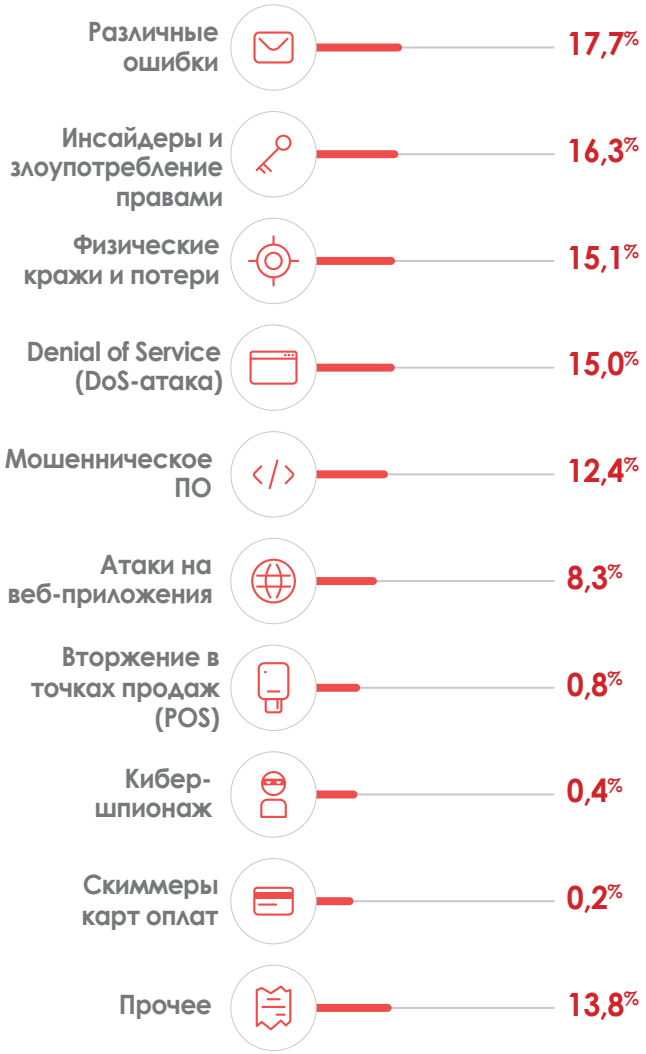
Злоумышленники тщательно изучают своих потенциальных жертв, чтобы лучше адаптировать стратегию своих атак для достижения максимально возможного результата. **За 62% угроз стоят хакеры,** которые активно занимаются анализом и адаптируют свои атаки соответствующим образом и с хирургической точностью.



Их действенность, эффективность и прибыльность постоянно подтверждаются. Только в 2017 году появилось до 100 000 новых дыр и инцидентов безопасности в корпоративных средах.

В рамках этого отчета мы увидели, как злоумышленники это делают и чего они достигают. При этом, кажется, что сейчас намного выше вероятность стать жертвой кибер-атаки. Частично это утверждение верно. И все же системы профилактики, обнаружения, реагирования и восстановления также стали намного более эффективными. Как в случае с Panda Adaptive Defense, они сочетают в себе решения и сервисы для **оптимизации защиты, уменьшения площади атаки и минимизации последствий от угроз**.

Благодаря этому развитию технологий, мы способны рассказать вам о ряде ситуаций, в которых Panda Security вовремя прервала атаку. Наши экспертные исследования сыграли тут решающую роль. Эти атаки демонстрируют развитие новых тенденций и методик нападений, подтверждая исследование Verizon, в котором утверждается, что **95% инцидентов безопасности может быть сведено к 9 моделям**.



Таким образом, мы также помогли улучшить протоколы и оборонительные структуры компаний, даже на рабочих станциях и системах, которые не имеют непосредственной защиты со стороны Panda Adaptive Defense.

Горизонтальные продвижения.

В качестве примера эволюции атак, мы начнем с представления скрытой атаки с адаптивными горизонтальными продвижениями. Такой тип атак становится очень распространенным. На этот раз компания имеет весь арсенал систем обнаружения и защиты (файервол, IPS, SoC, контроллеры доменов, прокси, традиционная защита и пр.)

Но ни одна система не заметила горизонтального продвижения, которое могло привести к успешной атаке на активы клиента.

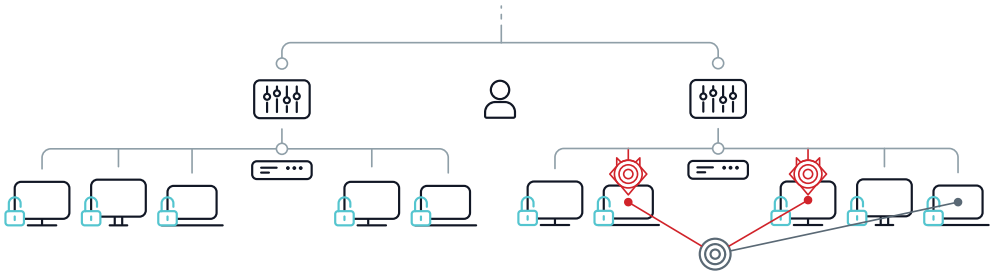
Впрочем, преступники не рассчитывали на то, что у компании был Adaptive Defense, который в действительности обнаружил их намерения и сорвал их планы атаки:

1 Вполне защищенная сеть

Окружение крупной компании из тысяч конечных устройств в двух доменах, несколько контроллеров доменов, файервол, IPS, антивирус и SoC. Внедрение Adaptive Defense началось на нескольких конечных устройствах в домене "B".

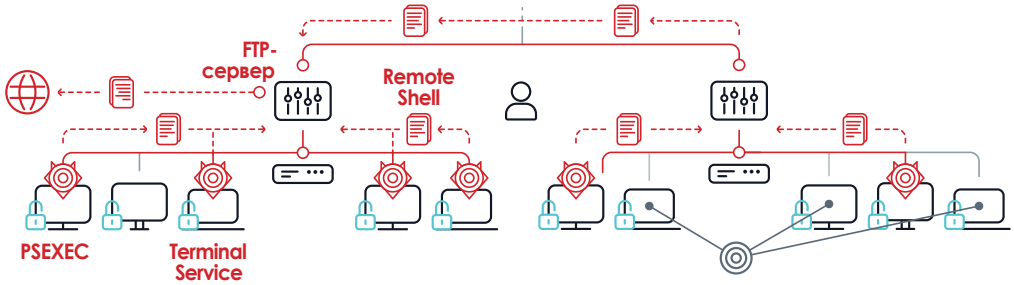
2 Модель безопасности Adaptive Defense

Блокирует ненадежные программы и отправляет телеметрию защищаемых конечных устройств для мгновенной обработки в облаке.



3 Threat Hunting и расследование

Сервисы и служба Threat Hunting при использовании ретроспективного анализа обнаружили, что кажущийся надежно защищенным сетевой домен "A" на самом деле был скомпрометирован, и определенные административные инструменты собирали и отправляли данные с конечных устройств в Малайзию.



Атака обнаружена командой Threat Hunting

Горизонтальные продвижения злоумышленников для получения контроля надо доменом "B" были обнаружены и пресечены решением Adaptive Defense до того, как он был скомпрометирован.

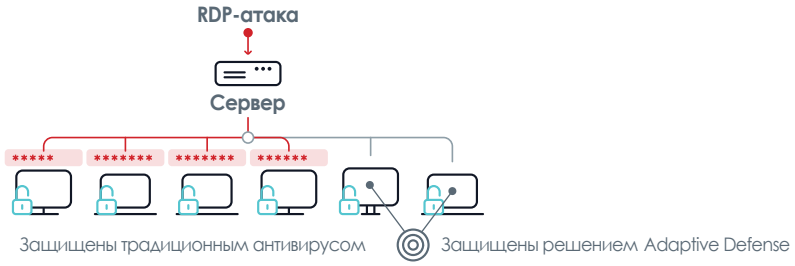
RDP: Атака без использования вредоносных программ.

Атака без использования вредоносных программ стала одной из любимых угроз кибер-преступников. **Только в 51% инцидентов безопасности, зарегистрированных в 2017 году, использовалась какая-нибудь вредоносная программа** в качестве атакующего маневра. Хакеры предпочитают оставаться незамеченными для традиционной защиты и не полагаться на взаимодействие с сотрудниками жертвы. В итоге, как показано в примере, они увеличивают свои прибыли за счет оптимизации эффекта атаки.

Как только потенциальные жертвы атаки локализованы, разворачивается **RDP-атака** для получения прибыли по двум направлениям: 1) генерация онлайн-трафика, который может быть продан сторонним веб-сайтам, или 2) продажа доступа к скомпрометированным машинам. Мы видели такие случаи с завидной периодичностью. Такие схемы можно суммировать в следующей инфографике:

1 Получение доступа и обеспечение живучести у жертвы

Хакер сканирует Интернет для поиска потенциальных жертв с включенной опцией удаленного рабочего стола. Когда они найдены, он использует атаку типа brute-force для входа в систему. Войдя в систему, он обеспечивает живучесть за счет изменения записи функции залипания клавиш в реестре. После активации этой функции (например, при нажатии клавиши CAPS 5 раз) он откроет бэкдор на компьютер жертвы, который позволит хакеру получать доступ к системе даже в том случае, если будут изменены регистрационные данные при подключении к удаленному рабочему столу.

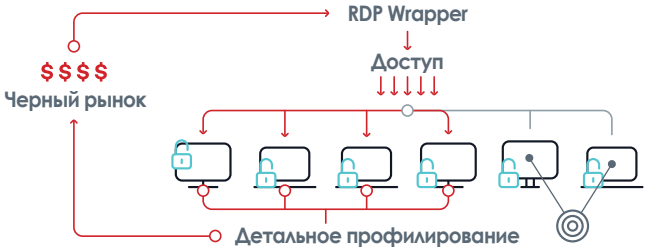


2.1 Монетизация взломанных устройств: генерация онлайн-трафика

Хакер скачивает "Traffic Spirit" - "законное" приложение для генерации трафика, которое используется для получения денег от наличия взломанных компьютеров. Это приложение в данной атаке не является вредоносной программой.

2.2 Монетизация взломанных устройств: продажа доступа к машинам

Как только хакеры получат доступ, они выполнят тщательное профилирование всех компьютеров. Затем они предложат на черном рынке доступ к этим машинам для различных целей (вымогательство, утечка данных, зомби, боты и пр.).



Атака обнаружена командой Threat Hunting

Атака обнаружена благодаря непрерывному мониторингу и видимости всех активностей на конечной точке. Эти данные, показанные командой Panda Threat Hunting, указывают на наличие аномального поведения на конечных устройствах, которые были скомпрометированы в рамках атаки brute-force (сотни попыток подключения в короткий промежуток времени).

Вымогательство со стороны бывшего сотрудника.

Одним из самых распространенных мотивов для запуска атаки против компании является негодование и желание отомстить.

В 2017 году мы видели случаи, когда бывшие сотрудники пытались шантажировать компании, откуда они были уволены. Причем **атаки, инициированные внутренними исполнителями, уже достигают 25% глобальных угроз**.

Общим знаменателем этих случаев является слабость политик защиты и наличие у бывшего сотрудника доступа к корпоративным ресурсам.

81% случаев незаконного доступа произошло из-за небезопасных паролей или в результате кражи паролей.

Несмотря на это, находясь внутри, сотрудники используют стратегии экспансии и контроля, достойные лучших хакеров, чтобы уклониться от остальных систем безопасности и причинить ущерб репутации компании и ее финансам:

1

Сотрудник уволен

Но его регистрационные данные не были отключены, поэтому он по-прежнему мог удаленно подключаться к своему ПК.

2

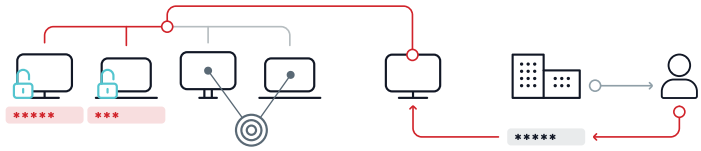
Подробное профилирование

Благодаря нескольким системным утилитам сотрудник получил список конечных устройств, подключенных к сети. Он запустил скрипт с MS-командой, чтобы узнать пользователей домена.

3

Атаки Brute-force

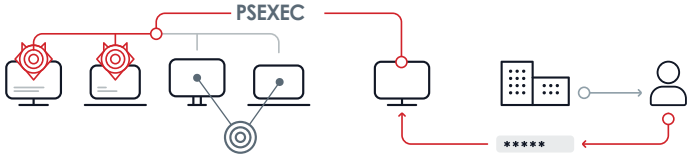
В течение последующих дней он запускал атаку типа brute-force и в конечном итоге получил доступ к некоторым конечным устройствам.



4

Атака шифровальщика

Он создал шифровальщика, который был скомпилирован за день до его внедрения. Со своего бывшего ПК и выполняя PSEXEC, он запустил скрипт для удаления всех существующих резервных копий, а затем скопировал и запустил шифровальщика.



Атака обнаружена командой Threat Hunting

Adaptive Defense заблокировал атаку на все машины, где он был установлен. После первой попытки атаки на конечные устройства, защищенные решением Adaptive Defense, команда Threat Hunting проанализировала процессы и поведение, которые выявили все подробности атаки и личности злоумышленника.

Общие аспекты.

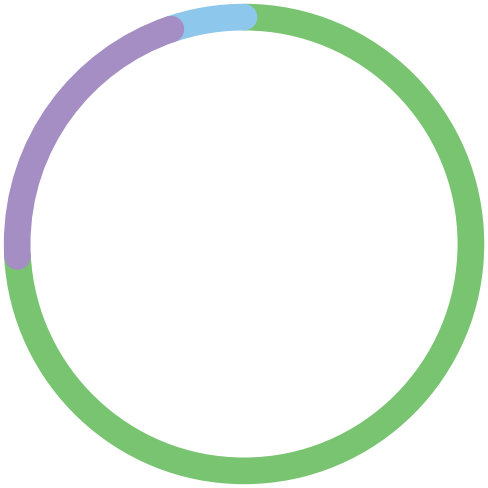
Несмотря на некоторые различия, все эти случаи имеют ряд сходных моментов:

Предварительное изучение слабых сторон компании при подготовке атаки

Адаптация атаки к этим недостаткам, скрытный доступ, который не вызывает подозрений или срабатывания со стороны систем оповещения в традиционных антивирусных решениях.

Тщательно спланированные и намеченные **внутренние продвижения** для достижения своих целей.

Общая цель для всех этих атак - это, как всегда, деньги. По данным Verizon, **финансовая цель наблюдается в 73% атак**, в то время как у 21% атак мотивом является шпионаж.



Другой общий знаменатель всех этих случаев связан с тем, что все эти атаки были обнаружены и вовремя предотвращены командой Threat Hunting и решениями с возможностями расширенной защиты, разработанными компанией Panda Security.

Цена атак.

Мы видели, как процесс "демократизации" кибер-атак облегчался за счет профессионализации хакеров, эволюции технологий и легкости доступа к данным.

Конечно, все это способствовало популяризации таких видов угроз, однако все же эти действия обусловлены высокой прибыльностью атак.

Недорогие кибер-армии позволяют кибер-преступникам получать серьезные финансовые выгоды.

		От	До
Инструменты атаки	Вредоносное ПО	$50	$200
	Шифро-вальщики	$1	$400
	ПО	$100	$700
	Оплата и подключения	$1	$25
Данные	Персональная информация	$3	$150
	Записи из БД	$25	
Услуги	Взлом	$100	$300
	Пользователи	$20	$150
	Вредоносное ПО	$1	$25
	Спам	$20	$400
	Ложные документы	$15	$25

Источник: Recorded Future.

GDPR: регулирование в Европе.

Новое Общее положение о защите персональных данных (General Data Protection Regulation, GDPR) в Евросоюзе было разработано в ответ на явный рост количества кибер-атак и направлено на борьбу с ними в рамках сотрудничества государственных и коммерческих предприятий и организаций.

Хотя он уже вступил в силу, **GDPR начнет функционировать в Евросоюзе в полной мере с мая 2018 года**. В настоящее время компании приводят свою деятельность в соответствии с новым законодательством.

С мая 2018 года все страны-члены Евросоюза должны будут перейти от соответствующего действующего национального законодательства к GDPR. Новый закон требует от компаний адаптировать свою политику к более ограничительным и строгим требованиям. Например, он будет обязывать компании сообщать о любых нарушениях персональных данных соответствующему агентству по защите данных, в противном случае на компанию могут быть наложены **штрафы размером до 4% от годового оборота**.

Организации также будут вынуждены внедрить системы шифрования и двухфакторной авторизации на всех уровнях работы с данными. Одним из наиболее существенных изменений, предусмотренных новым законодательством, наличие уполномоченного по защите данных (Data Protection Officer, DPO). Сотрудник, который будет занимать эту должность, должен иметь знания соответствующих законов и необходимых технологических инфраструктур для соблюдения положений GDPR.

Впрочем, еще предстоит определить весь круг обязанностей DPO. Также до конца не урегулировано, должен ли это быть выделенный сотрудник или его обязанности можно делегировать ответственным по информационной безопасности.

Общие аспекты GDPR:

- Более четко устанавливает правила обработки данных резидентов Евросоюза, включая компании, зарегистрированные за пределами Евросоюза.
- Требует явного согласия резидентов Евросоюза на сбор и обработку персональных данных, а также их возможное использование.
- Определяет, что относится к персональным данным, куда также включены данные профилей социальных сетей, фотографии, адреса электронной почты и даже IP-адреса.
- Рассматривает передачу данных через открытые и популярные форматы файлов.
- Регулирует "право на забвение", которое позволяет физическим лицам по запросу полностью удалить или исправить свои данные.
- Устанавливает, что организации всех размеров должны назначить сотрудника по защите данных, который будет отвечать за соблюдение положений GDPR перед соответствующими органами власти.
- Требует, чтобы вопросы конфиденциальности были интегрированы во все бизнес-процессы.
- Требует, чтобы информация о любом инциденте с персональными данными была сообщена в течение нескольких дней.
- Предусматривает огромные штрафы размером до 20 миллионов евро или до 4% годового оборота, что намного выше текущих значений.

Относится к компаниям, которые обрабатывают персональные данные граждан Евросоюза

Обязанность по отправке уведомлений об инцидентах с данными в течение 72 часов

Штраф за нарушение законодательства: до 20 миллионов евро

DPO будет нести ответственность за соблюдение положений GDPR

Последствия внедрения GDPR.

В большинстве штатов США существуют законы, обязывающие немедленно сообщать о любом нарушении безопасности данных клиентов. Неудивительно, что подавляющее большинство нарушений с данными, о которых сообщается в СМИ, связано с американскими компаниями.

До принятия GDPR многие страны Евросоюза не имели в своем национальном законодательстве подобной нормы.

Недавний громкий пример - это инцидент в Equifax, который считается самым серьезным нарушением конфиденциальности персональных данных в истории. Если бы такое произошло в Евросоюзе до вступления в силу GDPR, то, вероятно, о данном инциденте ни пострадавшие клиенты, ни органы власти, никто другой просто бы и не узнали.

Если подобное случится в Евросоюзе уже после вступления в силу всех норм и положений GDPR, то Equifax столкнулся бы с судебными исками со стороны Евросоюза и всех пострадавших клиентов. Учитывая средний годовой оборот в размере 500 миллионов долларов США, **Equifax мог бы получить штраф со стороны Евросоюза в размере 20 миллионов долларов США.** И это не считая убытков, которые компания бы понесла после рассмотрения судебных исков от всех пострадавших клиентов.

Со вступлением в силу всех норм и положений GDPR нас ждут серьезные изменения. В результате, вероятно, мы увидим резкий скачок количества инцидентов с кражей данных в Евросоюзе. Такие инциденты уже были.

Разница в том, что мы теперь узнаем о них.

Прогнозы ИБ.

Из вышеприведенного анализа следует, что проблемы ИБ становятся все более актуальными, особенно для средних и крупных предприятий, большинство из которых в тот или иной момент страдают от нарушений целостности данных. Интервал между утечкой данных и обнаружением данного инцидента увеличивается, и обычные методы предотвращения потери данных становятся менее эффективными.

Это лишь некоторые из волнующих нас сегодня проблем в сфере ИБ, но **какие угрозы нас ожидают в 2018 году?**

В этом разделе мы обсудим наши прогнозы относительно того, что, по нашему мнению, ожидает мир информационной безопасности в 2018 году.

Кибер-война и ее последствия.

Кибер-война - это реальность, в которой мы уже живем. Вместо открытой войны, где четко проведено разграничение между сторонами, кибер-войны идут в тени и состоят из изолированных атак в партизанском стиле, авторы которых, наверняка, никогда не будут известны.

Фрилансеры на службе у тех, кто больше заплатит.

Основные мировые державы уже имеют целые легионы кибер-солдат, десятки тысяч обученных воинов, которые способны атаковать в кибер-пространстве. Со временем, некоторые из них станут фрилансерами и будут предлагать свои услуги тем, кто больше всех заплатит. Банды профессиональных кибер-преступников смогут найти группу хорошо обученных профессионалов с доступом к кибер-оружию и ценными знаниями для запуска атак. Как следствие, **мы увидим стремительный рост наиболее сложных и продвинутых атак**.

Операция "ложный флаг".

Одной из наиболее привлекательных особенностей, которые кибер-атаки предлагают странам, участвующим в конфликте, - это анонимность, предоставляемая Интернетом. Конечно, всегда будут возникать подозрения в отношении исполнителей той или иной атаки, анализируя, например, жертву и делая выводы о том, кто бы мог извлечь выгоду от этой атаки.

Другой способ - это посмотреть следы, которые злоумышленники могли оставить после себя: характеристики используемого вредоносного кода, серверы, к которым подключались во время атаки для выполнения требуемых коммуникаций и т.д.

Несмотря на это, анонимность до сих пор представляет собой дополнительное оружие при таких атаках: **очень просто выполнять атаку через несвязанную с тобой третью сторону**. Этот тип операции "ложный флаг" станет очень популярным, а потому значительно сложнее будет выяснять, кто именно стоит за кибер-атакой, поддерживаемой правительством какой-нибудь страны.

Побочные жертвы.

WannaCry показал, что существуют атаки, которые могут проникать в корпоративные сети и неизбирательно атаковать любые и все уязвимые жертвы.

Но существуют и своего рода "хирургические" атаки, где цель определена очень хорошо. Это как раз случай с Petya/GoldenEye, который четко был направлен против государственных учреждений и частных компаний из Украины. Однако реальность такова, что в Интернете нет границ, и компании из десятков стран мира также пострадали от этой атаки, превратив их в побочных жертв конфликта, к которому они не имели никакого отношения.

Враг среди нас.

Один из самых ужасных кошмаров, которые мы можем себе представить, - это оказаться атакованным в защищенном окружении, где мы чувствуем себя в безопасности, например, у себя дома. Это ситуация, к которой мы не очень хорошо готовы, потому что: а) мы доверяем людям, которых мы приглашаем к себе домой; и б) даже если в качестве оружия можно использовать нож, то у всех нас дома он есть среди кухонной утвари. Эта аналогия служит иллюстрацией типа атак, с которыми нам предстоит столкнуться:

Хакерские атаки без использования вредоносных программ.

Одна из тенденций, которую мы увидим в 2018 году, - это рост числа атак, которые не используют вредоносные программы, и атак, которые злоупотребляют невредоносными инструментами.

В 2017 году мы видели, что **хакерские техники использовались в 62% случаев нарушения корпоративной безопасности**, причем почти в половине (49%) таких инцидентов вообще не использовались вредоносные программы, (по данным отчета 2017 Data Breach Investigations Report, составленному компанией Verizon).

Взломанные приложения.

Мы уже видели это в рамках атаки Petya/GoldenEye, когда популярная бухгалтерская программа M.E.Doc была взломана. Еще один случай, привлекший особое внимание, - это CCleaner, модифицированный неизвестными хакерами для выполнения, по всей видимости, атаки, направленной на определенных жертв крупных технологических компаний.

Мобильные устройства.

В каких пределах мы должны беспокоиться об угрозах в мобильной среде? Ответ: в пределах разумного. Учтите, что в мире существует больше смартфонов, чем компьютеров, и все же количество атак против них составляет небольшую долю от того, с чем приходится сталкиваться ПК.

Это не означает, что мы должны быть безучастны к вопросу безопасности наших мобильных устройств. Атаки будут происходить и дальше, но, кажется, что Google принял к сведению основные проблемы и постепенно предпринимает шаги для защиты своей операционной системы (**Android, которая имеет самую большую в мире долю рынка в секторе мобильных устройств**).

Но факт остается фактом: существуют миллионы угроз, направленных против Android, поэтому, конечно, необходимо должным образом защищать все данные, к которым мы подключаемся с наших мобильных устройств.

Интернет вещей.

Количество устройств, подключенных к Интернету, продолжает расти. Как это может сказаться на безопасности? Уже существуют бот-сети, состоящие из тысяч IoT-устройств (от IP-камер до принтеров), предоставляя кибер-преступникам возможность запускать массовые атаки.

В целом, IoT-устройства не являются первичной целью для кибер-преступников. Однако такие устройства увеличивают площадь атаки, поэтому все чаще будем видеть, что они используются в качестве точки входа для атак на корпоративные сети.

Все ради денег.

Шифровальщики.

Нет никаких сомнений в том, что основная цель кибер-преступных организаций - это извлечение прибыли.

Атаки шифровальщиков будут превалировать и в 2018 году, т.к. потенциальная отдача от инвестиций в них очень высока, в то время как риски остаются крайне низкими.

Больше усовершенствованных атак.

Атаки будут более профессиональными, особенно в случаях, когда потенциальные выгоды выше. Когда новые методы кибер-преступлений окажутся успешными, они будут мгновенно воспроизводиться в массовом порядке. Это одна из основных причин, по которой количество усовершенствованных атак будет значительно расти в 2018 году.

Следуя тенденции последних лет, **в 2018 году число атак увеличится на 50%** по сравнению с 2017 годом.

2018: год атак на компании.

Возможно, это правда, что мы пережили несколько самых крупных атак в прошлом с астрономическим объемом украденных данных. Каждый помнит, например, инцидент в Yahoo и кражу сотен миллионов регистрационных данных.

И в 2017 году, конечно, у нас были инциденты с Sabre и Equifax. Так почему мы думаем, что 2018 год будет достоин звания "год атак на компании"? На этот вопрос можно ответить аббревиатурой из четырех букв: GDPR.

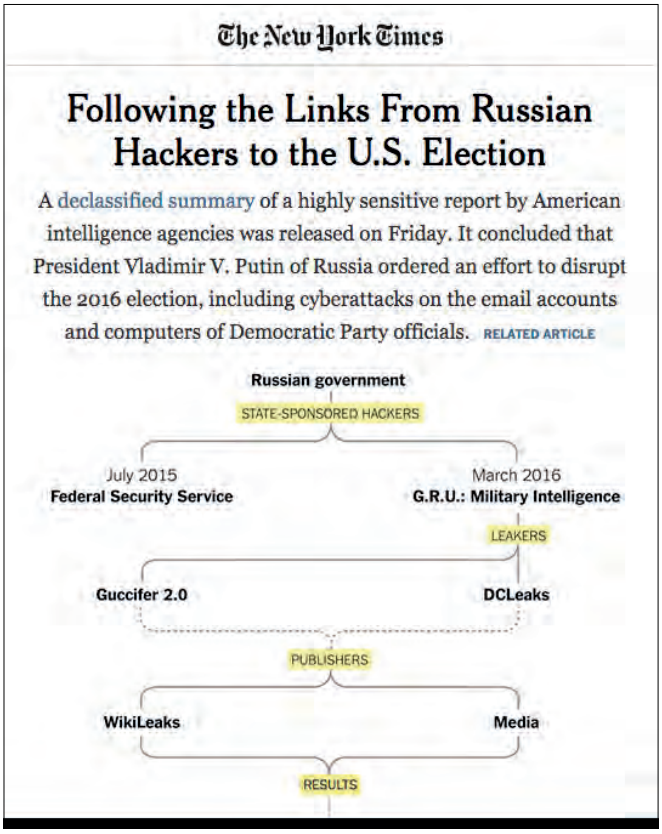
Это вовсе не означает, что в 2018 году компании будут подвергаться большему числу атак, чем в предыдущие годы.

Скорее всего, впервые в истории общественность будет знать о каждом или почти каждом инциденте с данными, включая те, которые ранее, до вступления в силу GDPR, могли быть неизвестны или сведения о них не разглашались.

Соцсети и пропаганда.

Никогда прежде в истории люди не имели доступа к таком огромному объему информации. Но по иронии судьбы, никогда ранее не было так сложно найти достоверную информацию, чем сейчас.

Проще говоря, социальные сети - это инструменты, где мы можем обмениваться информацией, а когда ими пользуются миллиарды людей во всем мире, они становятся очевидной мишенью для каждого, кто хочет повлиять на общественное мнение. В некотором смысле их роль сравнима с СМИ. Мы слышали, как **Президент США Б. Обама лично предупреждал основателя и руководителя Facebook** Марка Цукерберга очень серьезно относится к угрозе фальшивых новостей во время президентских выборов.



Facebook, крупнейшая в мире социальная сеть, уже предпринимает определенные действия в этом направлении. Если будет обнаружено, что какая-то страница Facebook неоднократно распространяла фейковые новости, то Facebook запретит ее рекламу где-либо в сети. Компания также публиковали объявления в своей сети и в СМИ, объясняя читателям, как они могут идентифицировать фейковые новости. Теперь они находятся в процессе изменения своей политики для рекламы, связанной с выборами, чтобы сделать ее максимально очевидной.

Криптовалюта.

Bitcoin и другие криптовалюты все чаще используются в качестве средства цифровых платежей. И хотя есть множество спекуляций на тему их будущего, все больше и больше коммерческих структур принимают платежи в этих валютах. Другая причина успеха криптовалют - их польза для кибер-преступников, т.к. они позволяют им быстро и анонимно оперировать крупными суммами денег.

Шифровальщики - лучший пример этого, потому что почти все эти атаки требуют выкуп в биткоинах.

Криптовалюты продолжат расти в стоимости и юзабилити, но вместе с ними будет развиваться и кибер-преступность:

- Заражение компьютеров и серверов программами для майнинга криптовалют
- Заражение веб-страниц для перевода всех посетителей страницы в майнеров
- Кража монет с криптовалютных бирж
- Кража крипто-кошельков.

Заключение.

После того как мы увидели глобальные атаки, которые поразили компании и учреждения во всем мире, важно знать, как мы можем защитить нашу конфиденциальность и безопасность в Интернете.

Обновление ПО и средств безопасности должно стать приоритетом для всех компаний. Такие случаи как WannaCry или Equifax подтверждают это, т.к. каждый день, который проходит без обновления уязвимой системы, подвергает риску всю компанию, а также целостность ее данных, включая сведения об ее клиентах и поставщиках. Производство может быть поставлено под угрозу, что может принести миллионные убытки. Один пример: группа AP Moller-Maersk стала одной из жертв атаки GoldenEye/NotPetya, и по ее расчетам, убытки составили от 200 до 300 миллионов долларов США.

Страны все больше и больше инвестируют в оборонительный и наступательный потенциалы с упором на критические инфраструктуры. Возможность удаленно запускать атаку, которая может привести к коллапсу, - это уже не теория: подобное уже случалось на Украине, и это может повториться в любой стране мира. Преступные группировки с ограниченным финансированием, тем не менее, могут иметь доступ к знаниям и инструментам, необходимым для запуска разрушительных атак на объекты критической инфраструктуры. Причем такие атаки могут осуществлять уже не только какие-то спецслужбы. Известно, что террористические группы, такие как ИГИЛ (запрещена в России), готовы использовать все имеющиеся в их распоряжении кибер-средства для дальнейшего распространения террора.

2018 год находится в более опасном положении. Многим специалистам **необходимо будет изменить менталитет (и стратегию), чтобы достичь самых высоких уровней безопасности** и защитить активы своих корпоративных сетей. Противодействие вредоносному ПО - это только начало. Мы вступаем в эпоху, когда лучшая стратегия безопасности предполагает отсутствие доверия к чему-либо. Любой новый процесс, который хочет запуститься на любом устройстве, подключенном к сети, должен быть предварительно разрешен, а те процессы, которым мы доверяем, необходимо постоянно и непрерывно контролировать, чтобы в максимально короткое время обнаруживать любое его аномальное поведение.

Что дома, что в офисе, **ключевые аспекты - это обучение и осведомленность**. Из этого следует, что информационная безопасность, о которой часто забывают руководители, будет требовать все больше инвестиций.

Наличие глубоких знаний об атаках и о том, из чего они состоят, должно стать основной для хорошей стратегии защиты. **Безопасность, основанная на обнаружении и реагировании в реальном времени**, в сочетании с экспертным анализом и подробной информацией о том, как произошла атака, имеют важное значение для отражения будущих вторжений. Gartner Peer Insights рекомендует Panda Adaptive Defense в качестве лидирующего EDR-решения.

Сигнатурные файлы больше не работают, а цифры говорят сами за себя: свыше 99% от числа всех вредоносных программ никогда больше нигде не встречаются. Сбор сигнатур - это уже недостаточный и неэффективный способ обеспечения обнаружения. Многие производители решений безопасности добавляют их только в том случае, если тестирующие лаборатории позже захотят провести тест обнаружения вредоносных программ по сигнатурам (а это становится все менее распространенной практикой), ведь многие до сих пор верят в то, что результаты таких тестирований показывают, способен ли продукт обнаруживать угрозу или нет.

Решения, которые останутся сосредоточенными на борьбе с вредоносными программами (большинство ныне доступных на рынке решений) обречены на вымирание, если они не изменят свою стратегию. Количество атак, которые не используют вредоносные программы, продолжает расти. И перед лицом этой реальности решения безопасности и их пользователи совершенно потеряны и беззащитны.

И, конечно, мы не можем забыть про **международное сотрудничество и создание единой нормативно-правовой базы,** например, GDPR. Наличие политической и экономической поддержки, а также соответствующего плана действий позволит извлечь выгоду из безопасного использования новейших технологических достижений.

В конце концов, все дело в том, что необходимо **пересмотреть принципы информационной безопасности**.

panda

pandalabs