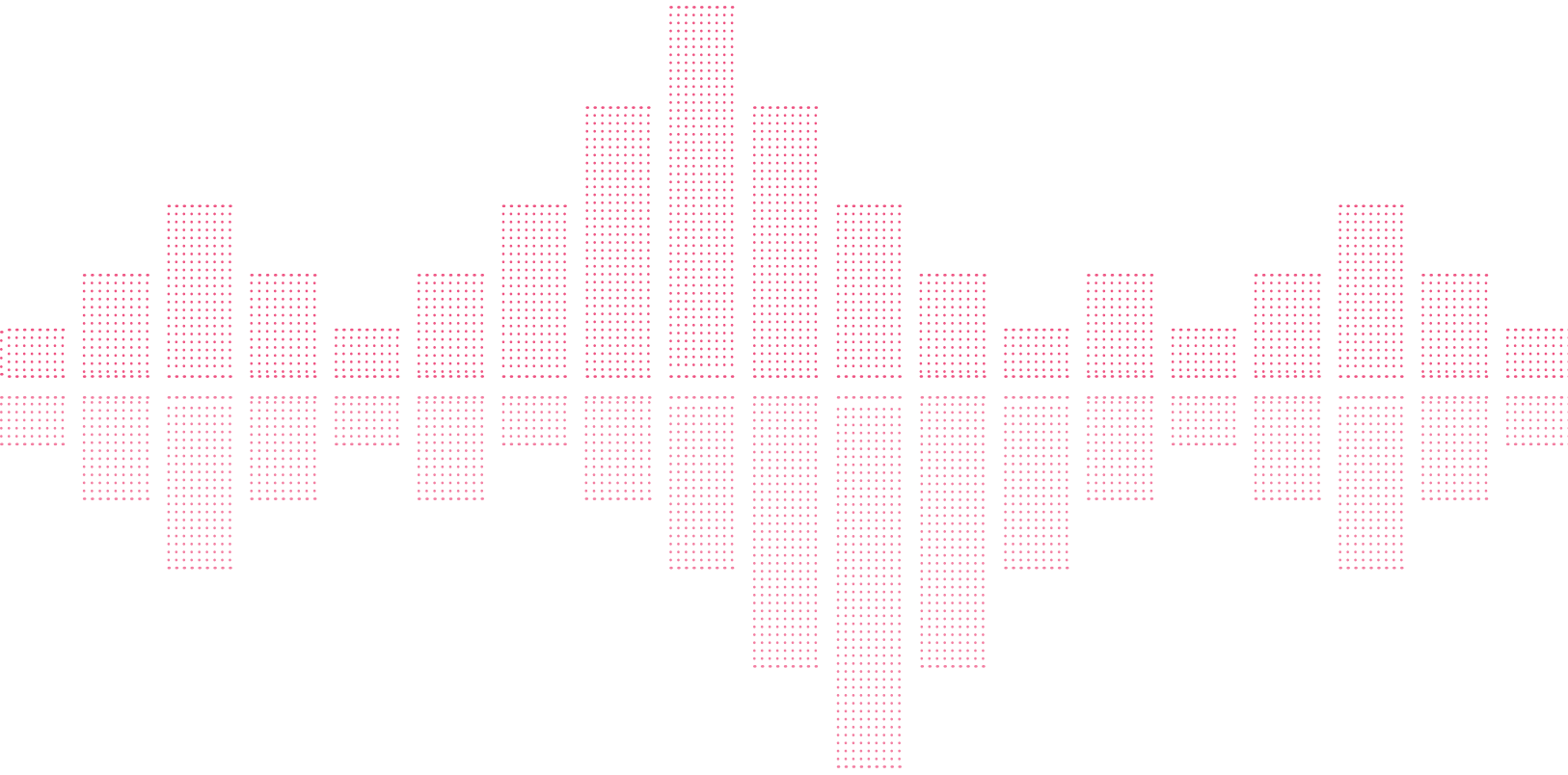
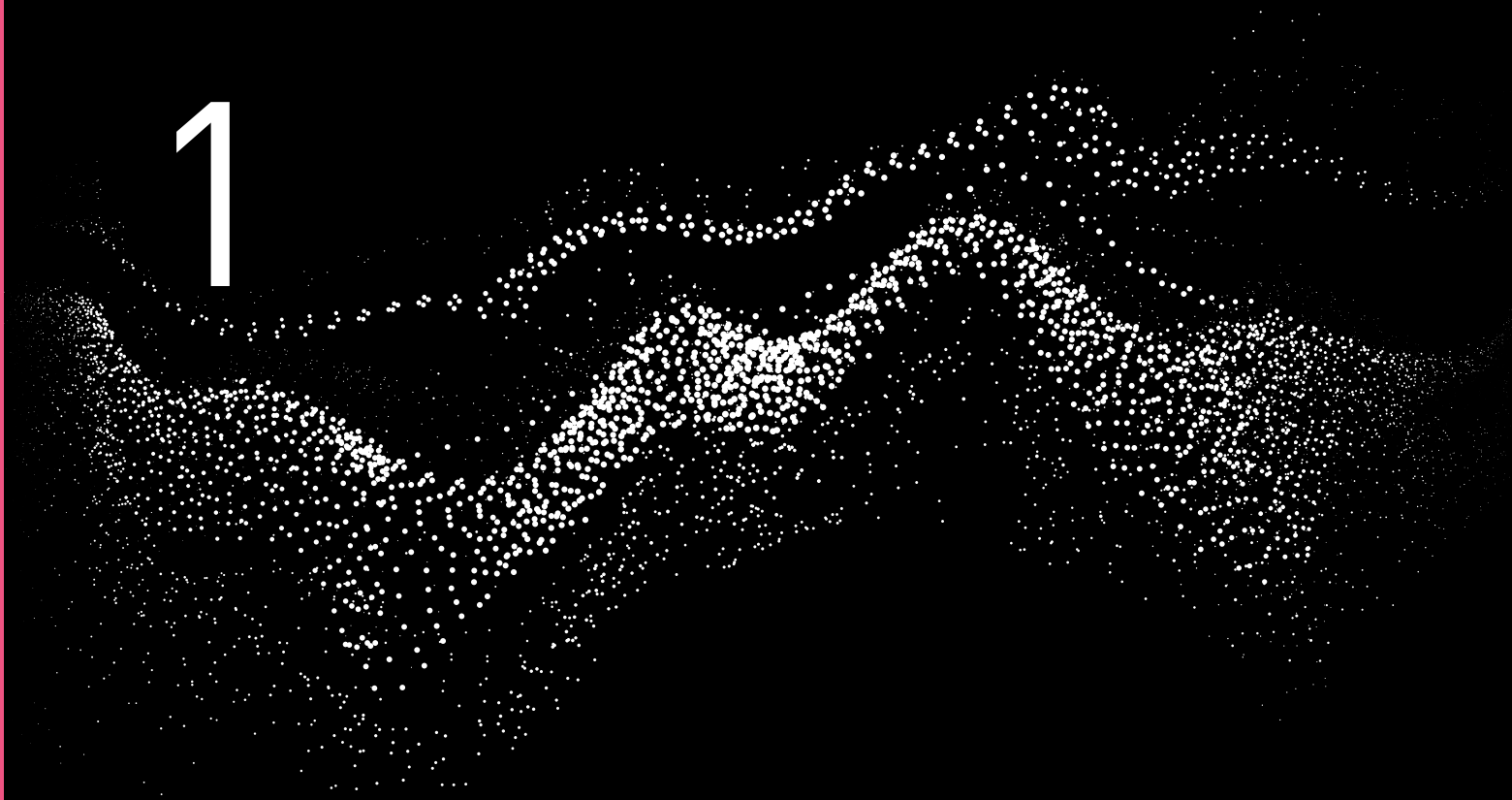


2016 ОТЧЕТ ПО БЕЗОПАСНОСТИ



1

ВВЕДЕНИЕ И МЕТОДОЛОГИЯ

> *«Мы застряли в технологиях, в то время как нам просто нужны вещи, которые работают».*
>
> Дуглас Адамс, писатель и сатирик

Приз за величайший взлом уходит к OPM – Федеральному офису США по управлению персоналом. Хакеры, предположительно из Китая, оставались незамеченными в сети OPM более года, прежде чем их присутствие было обнаружено. После того как взлом был в конце концов выявлен, первоначальная оценка жертв инцидента составила четыре миллиона. Но вскоре их число выросло до более чем 21 миллиона, включая 19 миллионов тех, кто подавал документы на получение допуска к секретным работам и проходил проверки, а также 1.8 миллиона супругов и сожителей кандидатов. Хакеры получили в свои руки сокровище из конфиденциальных данных, включая формы SF-86 людей, запрашивающих допуск. Эти формы содержат большой объем конфиденциальной информации не только о соискателях допуска, но и об их друзьях, супругах и других членах их семей.

— **Wired Magazine**, 23 декабря 2015

Хотя в 2015 году произошло достаточное число нашумевших взломов данных, взлом OPM привлек к себе большое внимание потому, что на его обнаружение ушло более года, а волновой эффект от этого конкретного взлома оказался далеко идущим. При чтении Отчета по безопасности за этот год можно ясно видеть, что защита современного предприятия является как никогда более сложной задачей, и проигрыш здесь является весьма вероятным. Взлом такого типа может случиться с каждым. Чтобы помочь вам защитить вашу организацию, ваши данные и ваших клиентов, мы скомбинировали рекомендации в каждой из следующих глав. Каждый взлом – это опыт, который учит нас, как лучше защищаться, и мы можем многому научиться на примере взлома OPM.

В апреле 2015 года была обнародована информация о том, что из Офиса США по управлению персоналом, центрального репозитория персональных данных государственных служащих США, были похищены более 21 миллиона записей, содержащих персональные данные. Эти данные включали в себя детализированные формы запросов на получение допуска к секретным работам наряду с отпечатками пальцев более чем 5.6 миллионов служащих. Согласно информации официальных лиц федерального уровня это стало

одним из величайших взломов правительственных данных за всю историю США.

Как пояснил официальный представитель Департамента национальной безопасности США Энди Озмент (Andy Ozment), взлом начался примерно за год до того, как его обнаружили. Атакующие сначала получили действительные аутентификационные данные пользователей для доступа в систему, возможно с помощью социальной инженерии. После проникновения внутрь они запустили пакет вредоносного ПО, создав таким образом «черный ход» для своих операций. Затем, они провели эскалацию своих привилегий, получив доступ к широкому спектру систем OPM.

Этот инцидент хорошо показывает, как незначительный взлом сети может вырасти в крупномасштабное хищение данных, длящееся несколько месяцев. Сети растут и сегментируются, затем сегменты могут объединяться, и часто бывает сложно соответствовать карте сетевых ресурсов. Большое число атак, нацеленных на все более и более размытую границу сети, еще сильнее усложняет положение. Как и в большинстве организаций, столкнувшихся со взломом, расследование по следам инцидента в OPM выявило несколько областей, требующих усовершенствования. Необходимо постоянно поддерживать актуальной инвентаризацию серверов, баз данных и сетевых устройств. Обеспечению безопасности также существенно помогают проактивное сканирование внутренних сетей, сегментация элементов сети и многофакторная аутентификация. Это должно являться обязательной частью мер по обеспечению базового состояния безопасности любой организации. При успешной атаке анализ методов взлома может многое рассказать об атакующих, их мотивах и о том, как можно в будущем наилучшим образом построить защиту от них.

Предотвращение: призыв к действию

Все организации могут извлечь уроки из взлома OPM. Предотвращение атак до того, как они нанесут урон, и использование единой архитектуры безопасности для упрощения и укрепления безопасности является обязательным при современном ландшафте угроз.

Сегментируйте вашу сеть и внедрите унифицированные политики на всех ее сегментах, используя архитектуру унифицированной безопасности.

Применение «заплаток» оставляет пробелы. Используйте виртуальные «заплатки» IPS для защиты, покрывающей периодические обновления заплаток.

Предотвращайте заражение вредоносным ПО в реальном времени, используя предотвращение угроз на уровне ЦП и ОС.

Мониторьте все сегменты сети на одном экране.

ТИПИЧНЫЙ ДЕНЬ В КРУПНОЙ ОРГАНИЗАЦИИ

КАЖДУЮ 81 СЕКУНДУ
Загружается известное вредоносное ПО

КАЖДЫЕ 4 МИНУТЫ
Используется приложение высокого риска

КАЖДЫЕ 4 СЕКУНДЫ
Загружается неизвестное вредоносное ПО

КАЖДЫЕ 5 СЕКУНД
Хост обращается к вредоносному веб-сайту

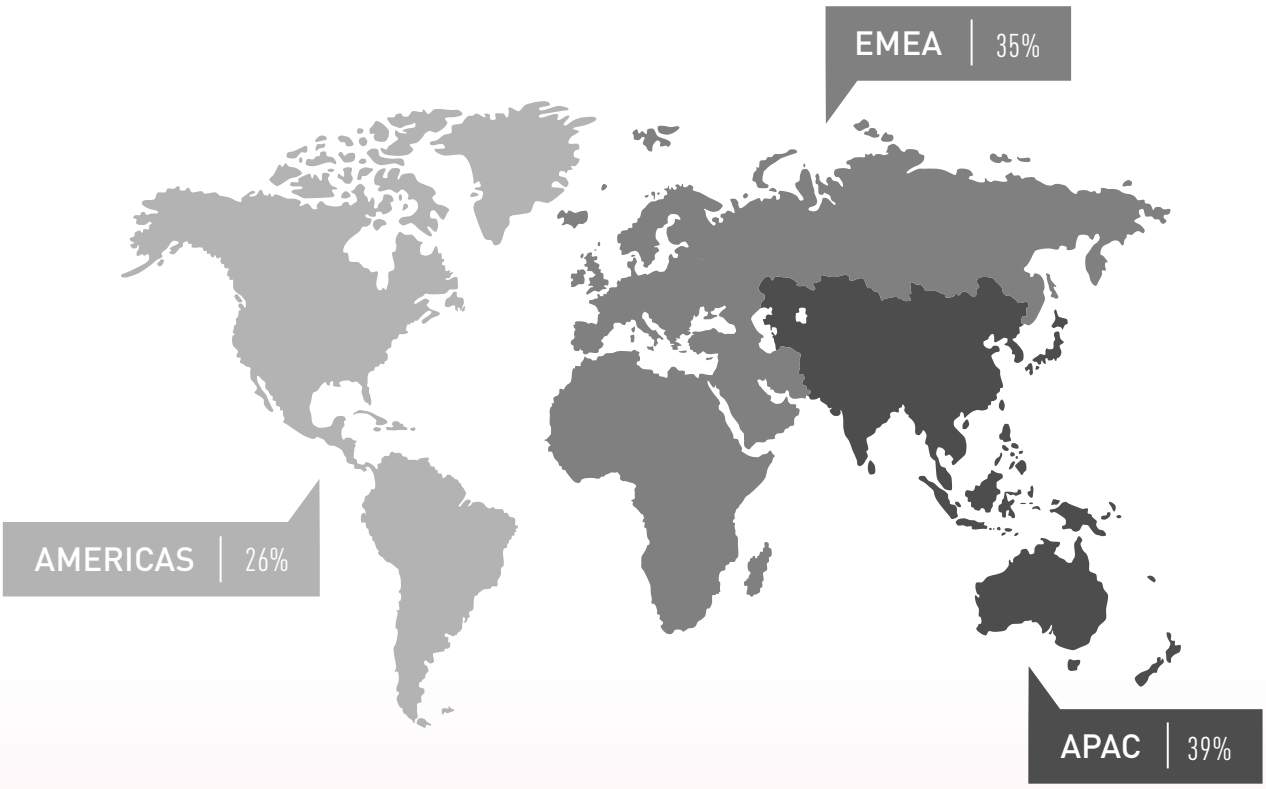
КАЖДЫЕ 53 СЕКУНДЫ
Бот связывается со своим центром управления

КАЖДЫЕ 30 СЕКУНД
Происходит событие эмуляции угрозы

КАЖДЫЕ 32 МИНУТЫ
Конфиденциальная информация отсылается за пределы организации

1.1 Источник: Check Point Software Technologies

РАСПРЕДЕЛЕНИЕ ОРГАНИЗАЦИЙ ПО ГЕОГРАФИЧЕСКОМУ ПОЛОЖЕНИЮ



1.2 Источник: Check Point Software Technologies

ИСТОЧНИКИ КОМПАНИИ CHECK POINT

Чтобы находиться на шаг впереди, мы в течение всего 2015 года собирали данные о событиях из различных источников по всему миру. В отчет вошли данные более чем 11 000 проверок безопасности Security Checkup, события, обнаруженные посредством системы ThreatCloud (которая соединена с более чем 25 000 шлюзов по всему миру), и данные с более чем 6 000 шлюзов, посылающих свои данные в нашу облачную систему Threat Emulation Cloud. Для выработки рекомендаций, приведенных в каждом разделе, мы комбинировали эти данные с результатами анализа внешних тенденций и заключениями, полученными от нашей внутренней исследовательской команды.

РАСПРЕДЕЛЕНИЕ ОРГАНИЗАЦИЙ ПО ОТРАСЛЯМ ЭКОНОМИКИ

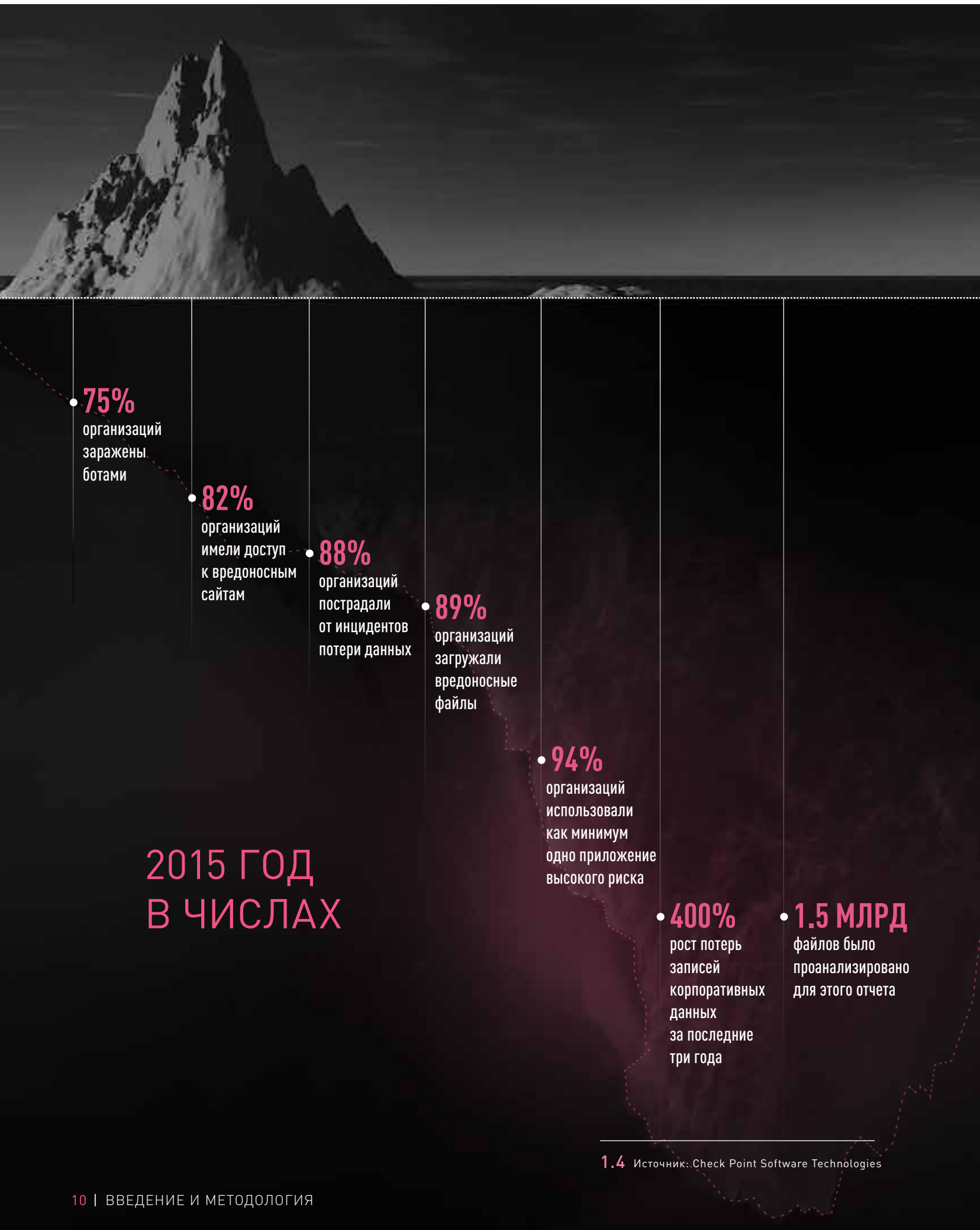
*Юридические организации, Развлечения/Гостиничный бизнес, Реклама/Медиа, Ценные бумаги и прочие организации

1.3 Источник: Check Point Software Technologies

СТРУКТУРА ОТЧЕТА ПО БЕЗОПАСНОСТИ 2016 ГОДА

Наш Отчет по безопасности 2016 года рассматривает виды известного и неизвестного вредоносного ПО, а также тренды атак, с которыми сталкиваются предприятия, равно как эффект от всевозрастающего использования мобильных устройств в крупных компаниях. Кроме того, мы рассматриваем ущерб, который успешные атаки наносят организациям, и их дополнительные расходы по покрытию вреда, нанесенного торговым маркам, которые существенно превышают обычную стоимость очистки информационных систем.

Глава 2 содержит обзор и анализ различных типов вредоносного ПО, а также способы, с



1.4 Источник: Check Point Software Technologies

помощью которых оно использует в своих целях особенности поведения пользователей. Основное число крупномасштабных взломов в 2015 году было осуществлено с использованием существующих уязвимостей, известного вредоносного ПО и, конечно, социальной инженерии. При росте числа попыток пользователя получить доступ к вредоносному сайту эффективность блокировки таких действий IT-службой возрастает немного быстрее, делая этот вектор атаки менее эффективным. В то же время, несмотря на снижение статистики заражения ботами, суточная частота попыток ботов установить связь возрастает.

Глава 3 рассказывает о том, как «мобильная революция» и растущее число мобильных устройств, без проверки подключающихся к корпоративным сетям, продолжает создавать новые возможности для атак. Организации сейчас осознают, что они не могут просто запретить пользователям подсоединять свои личные устройства к корпоративным ресурсам, потому что они осознали, что концепция BYOD («bring your own device» – «принеси свое собственное устройство») существенно увеличивает производительность. К сожалению, мобильная платформа является удобной целью для атакующих, так как большинство организаций не устанавливает никаких контрольных механизмов для их эффективной защиты.

В Главе 4 мы рассматриваем паттерны атак по регионам земного шара и их типам. США до сих пор лидируют в мире по числу вредоносных файлов и хостингу вредоносных веб-сайтов, большей частью благодаря большому общему числу пользователей и изобилию ресурсов. Что касается векторов атак, которые предпочитают хакеры, исполнение кода, такое как возвратно-ориентированное программирование (ROP – return–oriented programming) стало наиболее популярным вектором атак для злоумышленников, сделав в силу применения «заплаток» для уязвимостей менее привлекательными атаки переполнения буфера, лидера по популярности среди хакеров в 2014 году. В целом, число уязвимостей в 2015 году слегка снизилось, хотя связанные с наиболее распространенными из них производители поменялись. Тенденции могут меняться, но если организации не применяют у себя жизненно необходимых «заплаток», векторы атак нельзя будет полностью уничтожить.

В то время как начальные потери, связанные со взломом, обычно хорошо документированы, общий финансовый ущерб может оказаться значительно большей величиной. В Главе 5 мы рассматриваем эти «волновые эффекты» отсутствия безопасности, детально разбирая примеры из финансового сектора, медицины и промышленного сектора. Поддерживать скорость вашего бизнеса сохраняя его безопасным, – ваш лучший финансовый ход.

Быть на шаг впереди означает находиться в лидерах во всех областях: вредоносного ПО, тенденций атак, управления «мобильной революцией», и понимать ущерб от того что ты пропустил. В каждой главе вы найдете наши рекомендации, как сделать так, чтобы ваша организация была на шаг впереди любых киберпреступников.

> ***«Любая достаточно развитая технология неотличима от магии».***
>
> Артур Кларк, писатель-фантаст

2

АРСЕНАЛ АТАКИ: ИЗВЕСТНОЕ И НЕИЗВЕСТНОЕ ВРЕДОНОСНОЕ ПО

«Проваливая подготовку, вы готовитесь к провалу».

Бенджамин Франклин, политик, писатель

Известное вредоносное ПО

образец идентифицированного вредоносного ПО с различимой сигнатурой

Многие инструменты безопасности используют основанные на сигнатурах технологии для анализа и принятия решений о блокировке, что требует от пользователей поддерживать их определения в межсетевых экранах и антивирусах в обновленном состоянии.

Неизвестное вредоносное ПО

образец неидентифицированного вредоносного ПО без известной различимой сигнатуры

Создание неизвестного вредоносного ПО может быть достаточно простым – достаточно малой модификации известного вредоносного ПО или перепаковки вредоносного ПО другой полезной нагрузкой. Такая новая неизвестная версия может затем легко преодолеть защиту, основанную на сигнатурах.

Вредоносное ПО «нулевого дня»

эксплоиты, использующие преимущества ранее неизвестных уязвимостей, для которых еще не установлены защитные меры

Первым шагом атаки является преодоление вредоносным ПО барьера безопасности. В 2015 году это осуществлялось с использованием большого объема и разновидностей атак. Подавляющая часть вредоносного ПО скрывается под видом легитимного трафика, прикрепленных файлов или же эксплуатирует легитимные функции управления сетью или доступом. Скрываясь в ссылке, в документе или эксплуатируя уязвимость командной оболочки, атакующие используют широкий спектр и комбинацию методов проникновения.

Независимо от метода внедрения мы можем говорить о трех базовых типах вредоносного ПО: известном, неизвестном и вредоносном ПО «нулевого дня».

Каждый день появляется около одного миллиона новых видов вредоносного ПО[1]. Отчет по расследованиям взломов данных компании Verizon за 2015 год оценивает, что около 90% взломов 2015 года были совершены с использованием уязвимостей, существовавших с 2002 года. Недавний Отчет по киберрискам компании HP[2] отмечает, что из первой десятки уязвимостей, эксплуатированных в 2015 году, все были известны более года, а в 29% взломов, произошедших в 2010 году, использовался вектор заражения, для которого были доступны две различные «заплатки». Несмотря на то, что количество неизвестного вредоносного ПО растет, в ландшафте угроз все еще доминируют известные векторы.

КАЖДЫЕ 5 СЕКУНД ПОЛЬЗОВАТЕЛЬ ОБРАЩАЕТСЯ К ВРЕДОНОСНОМУ САЙТУ

На сегодня прогноз для центров обработки данных (ЦОД) в основном звучит как «облачно». По оценкам компании Cisco к 2019 году облачные ЦОД будут обрабатывать свыше 86% IT-нагрузки[3]. Согласно RightScale 95% компаний уже работают с облачными платформами, используя в среднем 3 публичных облака и 3 частных облака[4]. Несмотря на быструю миграцию в облака, немногие профессионалы IT осознают, как сервисы, работающие в среде виртуализованных публичного и частного облаков, могут стать причиной нестабильности их защиты. Причиной такой турбулентности является изменение паттернов трафика данных от потока типа «север/юг», характерного для традиционных ЦОД, к потоку «восток/запад» в публичных облаках и то, что нагрузка смещается за пределы площадки в домены публичного облака.

Не витать в облаках: ваш трафик данных может быть послан за безопасностью по ложному пути

Вы скажете, что традиционные ЦОД требуют месяцы для развертывания новых приложений и то, что они недостаточно масштабируемы. Кроме того, в своей работе они требуют гигантский объем ручных операций. Но с точки зрения безопасности традиционные ЦОДы достаточно хороши со своими правильными шлюзами безопасности, размещенными в стойках и соединенными к местам, где оптоволокно выходит из-под фальшпола. Все это потому, что в ЦОД «старой школы» трафик идет на «север» от серверов к шлюзу безопасности и возвращается на «юг» от шлюзов безопасности к серверам. Трафик может даже следовать по схеме «булавочного» поворота «север/юг» так, что он идет вверх от сервера к шлюзу и возвращается вниз к другому серверу в том же ЦОД так, что внутренний трафик тоже может инспектироваться на предмет угроз.

Однако в виртуализованных или программно-определяемых сетях, развернутых в среде частного облака, до 80% трафика проходит с «востока» на «запад» между виртуализованными приложениями и различными секторами сети. Более того, виртуализованные приложения могут мигрировать между хостами, как этого требует управление ресурсами. В этих условиях большинство трафика полностью обходит шлюз безопасности на периметре. Мобильные приложения, облачные приложения, приложения партнеров и даже приложения клиентов хостинга могут подключать сервисы ко внешним с точки зрения ЦОД пользователям используя различные пути, не сканируемые средствами защиты периметра. Если атакующие компрометируют хотя бы один из незначительных веб-сервисов организации с помощью вредоносного ПО, вся сеть, включая основные сервисы, окажется в зоне риска.

Таким образом, для поддержания IT-безопасности в виртуализованных публичных и частных облаках, полезно подумать о сегментации вашей сети и приложений с использованием тех же самых средств, как физические шлюзы, но с добавлением гибкой поддержки для программно-определяемой микросегментации, которая может централизованno управляться. Высокая видимость приложений также критична для обеспечения безопасности облачных сервисов, перемещающихся в новых направлениях благодаря облачным платформам и доменам.

БОЛЬШЕ УСТРОЙСТВ, БОЛЬШЕ ПУТЕЙ ВХОДА

Современное предприятие должно защищать стремительно растущее число удаленных работников, многочисленных офисов, облачных приложений и многочисленных устройств. Количество точек входа в сеть, которые нуждаются в защите, продолжает увеличиваться. Каждая проводная и беспроводная точка входа, серверы и инфраструктура, на которой развернуты корпоративные приложения, а также сигнатурные средства предотвращения угроз нуждаются, для их защиты в постоянном обновлении и установке «заплаток».

Необходимость находиться в состоянии, соответствующем текущему дню, для управления «заплатками» сохраняла свою злободневность на протяжении 2015 года, демонстрируя высокую актуальность проблемы известного вредоносного ПО.

ДИСЦИПЛИНА ОРГАНИЗАЦИИ: ЛУЧШЕ, НО ЕЩЕ НЕ ХОРОШО

Наше исследование показало, что организации стали лучше работать в плане предотвращения доступа своих пользователей к вредоносным сайтам. В 2015 году только 82% организаций обращались к вредоносным сайтам – показатель меньший по сравнению с 86% в 2014 году. К сожалению, другие метрики не столь позитивны.

В крупных организациях пользователи обращались к вредоносным веб-сайтам в 2015 году в пять раз чаще – каждые 5 секунд – по сравнению с каждыми 24 секундами годом ранее.

А с более частым доступом пришло и больше вредоносного ПО, затронувшего большее число предприятий. В 2015 году 89% организаций загрузили вредоносные файлы – сравните с 63% в 2014 году. В 2015 году организации загружали вредоносное ПО в четыре раза чаще – каждую 81 секунду – по сравнению с каждыми 6 минутами в 2014 году.

ПОЛЬЗОВАТЕЛЬ ЗАГРУЖАЕТ ВРЕДОНОСНОЕ ПО КАЖДУЮ 81 СЕКУНДУ

2.1 Источник: Check Point Software Technologies

Что это означает? Хотя организации прилагают все свои усилия, чтобы предотвратить доступ к вредоносным сайтам, гигантский объем атак дает преимущество атакующим. Организации должны оценивать и отфильтровывать возросший объем потенциально вредоносного контента, сохраняя в то же время показатели производительности пользователя. Они должны быстро изолировать и реагировать на заражение вредоносным ПО для минимизации его распространения и потенциального ущерба.

ИЗВЕСТНЫЕ АТАКИ БОТОВ В 2015 Г.

СЕМЕЙСТВО	УЩЕРБ	ДОЛЯ
SALITY	Похищает конфиденциальную информацию	18.6%
CONFICKER	Отключает сервисы безопасности, дает хакеру удаленный доступ	18.6%
ZEROACCESS	Допускает удаленные действия и загрузку вредоносного ПО	6.7%
CUTWAIL	Распространяет спам	5.1%
GAMARUE	Открывает «черный ход» для атак	3.0%
ZEUS	Похищает банковские данные	2.7%
LDPINCH	Похищает конфиденциальную информацию	2.1%
DELF	Похищает аутентификационные данные	1.1%
RAMNIT	Похищает банковские данные	1.0%
GRAFTOR	Загружает вредоносные файлы	0.9%

2.2 Источник: Check Point Software Technologies

ПРОБЛЕМА БОТОВ ПРОДОЛЖАЕТ СУЩЕСТВОВАТЬ

Боты остаются весьма значимой методологией атак для злоумышленников. Подобно червю или трояну бот исполняет широкий спектр автоматизированных действий, как только он оказался внутри сети и стал осуществлять связь с внешним миром на регулярной основе. Воспроизводя себя на соседних сетях и устройствах, или проецируя себя вовне относительно сети своего хоста, они рассылают спам или участвуют в атаках «отказ в обслуживании».

Некоторые боты остаются в спящем состоянии до момента удаленной активации по предопределенному действию компьютера-«жертвы» или до определенного момента времени в будущем. Несмотря на различия, боты обычно осуществляют связь со своим центром управления, для того чтобы сообщить свой активный статус и получить инструкции. Такие соединения могут и должны быть изолированы, отслежены и блокированы.

В 2015 году типичный бот осуществлял попытки связаться со своим сервером управления более 1630 раз в день, или каждые 52.8 секунды. Эта скорость и частота продолжает расти, скакнув на 12% относительно предыдущего года и на 95% по сравнению с 2012 годом.

Хотя заражения ботами уменьшились на 10% в 2015 году по сравнению с 2014 годом, их число все еще доставляет беспокойство. Почти 75% организаций обнаружили у себя заражение ботами в 2015 году, причем 44% из них были активны более четырех недель.

Атаки ботов приводят к хищению конфиденциальной информации, такой как аутентификационные или банковские данные, отключению систем безопасности и получению удаленного доступа для атак. Боты также участвуют в удаленных операциях и загрузке дополнительного вредоносного ПО.

Анализ данных атак ботов показывает, что четыре типа ботов: Sality, Conficker, ZeroAccess и Cutwail – несут ответственность за 50% выявленных атак ботов в 2015 году.

БОТ ПЫТАЛСЯ СВЯЗЫВАТЬСЯ СО СВОИМ ЦЕНТРОМ УПРАВЛЕНИЯ СВЫШЕ 1630 РАЗ В ДЕНЬ, ИЛИ КАЖДЫЕ 52.8 СЕКУНДЫ

274 НОВЫХ, НЕИЗВЕСТНЫХ ВИДА ВРЕДОНОСНОГО ПО БЫЛО ОБНАРУЖЕНО ЗА КАЖДУЮ МИНУТУ В 2015 ГОДУ

РОСТ НЕИЗВЕСТНЫХ ВРЕДОНОСНЫХ ПРОГРАММ ПРОДОЛЖАЕТСЯ

В общем использование атакующими неизвестного вредоносного ПО остается на исторически высоких уровнях, немного увеличившись, согласно AV-TEST, в 2015 году[5]. Почти 144 миллиона новых образцов вредоносного ПО было обнаружено в 2015 году, что означает, что каждую минуту было произведено и запущено 274 новых вида неизвестного вредоносного ПО.

На протяжении 2015 года компания Check Point проанализировала свыше 600 шлюзов, обнаружив, что через 52.7% из них был загружен как минимум один файл, содержащий неизвестное вредоносное ПО. В среднем на каждый шлюз приходилось 2 372 зараженных файла.

На стороне пользователей атаки были более частыми и разнообразными. Многие организации столкнулись с необходимостью сдерживать поток из более чем 971 загрузки неизвестного вредоносного ПО в час, что более чем в 9 раз больше по сравнению со 106 загрузками в час в предыдущий год.

Большинство пользователей знает, что риск заражения для отдельных типов файлов выше, чем для других. Как и следовало ожидать, .exe файлы составляют около 30% зараженных файлов, в то время как форматы архивов, такие как .zip и .jar занимали более 16% в 2015 году. Рост вредоносного ПО продолжается и для

75%

ОРГАНИЗАЦИЙ УЗНАЛИ, ЧТО ОНИ ЗАРАЖЕНЫ БОТАМИ

52%

ШЛЮЗОВ ЗАГРУЗИЛИ КАК МИНИМУМ ОДИН ФАЙЛ С НЕИЗВЕСТНЫМ ВРЕДОНОСНЫМ ПО

971

СЛУЧАЙ С НЕИЗВЕСТНЫМ ВРЕДОНОСНЫМ ПО ИМЕЕТ МЕСТО В ОРГАНИЗАЦИИ КАЖДЫЙ ЧАС

28%

ФАЙЛОВ, ЗАРАЖЕННЫХ ВРЕДОНОСНЫМ ПО, БЫЛИ В ФОРМАТЕ SWF (SMALL WEB FLASH)

2.3 Источник: Check Point Software Technologies

типов файлов, которым большинство пользователей доверяют, таких как PDF, Flash или файлы Microsoft Office. Таким образом, хакеры используют преимущества работы с теми типами файлов, которые вызывают меньше подозрений. В 2015 году файлы формата Microsoft Office встречались среди вредоносных более чем в 9% случаев, а PDF – в 7.5%.

Процент использования Flash как механизма доставки вредоносного ПО продолжает расти, составив 28% загруженных файлов, зараженных неизвестным вредоносным ПО. В случаях, когда вредоносный контент запакован как файл Flash, пользователь гораздо в меньшей степени ожидает, что может произойти заражение. Заражения, связанные с вредоносной рекламой или эксплоитами «drive-by», делают пользователя более открытым для воздействия большего числа вредоносного ПО без каких-либо специальных действий со стороны работника.

Использование неизвестного вредоносного ПО в атаках увеличивает вероятность успеха киберпреступников. При его применении хакеры работают более изощренно, достигая успеха путем меньшего числа действий. Создание неизвестного вредоносного ПО стало как нельзя более легким делом. Если используются антивирусные системы с блокировкой по известным сигнатурам, даже незначительная модификация существующего вредоносного ПО позволяет создать новый неизвестный вариант.

При 12 миллионах новых вариантов вредоносного ПО, обнаруживаемого каждый месяц, за последние два года было открыто больше нового вредоносного ПО, чем в сумме за предыдущие 29 лет[6].

СОСТОЯНИЕ ЗАЩИТЫ

Хотя скорости роста количества атак и заражения в 2015 году не такие экспоненциальные, как в 2013 или 2014 годах, эти показатели все еще стабильно увеличиваются. И несмотря на то, что скорость заражения немного замедлилась из-за использования лучшей защиты ресурсов в комплексе с обучением персонала, продолжающийся процесс размывания периметра сети и увеличение числа устройств, получающих доступ ко внутренней сети, продолжает усложнять задачу защиты информации.

В современном лишенном границ мире с облаками, мобильными устройствами, IoT и гибридными ЦОД инструменты кибербезопасности должны обеспечивать детальный контроль над всеми средами и сегментами сети. При смещении акцента от возможного к обязательному применению традиционные технологии «песочниц» вносят задержку на обработку данных. Для защиты от сегодняшних атак упор должен быть сделан на скорость и предотвращение. Новые технологии позволяют проводить анализ поведения на уровне центрального процессора (ЦП), обнаруживая и блокируя вредоносное ПО в фазе эксплоита перед тем, как у него появляется возможность произвести свое развертывание.

Необходимость защиты от большого объема известных и неизвестных атак, а также атак «нулевого дня» диктует необходимость использования многослойного подхода к защите предприятия. В то время как не существует ни одной техники или технологии, позволяющей обеспечить полную защиту от всех векторов атак, хорошо организованный подход, сочетающий различные методы защиты и обнаружения, может минимизировать вероятность успешных атак. Совместно с дополнительными механизмами защиты для периода после заражения организации могут ограничить ущерб и сопутствующие потери.

В 2015 ГОДУ ЗАГРУЖЕНО В 4 РАЗА БОЛЬШЕ ВРЕДОНОСНОГО ПО

РЕКОМЕНДАЦИИ

С развитием IT меняется и ландшафт угроз. Чтобы быть впереди изменений, необходимо иметь многоуровневую архитектуру безопасности, которая обеспечивает предотвращение угроз в режиме реального времени, и единое управление, которое охватывает виртуальные, облачные и мобильные среды.

ПРЕДОТВРАЩЕНИЕ

1 СОЗДАЙТЕ МНОГОСЛОЙНУЮ КИБЕРЗАЩИТУ

Безопасность должна быть реализована на нескольких слоях, которые осуществляют автоматическую координацию действий между различными механизмами защиты, включая усовершенствованное предотвращение угроз, шлюз безопасности, контроль приложений, антибот, антивирус, использование идентификационной информации, антиспам и защиту электронной почты, систему предотвращения вторжений и фильтрацию URL.

2 ПРЕДОТВРАЩАЙТЕ ВРЕДОНОСНОЕ ПО «НУЛЕВОГО ДНЯ»

Неизвестные атаки делают традиционные «песочницы» неэффективными. Предотвращение угроз в режиме реального времени, блокирующее вредоносное ПО при первом контакте является новым стандартом для предотвращения угроз. Тем не менее даже самая лучшая «песочница» может пропустить угрозу, встроенную в документ. Изъятие активного контента из документов предотвращает скрытые угрозы и предоставляет пользователям своевременный доступ к безопасному контенту.

3 ИСПОЛЬЗУЙТЕ ВИРТУАЛЬНЫЕ «ЗАПЛАТКИ»

Постановка «заплаток» программного обеспечения является необходимой лучшей практикой, однако этого недостаточно для предотвращения угроз. Во-первых, не существует патчей для уязвимостей ПО «нулевого дня», которые еще только предстоит обнаружить исследователям в области безопасности. Для обнаруженных уязвимостей процесс создания и распространения «заплаток» поставщиками ПО может занять значительное время, оставляя сети открытыми для атак. И наконец, нехватка персонала IT-служб может также увеличить время развертывания «заплаток».

Постановка виртуальных «заплаток» с использованием IPS защищает от эксплоитов, которые нацелены на обнаруженные уязвимости и уязвимости «нулевого дня», которые не могут быть исправлены или еще не были закрыты «заплатками».

АРХИТЕКТУРА

1 УПРОСТИТЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

Переключение между консолями для управления безопасностью для каждого сегмента сети является неэффективным, способствует возникновению ошибок конфигурации и несоответствий между слоями безопасности. Управление всеми функциями безопасности, сегментами и средами с помощью одной консоли помогает уменьшить количество ошибок при согласовании политик для слоев защиты по всем сетевым сегментам.

2 УНИФИКАЦИЯ ЭЛЕМЕНТОВ УПРАВЛЕНИЯ

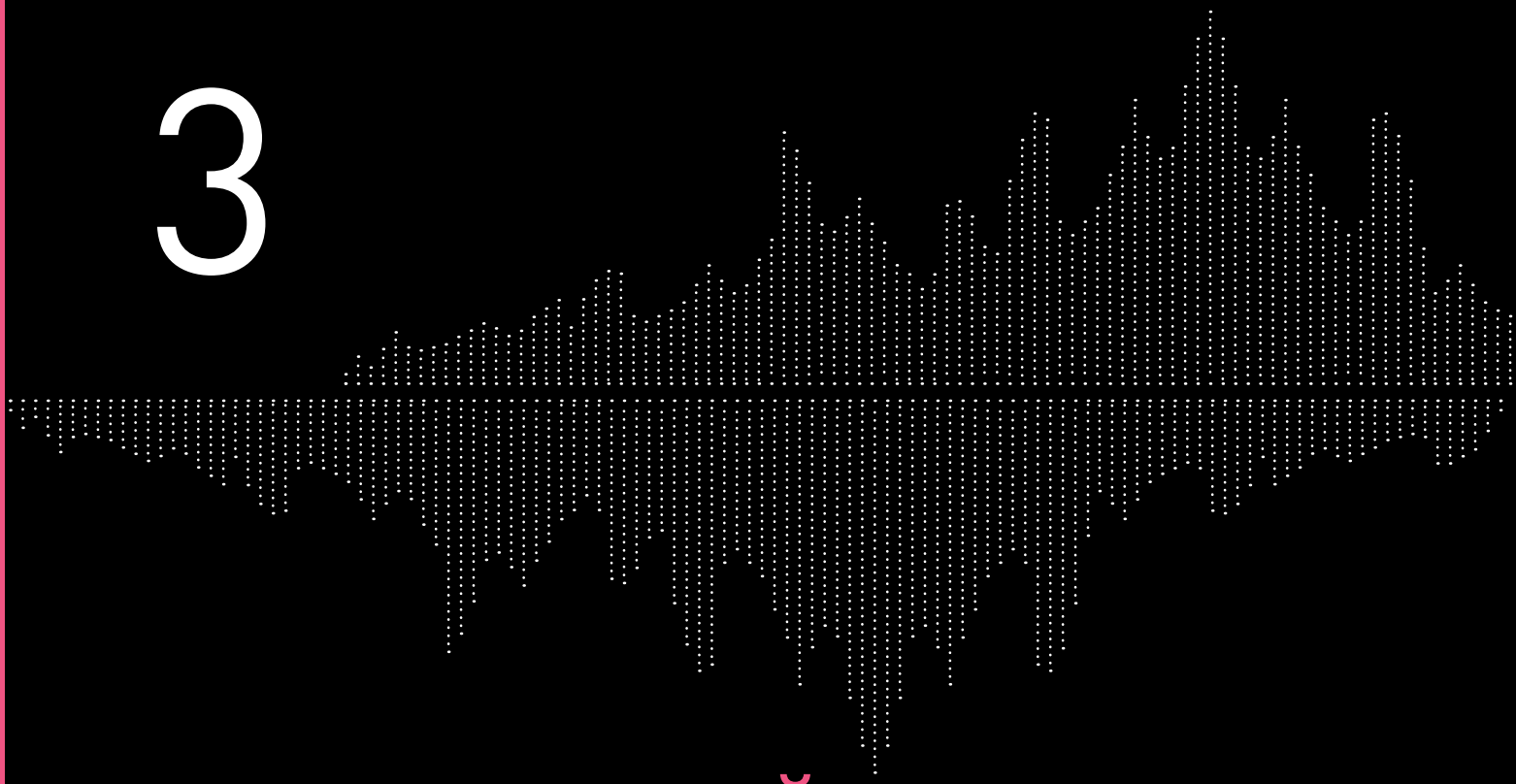
Внедряйте унифицированные элементы управления, которые распространяются на все сети, системы, конечные точки и среды, включая традиционные, облачные, виртуальные, мобильные, IoT и гибридные.

УЗНАЙТЕ БОЛЬШЕ

checkpoint.com/sandblast

ДЕЙСТВУЙТЕ

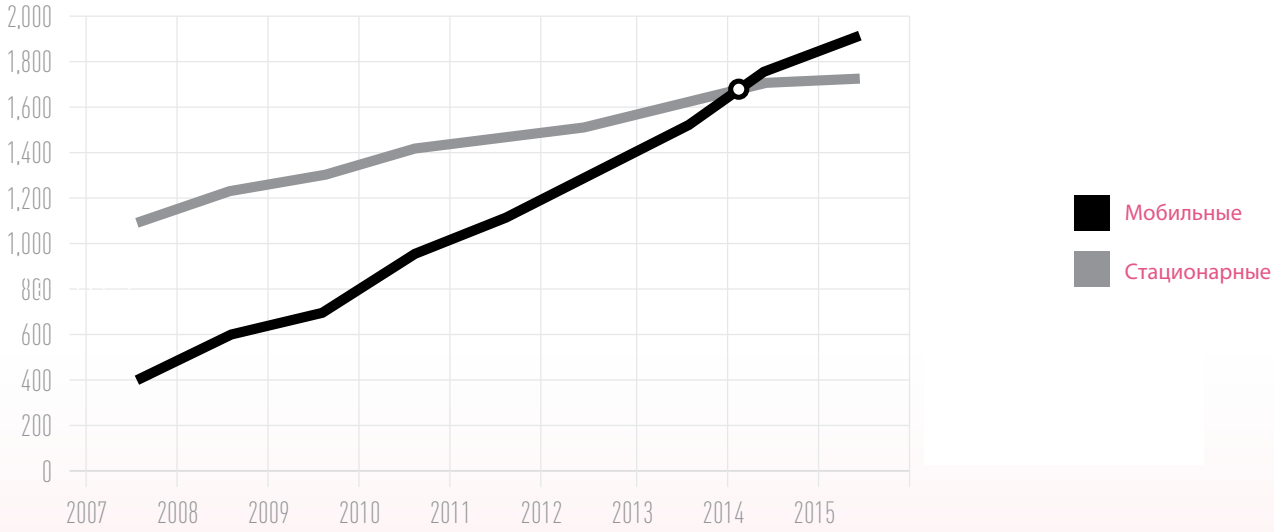
3



ОДНО УСТРОЙСТВО ДЛЯ СЕБЯ И БИЗНЕСА

> ***«Я получаю почту. Значит я существую»***
>
> Скотт Адамс, мультипликатор, создатель *Dilbert*

КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ В МИРЕ (МИЛЛИОНЫ)



3.1 Источник: The U.S. Mobile App Report, comScore Whitepaper, August 2014

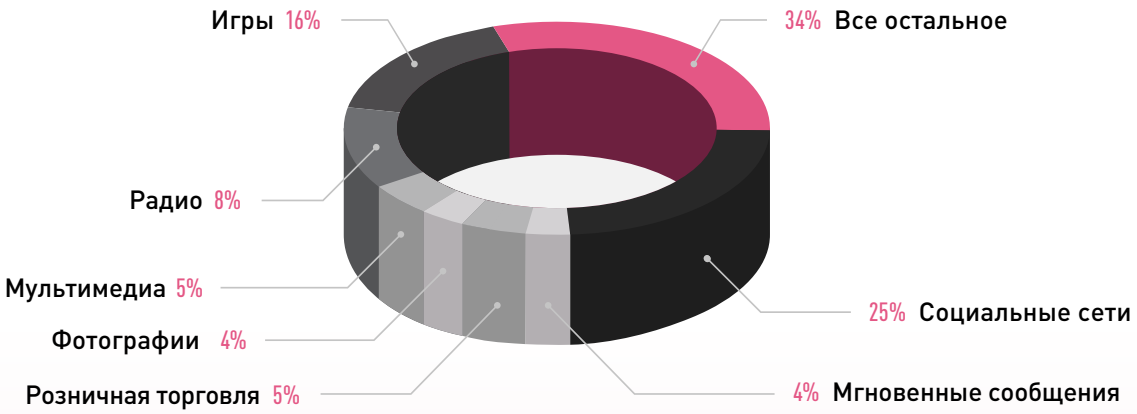
Более мощные, чем когда-либо, мобильные устройства постоянно совершенствуют доступность и производительность работников. Большинство сотрудников носят с собой такие, ставшие доступными устройства на протяжении всего своего рабочего дня, неважно пользуясь ими или нет. При такой распространенности мобильные устройства интегрируются в саму ткань бизнеса путями заметными и незаметными для нас.

С увеличением числа мобильных пользователей появляется переломный момент в характере использования, как мы можем видеть в отчете comScore. Во-первых, мобильные устройства обошли стационарные по доступу в медиа и веб-сайтам[1]. Наряду с этим пользователи стали более комфортно размывать грань между своей работой и личным использованием таких устройств. И неважно, поддерживает это компания или нет, сотрудники делают работу на своих личных устройствах и получают доступ к личной информации на своих рабочих устройствах, не всегда задумываясь о последствиях.

Использование смартфонов за последние четыре года возросло на 394%, а планшетов — более чем на 1700%. Совокупно использование этих платформ занимают 60% времени, затраченного на цифровые средства информации[2]. Третье исследование, проведенное comScore и Yahoo Flurry Analytics, показывает, что в среднем американцы проводят 162 минуты в день за использованием для различных своих действий мобильных устройств[3]. Вместе три эти тенденции подчеркивают возросшее желание мгновенного и непрерывного доступа к данным независимо от того, чье это устройство – компании или личное.

ВСЕ ЧТО НУЖНО ДЛЯ УЩЕРБА КАК ЛИЧНЫМ ТАК И КОРПОРТИВНЫМ ДАННЫМ И СЕТЯМ – ЭТО ОДНО ЗАРАЖЕНИЕ УСТРОЙСТВА

РАСПРЕДЕЛЕНИЕ ВРЕМЕНИ, ПРОВЕДЕННОГО В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ



3.2 Источник: U.S. Mobile App Report, comScore, August 2014

ГДЕ ПОДХОДИТ БЕЗОПАСНОСТЬ

Подобно вебсайтам в 90-х или удаленному доступу десятилетием позже мобильные устройства несут в себе как проклятие доступа, так и благословение бизнес-производительности. Как и в случае с трендами доступа ранее, пробелы в мобильной безопасности преследуют широкое освоение мобильных устройств, так как пользователи постоянно находят новые способы их использования.

Мобильная безопасность является трудной темой для предприятий. Она остается постоянным предметом спора между производительностью, защитой и частной жизнью. Предприятия и пользователи хотят одновременного увеличения производительности мобильных устройств и защищенности при доступе к корпоративной информации, но ни одной стороне не нравится ни идея односторонних ограничений, ни мысль о том, что за ними будут следить.

Пользователи ожидают повсеместного доступа и возможности использования личных устройств для работы. И это обязанность их работодателя выяснить, как обезопасить его собственные данные, но не так, что это означало бы предоставление любых прав по мониторингу их действий онлайн. Предприятие, с другой стороны, должно защищать корпоративные данные с дополнительными обязанностями по соответствию законам относительно персональных данных, различным для разных стран. Обязательные требования личной идентификации в одной стране могут нарушать законы о частной жизни в другой, и компания должна соответствовать и тому и другому.

ОДИН ИЗ ПЯТИ СОТРУДНИКОВ БУДЕТ ПРИЧИНОЙ ВЗЛОМА СЕТИ КОМПАНИИ ПОСРЕДСТВОМ ЛИБО ВРЕДОНОСНОГО ПО, ЛИБО ВРЕДОНОСНОГО WI-FI

Вредоносное ПО, фишинг, точки доступа-«ловушки» Wi-Fi и другие опасности онлайн угрожают и являются предметом беспокойства для каждого. Сотрудники не хотят становиться причиной взлома сети компании. Хотя один из пяти станет таковым либо из-за вредоносного ПО, либо из-за вредоносного Wi-Fi[4].

Мобильная безопасность должна включать в себя несколько строительных блоков, которые отвечают на различные аспекты вызовов безопасности:

Безопасные Контейнеры — предотвращают утечку данных, блокируя их обмен между рабочими и личными приложениями, размещенными на одном устройстве;

Предотвращение Мобильных Угроз — защищает от неизвестных угроз и вредоносного поведения приложений и предотвращает в реальном масштабе времени известные и неизвестные угрозы, а также угрозы «нулевого дня», направленные на устройства iOS и Android.

Ни одно из этих средств в одиночку не является достаточным, и, конечно, группам IT не нужна еще одна система для управления. Приоритетом должна быть интеграция всех компонентов в единую консоль безопасности.

ТЕНДЕНЦИИ МОБИЛЬНЫХ АТАК

По результатам анализа данных 2015 года мы получили новую перспективу относительно точек входа атак, а также типов похищенной информации. Тремя главными векторами атак на мобильные устройства являлись зараженные приложения, сетевые атаки и эксплоиты операционных систем. Как только киберпреступники получали доступ внутрь мобильного устройства, они осуществляли эксфильтрацию информации посредством электронной почты, аутентификационной информации учетных записей и встроенных датчиков таких как микрофон или камера, а также отслеживания местоположения устройства.

В период между сентябрем 2014 года и февралем 2015 года Apple iOS была наиболее частой целью киберпреступников, использовавших пять различных атак на ОС: XSSer, WireLurker, Masque, Pawn Storm и Commercial mRAT. К осени 2015 года число атак возросло почти в пять раз как на Apple iOS, так и на Android.

МОБИЛЬНЫЕ УГРОЗЫ

3.3 Источник: Check Point Software Technologies

Мобильность: пять новых тенденций вредоносного ПО для Android

Доминирование ОС Android в мобильных компьютерах открыло новую эру вредоносных программ. За считанные годы изощренность вредоносного ПО, нацеленного на устройства Android, существенно возросла. Вот некоторые из самых последних угроз для Android, обнаруженных исследователями мобильной безопасности компании Check Point.

1. Обфускация. По мере того как поставщики средств безопасности борются с вредоносным ПО для Android, киберпреступники развивают новые способы, чтобы скрыть или обфусцировать (сделать неявным) вредоносное ПО. Шифруя вредоносные компоненты своего ПО, злоумышленники могут обойти многие решения в области безопасности, включая Google Bouncer, который защищает магазин приложений Google Play. Некоторые авторы вредоносных программ также обфусцируют ключи, которые они используют для раскрытия вредоносных компонентов, делая вредоносные программы еще более сложными в обнаружении.

2. «Капельницы». Вирусописатели используют «капельницы», чтобы проникнуть в Google Play с вредоносными приложениями. Схемы «капельница» начинаются с загрузки, казалось бы, доброкачественного приложения в Google Play. Google утверждает такое приложение, так как оно не содержит вредоносного кода. После того, как пользователь устанавливает приложение на устройстве, приложение обращается к серверу атакующего, загружая вредоносный компонент на устройство пользователя.

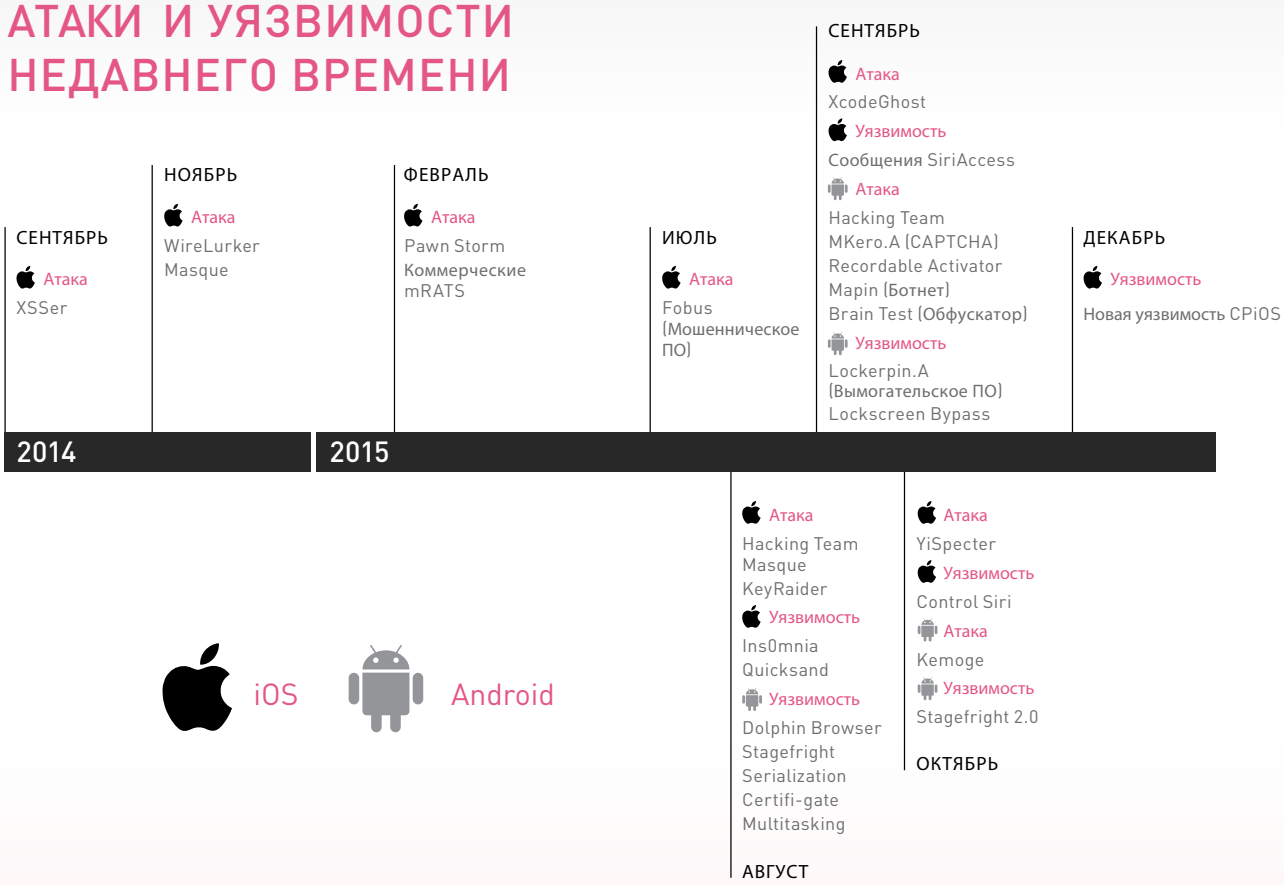
3. Избыточность. Зачастую вредоносное ПО состоит из нескольких компонентов, каждый из которых предназначен для различных вредоносных целей. Два компонента могут быть разработаны для достижения той же цели с разных направлений. Таким образом, если один компонент вредоносных программ обнаружен и обезврежен, атака может продолжаться с использованием второго компонента. Даже если критический компонент отключен, для атакующего проще изменить эту часть, чем изменить все вредоносное ПО целиком.

4. Постоянство. Создатели вредоносного ПО используют несколько тактик, чтобы гарантировать, что их вредоносные программы останутся на зараженном устройстве. Например, они могут скрыть значок приложения, задерживать вредоносную активность в течение нескольких недель или месяцев, маскироваться под различные приложения и получить повышенные привилегии, чтобы предотвратить его удаление пользователями. Основная цель все та же: оставаться на устройстве для достижения вредоносной цели.

5. Эскалация привилегий. В последнее время создатели вредоносного ПО использовали методы социальной инженерии, чтобы обманом вынудить пользователей дать им повышенные привилегии. Другие злоумышленники используют эксплоиты для получения привилегированных прав доступа. В силу того, что существует и используется множество различных версий Android, каждая со своими уязвимостями, может пройти несколько месяцев пока «заплатки» безопасности достигнут пользователей Android. Это оставляет их уязвимыми для известных угроз в течение длительных периодов времени. Создатели вредоносного ПО используют эти задержки для направления на таких пользователей эксплоитов, способных злоупотребить известными недостатками в устройствах Android.

Создатели вредоносных программ являются столь же инновационными и хорошо финансируемыми, сколь они настойчивы. Несомненно, они будут продолжать разрабатывать новые методы для достижения своих целей. Для того чтобы находиться на шаг впереди эволюционирующих угроз для Android, предприятия и пользователи должны использовать передовые решения, предотвращающие мобильные угрозы.

АТАКИ И УЯЗВИМОСТИ НЕДАВНЕГО ВРЕМЕНИ



3.4 Источник: Check Point Software Technologies

В целом, существуют пять основных категорий атак и уязвимостей, бросающих вызов миру мобильных устройств. Ими являются:

1. Системные уязвимости. Вариации в операционных системах предлагают широкий спектр векторов атак. Особенно уязвима ОС Android, поддерживающая более чем 24 000 различных типов смартфонов и планшетов. Выпуск «заплаток» и обновлений безопасности может занять несколько недель или даже месяцев разработки и тестирования после первой публикации эксплоита, что делает многих пользователей легкой добычей.

2. Корневой доступ и Изменения конфигурации. Получение корневого доступа или джейлбрейк телефона не только дает более широкий доступ энтузиастам, но также и киберпреступникам. Серии атак, направленных на обход политики ограничений изменения настроек и конфигурации позволяют внести легкие изменения, о которых пользователи даже не будут подозревать.

3. Перепакованные, или Поддельные приложения. Подобно фишингу поддельные приложения выглядят очень реально, но имеют дополнительные неожиданные особенности. Вредоносные программы удаленно захватывающие управление, включающие микрофон устройства, камеру или слежение GPS в настоящее время получили большое распространение и стали весьма популярными.

4. Трояны и Вредоносное ПО. Встраивание вредоносного кода в прикрепленные файлы и приложения остается большой проблемной областью для мобильных устройств. Многие из них не имеют никакого антивируса или средства предотвращения угроз, кроме того на

небольших экранах гораздо труднее заметить такие детали, как неточности в графическом интерфейсе приложения.

5. Атаки «Человек посередине». Бесплатные и общественные точки доступа Wi-Fi очень легко имитировать, что делает такие атаки более распространенными. Подмена сертификатов безопасности для шифрования облегчает перехват, изменение проходящих данных или установку троянов.

Безопасные мобильные вычисления требуют от пользователей осведомленности и бдительности по отношению к угрозам, но часто пользователи не проявляют таких качеств. В то время как типы атак меняются, цель предприятия остается неизменной. Команды безопасности предприятия должны создать барьер между личным устройством работника и сетью компании. Достижение этого требует нескольких элементов, работающих параллельно.

СОЗДАВАЯ БАРЬЕР

Система предотвращения мобильных угроз создает надежный барьер. Она использует поведенческий анализ для блокировки угроз до того, как они проникнут в мобильные устройства, а также предоставляет хороший обзор попыток атак.

На более высоком уровне интеграция систем управления устройствами и предотвращения угроз с вашим межсетевым экраном нового поколения и виртуализированной облачной защитой усиливает характеристики как обнаружения, так и блокировки попыток атак. Конечно, все эти ресурсы требуют управления, поэтому их интеграции в единую платформу управления имеет важное значение для эффективности вашего барьера мобильной безопасности.

> ***«Как только вы приносите в мир жизнь, вы должны защищать ее. Мы должны защищать ее, изменяя мир» .***
>
> Эли Визель, писатель, политический активист

ЛУЧШИЕ ПРАКТИКИ ДЛЯ ЗАЩИТЫ ВАШЕГО МОБИЛЬНОГО БИЗНЕСА

ДЕЙСТВУЙТЕ

1 ОБУЧАЙТЕ ВАШИХ СОТРУДНИКОВ

Мы часто недооцениваем, до какой степени наши смартфоны и планшеты предоставляют нам конфиденциальность и безопасность. Убедитесь, что ваши сотрудники понимают угрозы, такие как фишинг и незащищеные точки доступа Wi-Fi. Ведь становясь их жертвой, они не только ставят под угрозу конфиденциальность собственных личных данных, но также могут поставить под угрозу конфиденциальность корпоративной информации на своих мобильных устройствах.

2 ОПРЕДЕЛИТЕ СТЕПЕНЬ ПРИЕМЛЕМОГО РИСКА

Не все предприятия имеют такие же требования в области мобильной безопасности, и не все работники требуют такого же уровня защиты. Важно также найти правильный баланс между защитой от угроз и удобством для пользователя. Рассмотрите предписывающий подход к безопасности мобильных устройств, который решает эти две задачи. Определите политику, основанную как на ролях людей, которые имеют доступ, так и видах защиты, которые имели бы смысл для различных типов конфиденциальных данных.

3 СЛЕДИТЕ ЗА СОБЛЮДЕНИЕМ БАЗОВОЙ ГИГИЕНЫ

Удивительно большое число людей не в полной мере понимает основы мобильной безопасности: разрешить пароли или биометрические замки, активировать возможности удаленного определения местоположения и стирания информации, использовать шифрование устройства, если это доступно. Убедитесь, что конечные пользователи всегда обновляются до последней версии операционной системы. Даже такие основные шаги для поддержания безопасности мобильных устройств и данных могут оказать большое влияние на ваши общие усилия по защите и также сохранят в безопасности их личные данные.

4 РАЗДЕЛИТЕ РАБОЧИЕ И ЛИЧНЫЕ ДАННЫЕ

Создание барьера безопасности между конфиденциальными корпоративными и личными данными сотрудников, которые они содержат на своих мобильных устройствах является отличным способом, чтобы помочь уберечься от ошибок. Сообщения и файлы, хранящиеся в безопасных контейнерах, могут быть защищены и зашифрованы отдельно от личного пространства на устройстве. И управлять безопасными контейнерами для управления данными будет быстрее и проще, чем управлять устройствами и многочисленными политиками.

5 ИНВЕСТИРУЙТЕ В НЕОПРЕДЕЛЕННОЕ БУДУЩЕЕ

Вы можете быть уверены, что угрозы, о которых вы не знаете сегодня, являются теми, которые застанут вас врасплох завтра. Поэтому важно вкладывать средства в технологии предотвращения, которые способны опережать угрозы. Но также они должны интегрироваться с решениями, которые у вас есть на сегодняшний день, чтобы помочь им поддерживать мобильные устройства более защищенными при расширении возврата ваших инвестиций.

УЗНАЙТЕ БОЛЬШЕ

checkpoint.com/mobilesecurity

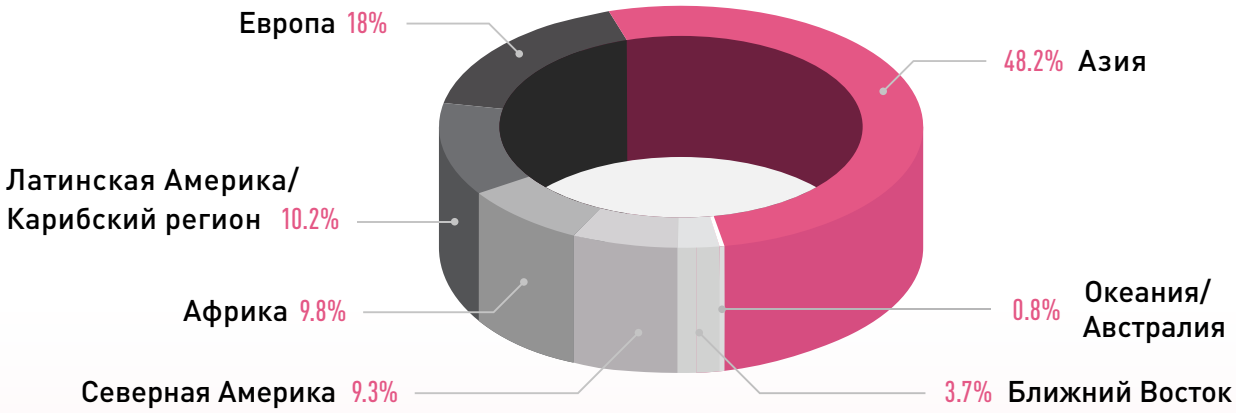
4

ИЗУЧАЯ ПАТТЕРНЫ АТАК

«Все технологии надо считать виновными, пока они не докажут свою невиновность».

Джерри Мандер, писатель
и общественный деятель

ПОЛЬЗОВАТЕЛИ ИНТЕРНЕТА ПО РЕГИОНАМ



4.1 Источник: Internet World Stats, www.internetworldstats.com/stats.htm, November 2015

Для того чтобы находиться на шаг впереди атакующих, требуется понимание методов, которые они используют, путей, которыми они идут, для того чтобы достичь успеха. Важнейшую информацию для этого нам даст изучение паттернов и тенденций атак.

В 2015 году «вымогательское» вредоносное ПО появилось как новая сенсационная методология атак, вынудившая как компании, так и индивидуальных пользователей платить выкуп за восстановление доступа к файлам, зашифрованным вредоносной программой. Отсутствие резервных копий или большое время, требуемое на восстановление данных из резервных копий, приводило многие компании к решению заплатить за ключ для дешифровки их данных и одновременно фокусироваться на предотвращении следующей атаки. Как скоро находились решения для противодействия одному типу атак, так же скоро или на их месте появлялись новые альтернативные технологии, или векторы атак переключались на другие методы.

Анализ обнаруживает четкие паттерны в этих вновь возникающих угрозах. Например, несмотря на то, что 50% всех пользователей Интернета в мире находятся в Азии, они демонстрируют наименьший уровень вредоносного поведения[1]. В то же время США, представляющие менее 10% пользователей в мире, являются «домом» для 26% организаций, осуществляющих хостинг вредоносного контента.

В то время как может сложиться впечатление, что атакующие постоянно изобретают новые виды атак, анализ показывает, что гораздо чаще вредоносное ПО и технологии атак используют преимущества предыдущих атак и известных слабых мест. Использование известного вредоносного ПО для создания новых неизвестных вариантов сравнительно недорого и несложно даже для начинающих хакеров. Наборы эксплоитов (EK, Exploit Kits) эволюционировали из простых пакетов инструментов для взлома в предложения типа «ПО для киберпреступлений как сервис» (CaaS, Crimeware as a Service). И в рамках этой модели CaaS заказчик платит за использование сервиса только в случае успешной установки вредоносной программы на машину-«жертву». У хакеров есть большое множество

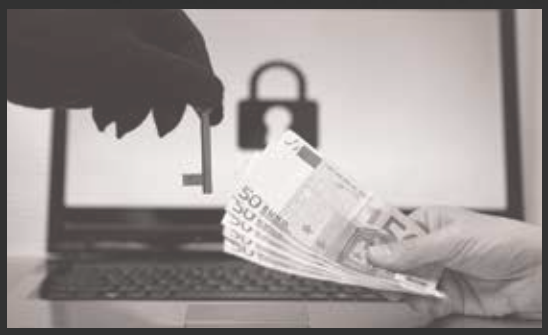
«Вымогательское ПО»: украсть умнее, а не больше

Подобно легальным компаниям операторы угроз должны время от времени менять свои инструменты, когда их «продукт» «теряет сцепление». Анализируя данные этого года, Check Point застал преступников в момент увеличения потока атак «вымогательского» вредоносного ПО с одновременным уменьшением масштабов использования троянов для банков. Мы полагаем, что есть несколько причин того, почему ПО-«вымогатель», которое шифрует пользовательские файлы и затем требует деньги за их расшифровку, стало популярным выбором атаки для тех, кто хочет «украсть умнее, а не больше».

Украсть больше: вредоносное ПО для банков

Провести налет на банковские учетные записи было достаточно легким делом: направь пользователя на поддельную зеркальную страницу банковского веб-сайта, запиши данные аутентификации пользователя и, используя эти данные, зайди на реальный сайт банка для перевода средств на счет посредника. Сейчас, после того как банки ввели дополнительные расширенные меры безопасности, атакующие должны бороться с двухфакторной аутентификацией и требованием, чтобы все соединения с банком происходили с известных компьютеров и устройств.

Кроме того, перевод средств может вызвать блокировку переводов или счета со стороны систем противодействия мошенничеству (антифрод). Атакующие также должны подделать контент для имитации каждого веб-сайта банка-«жертвы».



Украсть умнее: «вымогательское» ПО

«Вымогательское» ПО может атаковать любого пользователя, не только клиентов банков, что существенно расширяет группу потенциальных жертв по сравнению с вредоносным ПО для банков. ПО-«вымогатель» быстро вынуждает жертву заплатить, иначе он потеряет доступ к жизненно важному контенту. И все это без необходимости входа в систему и записи его аутентификационных данных. После шифрования данных жертвы уведомление о выкупе сообщает пользователю, как он должен заплатить или как найти «владельца» в анонимизированном подполье сети TOR. Последние данные показывают, что «вымогательское» ПО может уже содержать ключ шифрования, так что в этом случае отсутствует необходимость связи с внешним

сервером для получения такого ключа, чтобы начать атаку. Таким образом, один подход к вымогательству работает для всех пользователей без необходимости иметь множественные зеркальные веб-сайты. Единственным необходимым моментом является локализация кратких сообщений о требовании выкупа, хотя атакующие могут перенаправлять жертву к Google Translate для полного исключения необходимости локализации контента.

Для надежного доступа к деньгам вредоносное ПО-«вымогатель» использует для платежей альтернативные методы, такие как биткоин, позволяющие размыть переводы средств таким образом, что пользователь не сможет оспорить их, а банки – отменить. Переброска средств через кошелек биткоинов предотвращает попытки властей по отслеживанию транзакций. Кроме того, биткоины легко анонимно конвертировать в любую валюту.

Заключение

Четыре фактора обуславливают распространенность атак «вымогательского» ПО:

1. Целью ПО-«вымогателей» является гораздо более широкий круг потенциальных жертв.
2. Атаки имеют низкие накладные расходы, нет необходимости создавать и содержать индивидуальные поддельные зеркальные сайты для каждой цели.
3. Атаки легче реализуемы от начала до конца.
4. Платежи от жертв получаются с большей вероятностью и полностью не отслеживаются.

Предсказания

- Учитывая высокий доход и низкие накладные расходы, мы ожидаем увеличение числа атак «вымогательского» вредоносного ПО.
- Как и в случае вредоносного ПО для банков, мы ожидаем, что усовершенствованные средства безопасности вынудят ПО-«вымогатель» становиться более сложным и скрытным.
- По мере уменьшения числа пользователей, ставших жертвами «вымогательского» ПО, для увеличения прибыли от каждой атаки целями угрозы будут становиться более крупные организации. Мы ожидаем увеличение количества случаев, подобных атакам Samsam APT, на больницы и предприятия.
- Атаки будут перемещаться буквально внутри организации или в направлении разделяемых систем хранения, где данные могут быть зашифрованы. Это увеличит размер выплат путем вовлечения большего числа пользователей.
- Для организаций из общественного сектора мы ожидаем появление новых форм атак «вымогательского» ПО, таких как шантаж с применением угроз публикации компрометирующей информации, за предотвращение факта обнародования которой пользователи будут согласны платить выкуп.

вариантов, имеющих успешную историю применения, использующих известное и неизвестное ПО и готовые к эксплуатации точки входа в ОС Android и Microsoft Windows.

Находясь на шаг впереди, наша исследовательская группа анализирует широкий диапазон этих аспектов атак и постоянно совершенствует защитные механизмы против неизвестных угроз и угроз «нулевого дня». Такие аспекты включают в себя:

- местонахождение источника атаки;
- наиболее популярные типы атак;
- крупнейшие области уязвимостей;
- метод, которым атакующий проник внутрь.

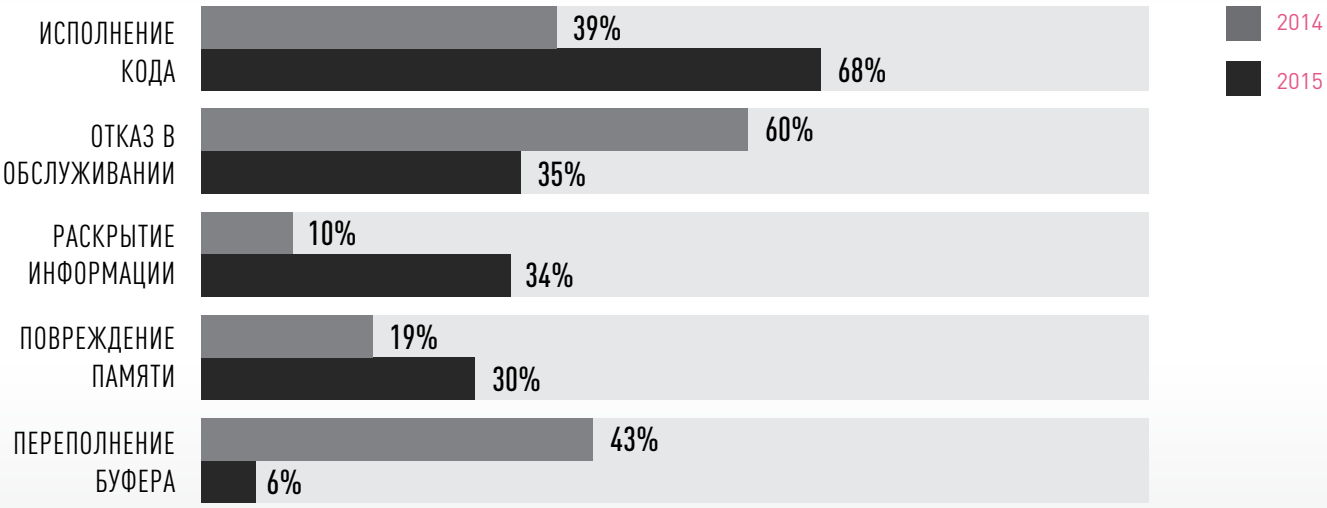
Эти данные, сами по себе и их комбинация, помогают компании Check Point изменять и тонко настраивать наши потоки аналитической информации по угрозам. Понимание тенденций в источниках атак, их целях и ключевых методах формирует наилучший подход для более эффективной защиты.

ОТКУДА НАЧИНАЮТСЯ АТАКИ

Из 7.4 миллиардов жителей нашей планеты менее 5% живет в Соединенных Штатах. Несмотря на это США лидируют в хостинге вредоносных файлов и вредоносных веб-сайтов. И хотя это выглядит диспропорционально, но США обеспечивает хостинг в два раза больший по процентному соотношению, чем число пользователей Интернет во всем остальном мире – в среднем 87.5% против в среднем 44.2% для остального мира[2]. Также США являются «домом» для многих компаний-лидеров Интернет, представляющих из себя притягательные цели. Технически грамотное население создает больше инноваций – как полезных, так и вредоносных.

4.2 Источник: Check Point Software Technologies

ПРОЦЕНТНОЕ СООТНОШЕНИЕ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ ВЕКТОРОВ АТАК



4.3 Источник: Check Point Software Technologies

НАИБОЛЕЕ ПОПУЛЯРНЫЕ ТИПЫ АТАК

Шлюзы безопасности Check Point ежегодно сообщают о наиболее излюбленных методах атак, или самых распространенных векторах атак. В 2014 году тремя наиболее крупными векторами атак были атаки «отказ в обслуживании», переполнение буфера и исполнение кода. В 2015 году количество эксплоитов, связанных с переполнением буфера, неожиданно существенно снизилось, сделав исполнение кода наиболее популярным вектором атак.

Ошибка Heartbleed Bug сделала атаку с использованием переполнения буфера широко известной историей и определило доминирование этого метода в 2014 году. Ее название происходит от эксплуатации ошибки чтения буфера в функции «пульса» (heartbeat) протокола TLS (Transport Layer Security).

С помощью этой ошибки атакующие использовали уязвимые сервера, для того чтобы итеративными действиями по частям в 64K собирать конфиденциальную информацию из памяти компьютера. Особое беспокойство вызывало то, что все эти действия нельзя было отследить. Дополнительную информацию на эти тему можно найти в блоге Heartbleed на сайте www.checkpoint.com.

Как только стали доступны «заплатки» для этой уязвимости, организации внедрили их и стали защищенными, вынудив атакующих переключиться на другие векторы атак. Хотя даже спустя годы после того, как «заплатки» к Heartbleed стали доступны, этот эксплоит все еще действует[3], так как не все организации эти «заплатки» установили.

В 2015 году паттерны атак сместились – около 68% организаций испытали как минимум одну атаку исполнения кода. Этот тип атак фокусируется на возможности удаленного исполнения кода в системе.

В 2015 ГОДУ КАЖДЫЙ ДЕНЬ ПРОИСХОДИЛО 36 АТАК ИСПОЛНЕНИЯ КОДА

Исполнение кода может запускаться даже в случае наличия защитных механизмов, что делает эти атаки еще более привлекательными. Одним из наиболее популярных методов является Возвратно-ориентированное программирование (ROP, Return-Oriented Programming). При открытии зараженного документа ROP перехватывает маленькие порции легитимного кода и перенаправляет ЦП на загрузку и исполнение вредоносного ПО. Кажущиеся для большинства систем безопасности легитимными, такие манипуляции на уровне ЦП чрезвычайно важно вовремя обнаруживать, чтобы остановить атаки до их начала.

«Отказы в обслуживании» продолжают оставаться привлекательными средствами атаки и нарушения работы систем, так что 35.1% организаций стали жертвами как минимум одной DDoS атаки. В 2015 году количество атак «распределенный отказ в обслуживании» выросло до 73 в день, превзойдя уж и без того высокий показатель в 48 событий в день в 2014 году.

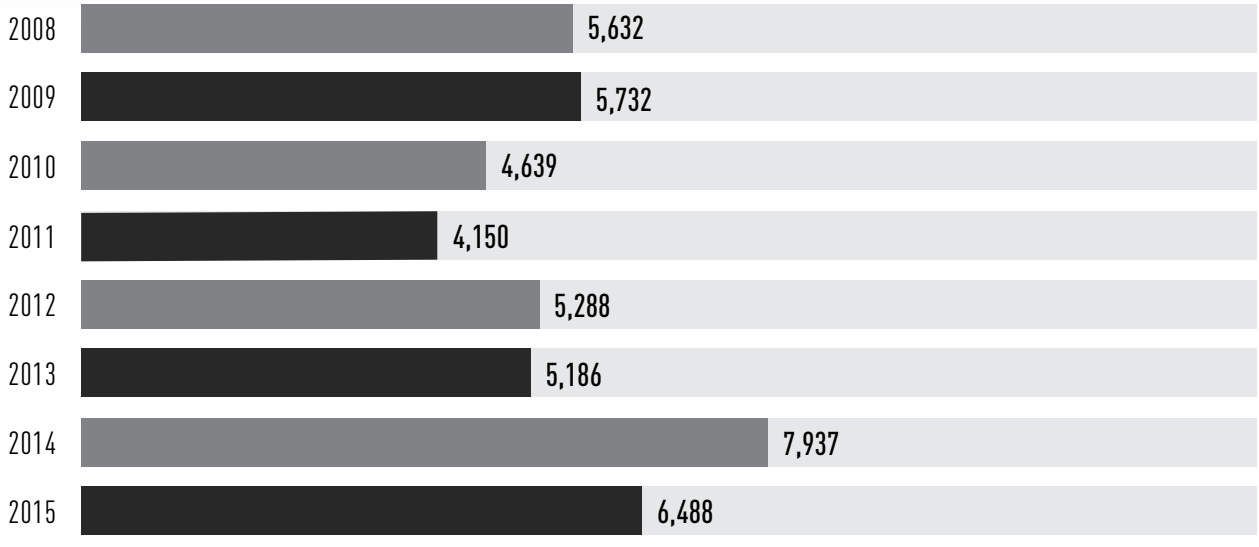
КАЖДЫЕ 20 МИНУТ

ПРОИСХОДИТ НОВАЯ АТАКА DDOS

ВЕЛИЧАЙШИЕ ОБЛАСТИ УЯЗВИМОСТЕЙ

Уязвимости существуют в большинстве программного обеспечения, на которое мы полагаемся в работе своего предприятия. Одним из крупнейших репозиториев организаций, извещающих об известных уязвимостях, является база данных CVE (Common Vulnerabilities and Exposures). Согласно ее данным общее число уязвимостей в 2015 годы выросло в среднем на 15% по сравнению со значениями, наблюдаемыми за последние восемь лет. Известное вредоносное ПО остается значительной угрозой, поэтому постоянное применение «заплаток» и обновлений является важнейшей задачей, относящейся ко всему программному обеспечению.

КОЛИЧЕСТВО ОБЩИХ УЯЗВИМОСТЕЙ И ОТКРЫТЫХ МЕСТ



4.4 Источник: Common Vulnerabilities and Exposures Database (CVE)

РАСПРЕДЕЛЕНИЕ СОБЫТИЙ БЕЗОПАСНОСТИ ПО КРУПНЕЙШИМ ПОСТАВЩИКАМ ПО

4.5 Источник: Check Point Software Technologies

Точки входа для взлома существуют везде. Борьба с известным вредоносным ПО требует непрерывного применения «заплаток» и обновлений по всему постоянно расширяющемуся спектру оборудования. Сервера, инструменты безопасности, компьютеры, беспроводные точки доступа и даже сетевые принтеры требуют регулярной установки «заплаток». С таким большим количеством устройств и сетей легко можно что-то упустить из виду.

КАК ХАКЕРЫ ПРОНИКАЮТ ВНУТРЬ

Хотя за последнее время этот показатель немного снизился, гигантская инсталляционная база решений Microsoft – от операционных систем и браузеров до решений для повышения производительности труда – продолжает занимать лидирующие позиции по количеству событий безопасности в ПО. Решения Joomla и WordPress для веб- и электронной коммерции подняли свои позиции за последний год. Приложения открытого кода и широко используемые системы управления контентом (CMS) на подобие вышеприведенных привлекают киберпреступников в качестве средств распространения вредоносного ПО.

В 2015 годы на сцене внезапно появилось и быстро вышло на верхние позиции SuperFish. Это рекламное ПО, обнаруженное на многих компьютерах Lenovo, пошло гораздо дальше простого перехвата поиска по веб. Расширяя свою зону деятельности на зашифрованный поиск, SuperFish устанавливало неуникальный доверенный корневой сертификационный центр (CA), позволяющий ему и умелым атакующим подделывать трафик HTTPS. Это давало злоумышленникам возможность выполнять классические атаки «человек посередине» без оповещения со стороны браузера. SuperFish стало популярным вектором атак, что вынудило правительство США выпустить в феврале 2015 года предупреждение для пользователей Lenovo[4], что Lenovo более не будет включаться в поставки оборудования.

После двух десятилетий уловки фишинга, убеждающие пользователя поделиться конфиденциальной информацией, такой как номера кредитных карт и аутентификационные данные для доступа к банковским системам, остаются популярным источником дохода киберпреступников. Поскольку пользователи стали уделять больше внимания рискам такого рода, а также из-за совершенствующихся методов обнаружения спама и фишинга, злоумышленники обратились к определенным технологиям, чтобы увеличить процент успеха в их фишинговых атаках. Однако такие новые подходы требуют больше времени и усилий для достижения сравнительно скромных доходов от каждого преступления. Для максимизации своего куша, как можно видеть, преступники перенацелили свои фишинговые схемы с массовых атак на случайных пользователей в сторону сфокусированных атак на значимых сотрудников предприятий.

Фишинг: большой крючок для ловли предприятий

Эволюция фишинга

«Гарпунный фишинг» – такое название получили сфокусированные атаки, использующие обман и социальную инженерию для хищения аутентификационных данных и другой значимой информации у определенных специфических групп пользователей, определенных компаний или у определенных людей. Для проведения успешной «гарпунной» фишинговой атаки злоумышленник инвестирует гораздо больше времени и усилий, проводя разведку для сбора информации о намеченных целях. Например, атакующий может изучить, решениями каких производителей пользуется компания, или кто является поставщиком бухгалтерских услуг, или какие бизнес-партнеры есть у компании. Атакующий затем определяет конкретных людей и их адреса электронной почты, посылая им поддельные сообщения, кажущиеся легитимными и вызывающие всяческое доверие. Такие сообщения электронной почты либо побуждают пользователя открыть вложение, либо отсылают получателя на высококачественный поддельный веб-сайт. Чистый эффект от применения социальной инженерии выражается в гораздо более высоком проценте успеха таких атак. Кроме того, компании обычно имеют гораздо более глубокие «карманы», так что куш от каждой операции «гарпунного» фишинга получается значительно большим.

Охота на китов

«Гарпунный» фишинг получил свое дальнейшее развитие в атаках, называемых «охота на китов». Эта особая форма «гарпунного» фишинга обычно нацелена на руководителей высшего звена, о чем говорит ее название «фишинг больших рыб». Например, в случае «охоты за китом» злоумышленник может посылать поддельное сообщение электронной почты, замаскированное под письмо от исполнительного директора (CEO) к директору по финансам (CFO) с требованием перевести деньги на определенный банковский счет. При наличии эффективного исследования социальной инженерии о том, что могло бы выглядеть достоверным для высшего руководства, такой подход может убедить многих профессионалов попасться в ловушку. К моменту, когда правда выйдет наружу, деньги будут уже далеко. Для того, чтобы замести следы, некоторые злоумышленники задействуют подставные банковские счета, используемые только для одной атаки. Согласно данным ФБР за последние два с половиной года атаки типа «охота на китов» лишили компании средств на сумму свыше 2.3 миллиардов долларов США.

С уверенностью можно сказать, что злоумышленники будут продолжать развивать инновационные пути обмана пользователей для компрометации их систем. Для того чтобы пользователи не становились жертвами такого обмана, необходима комбинация регулярных тренингов по повышению информированности и применения передовых технологий.

ЛУЧШИЕ ПРАКТИКИ

Предприятия нуждаются в единой стратегии предотвращения угроз. Известные вредоносные программы до сих пор остаются серьезной угрозой. Новые технологии приносят значительный рост неизвестных вредоносных программ и вредоносного ПО «нулевого дня», требующих решений, которые могут предотвратить известные и неизвестные угрозы в режиме реального времени, в том числе даже использующие методы уклонения. Мониторинг исходящих соединений также важен для обнаружения аномального поведение до момента нанесения ущерба.

1 УНИФИЦИРОВАННАЯ АРХИТЕКТУРА

Защищайте сети от сложных угроз вредоносного ПО и угроз «нулевого дня». Расширьте механизмы защиты на пользовательские конечные устройства и облачные сервисы и виртуальные среды для предотвращения угроз по всей организации.

2 ЗАЩИЩАЙТЕ ВСЕ СРЕДЫ

Используйте независимую от среды архитектуру безопасности для единообразного предотвращения угроз ЦОД, облачным платформам, программно-определяемым ЦОД, SaaS, гибридным и мобильным средам.

3 ПРЕДОТВРАЩАЙТЕ ВРЕДОНОСНОЕ ПО «НУЛЕВОГО ДНЯ» И ЭКСПЛУАТАЦИЮ

Увеличившиеся в объеме атаки исполнения кода, включающие такие передовые технологии, как Возвратно-ориентированное программирование (ROP), обходят традиционные «песочницы». Эмуляция угроз на уровне ЦП позволяет застигнуть вредоносное ПО в фазе эксплоита, перед тем как хакеры смогут применить технологию уклонения для обхода «песочницы».

4 УПРАВЛЯЙТЕ ВСЕЙ ЗАЩИТОЙ ЧЕРЕЗ ОДИН ЭКРАН

Унифицированное управления безопасностью повышает точность настроек защиты и улучшает видимость при мониторинге журналов.

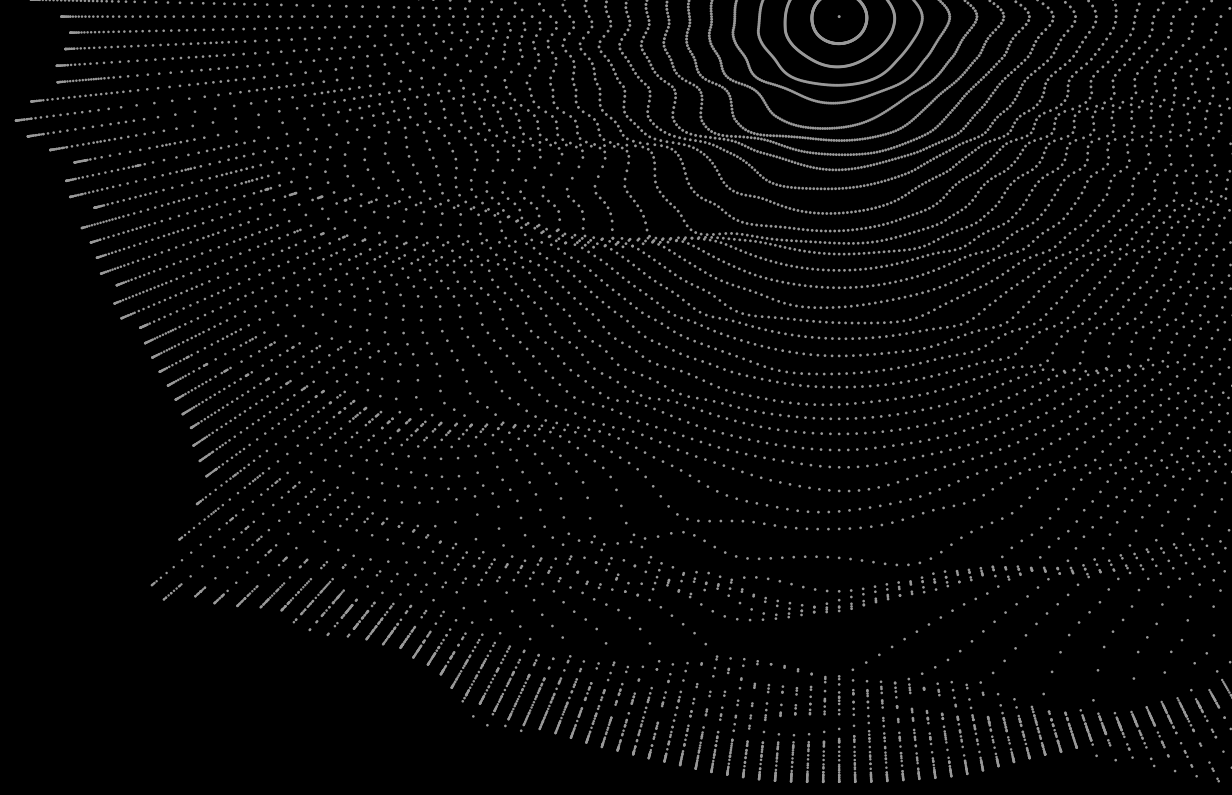
5 ИМЕЙТЕ ПЛАН РЕАГИРОВАНИЯ НА СЛУЧАЙ ИНЦИДЕНТА

Пока у вас нет системы предотвращения в реальном времени, вы нуждаетесь в реагировании на инциденты. Команда реагирования на инциденты Check Point доступна в режиме 24x7x365 для расследования и решения действия вредоносного ПО и других событий безопасности, воздействующих на вашу организацию.
Звоните 866-923-0907 или отправьте сообщение электронной почты на адрес emergency-response@checkpoint.com.

УЗНАЙТЕ БОЛЬШЕ

checkpoint.com/management

ДЕЙСТВУЙТЕ



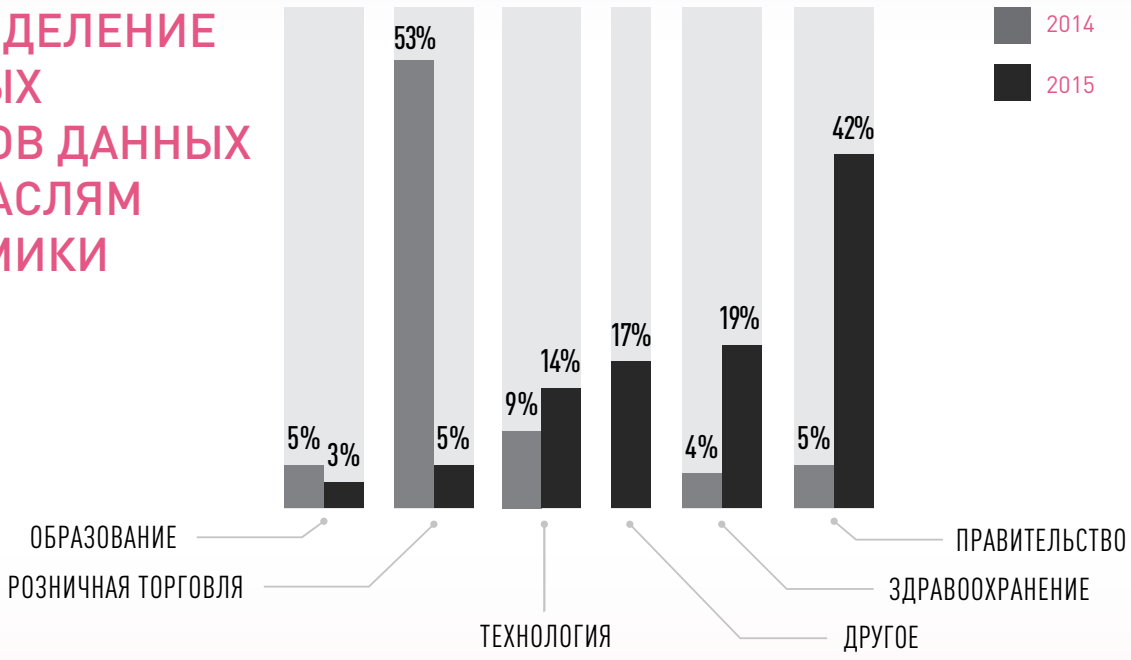
5

ВОЛНОВЫЕ ЭФФЕКТЫ НЕЗАЩИЩЕННОСТИ

«Все, что мы делаем, даже малейшее, что мы делаем, может иметь волновой эффект и последствия, которые от этого исходят. Если бросить камешек в воду на одной стороне океана , он может создать приливную волну на другой стороне».

Виктор Уэбстер, актер

РАСПРЕДЕЛЕНИЕ КРУПНЫХ ВЗЛОМОВ ДАННЫХ ПО ОТРАСЛЯМ ЭКОНОМИКИ



5.1 Источник: Gemalto's Breach Level Index

Ущерб от киберпреступности стоит больше, чем цена украденной информации. Волновые эффекты часто более разрушительны, нежели фактическое хищение. Потеря доверия как со стороны вашей компании, так и со стороны ваших клиентов толкает вас к перерасходу средств на устранение последствий атаки, заставляет чувствовать себя обязанными платить пострадавшим поставщикам и партнерам и по крайней мере в течение некоторого промежутка времени является причиной ухода ваших клиентов.

Если бы кто-то вломился в ваш дом, вы чувствовали бы себя пострадавшим. Ваша страховая компания возместила бы вам стоимость каких-либо украденных предметов, но ощущение безопасности не может так же легко быть восстановлено. Вы стали бы после этого осторожным, возможно, чрезмерно, инвестируя в модернизацию системы безопасности, или стали бы хранить ценности за пределами вашего дома, или даже стали бы меньше выходить на улицу – все это, чтобы чувствовать себя в большей безопасности.

Вы бы инвестировали в изменение своих привычек не для того, чтобы быть в большей безопасности, но чтобы ощущать себя в большей безопасности, что может оказаться более дорогостоящим. Корпоративные взломы ничем не отличаются от этого. Здесь тоже волны могут стать более разрушительными, чем первоначальный всплеск.

Расчет финансовой ценности информации является сложной задачей, хотя на сегодняшний день существует несколько способов, чтобы ее оценить. В 2013 и 2014 годах волна взломов в попытке получения персональных данных захлестнула такие громкие имена экономики, как Anthem, Target, Home Depot и Sony. При средней цене взломанных данных на уровне 154 доллара США за одну запись (согласно Ponemon Research) и учитывая, что многие инциденты затронули тысячи или даже миллионы записей, средняя общая стоимость одного взлома данных выросла на двадцать три процента до 3.79 миллионов долларов США в 2015 году[1].

По данным исследовательской фирмы Gemalto в 2015 году число взломов незначительно снизилось с 1 млрд. записей в 2014 году до чуть более 700 миллионов в 2015 году[2]. Хотя это и выглядит многообещающим, не все записи имеют одинаковую ценность.

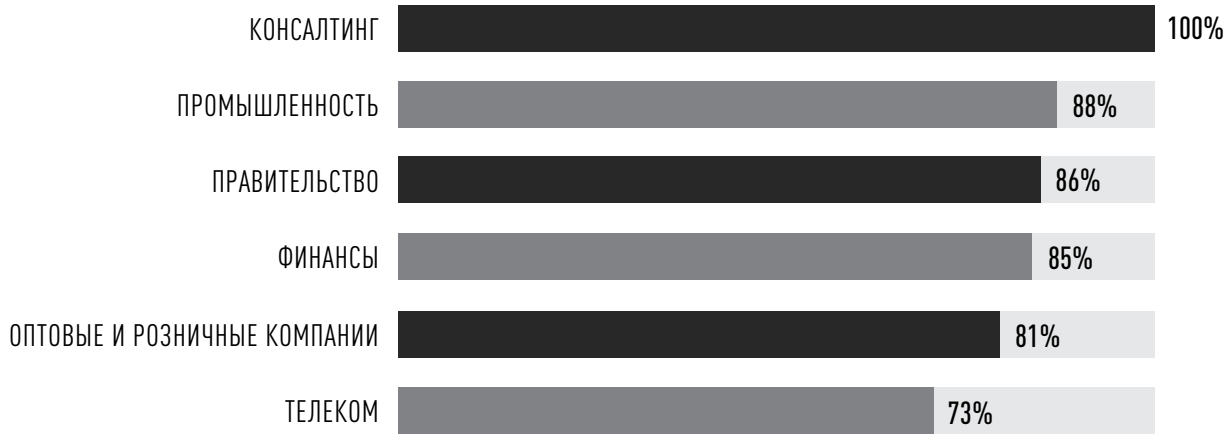
В 2014 году основной целью были данные кредитных карт, которые имеет относительно короткий период «свежести»: компании кредитных карт достаточно быстро блокируют карточные счета и перевыпускают карты. В 2015 году атакующие переориентировались на данные с большим жизненным циклом – персональным данным и к кражам идентичности. Кроме того, злоумышленники перешли от сосредоточения своей деятельности в основном на розничной торговле и финансовых организациях в 2014 году на государственные и медицинские учреждения в 2015 году. Чем дольше срок годности записи, тем дороже будет зачистка.

Расчет первоначального ущерба от взлома включает в себя несколько прямых расходов:

- стоимость украденной интеллектуальной собственности;
- простои, связанные с анализом, ремонтом и повторным укреплением всех взломанных систем;
- проверку всех систем компании на скрытое заражение;
- восстановление системы из резервных копий, в том числе проверки этих резервных копий на наличие уязвимостей;
- изменение процедур безопасности и обучения персонала новым средствам защиты.

Менее очевидны затраты, вызванные «волной», однако они быстро превышают затраты прямые. В случае взлома Target в конце 2013 года было украдено 40 миллионов кредитных и дебетовых карт, что стоило Target 248 миллионов долларов США прямых расходов за первые два

ПРОЦЕНТ КОМПАНИЙ, ИСПЫТАВШИХ ПОТЕРЮ ДАННЫХ



5.2 Источник: Check Point Software Technologies

ПОТЕРИ ДАННЫХ БИЗНЕСА УВЕЛИЧИЛИСЬ ЗА ПОСЛЕДНИЕ ТРИ ГОДА БОЛЕЕ ЧЕМ НА 400%

5.3 Источник: Check Point Software Technologies

года, но это число продолжает расти. Некоторые источники оценивают, что в конечном счете затраты превышают 2.2 млрд. долларов США, если включить сюда потери от мошеннических платежей, возмещения ущерба поставщикам, а также штрафы в результате исков. Аварийное восстановление является дорогостоящим делом.

Взломы безопасности, как правило, связаны с кражей информации, и зачастую более мелкие компании легче атаковать, чем крупные. Согласно исследованию Trustwave 90% взломов данных поражают малые предприятия, и эти предприятия гораздо труднее восстанавливаются от ущерба. В то время как небольшие компании могут и не обладать большими объемами персональных данных, они часто держат ключи доступа к тем, кто обладает.

Волновой эффект для репутации компании оценить трудно, но вполне реально. Если компания имеет сильную поддержку клиентов и тщательно обрабатывает ситуацию, клиенты могут быть начать колебаться, но не уйдут. Для небольших компаний, однако, любая потеря доверия клиентов является разрушительной.

В то время как вопрос доверия к правительству в результате взлома является большой проблемой, финансовый ущерб в этом случае ограничен по сравнению с общественным или частным бизнесом. В частном сегменте рынка тремя секторами, испытывающими наибольшие финансовые последствия после взлома, являются сектор финансовых услуг, здравоохранения и промышленный сектор. Так как многие люди имеют дурную привычку многократно использовать одни и те же пароли, потеря пароля для одного сайта часто имеет волновой эффект. Злоумышленники используют один украденный пароль, чтобы получить доступ к другим сайтам и приложениям, используемым жертвой, что приводит к многочисленным взломам.

ФИНАСОВЫЙ СЕКТОР

Наше исследование показывает, что финансовые институты сталкиваются с гораздо более высоким уровнем попыток атак, чем любой другой сектор рынка. В докладе, опубликованном Websense Security Labs в 2015 году, отмечается, что финансовые институты испытывают на 300% больше кибератак, чем любой другой сектор[10]. Объем этих атак превышает аналогичные показатели во всех других отраслях в соотношении 3:1.

Финансовые компании представляют собой идеальные цели, потому что их данные имеют

Показатели безопасности для финансового сектора в 2015 году

Некоторые из наиболее значительных примеров давления на финансовый рынок в 2015 году:

83% руководителей компаний финансовых услуг соглашаются, что возможность борьбы с киберугрозами и защиты персональных данных является одной из самых больших проблем в создании репутации в течение следующих 12 месяцев[3];

24% -е увеличение финансовых потерь от инцидентов[4];

73% американских потребителей сменили своих поставщиков финансовых услуг из-за взлома или кражи персональных данных[5];

61% потребителей не доверяют финансовым институтам[6];

44% финансовых компаний сообщили о потерях бизнеса в размере 20% или более в течение последних двенадцати месяцев из-за проблем с репутацией и удовлетворенности клиентов; в среднем потери составили 17%, почти вдвое превысив средний показатель 2014 года[7];

42% потребителей в США считают, что неспособность защитить персональную и финансовую информацию является самой большой угрозой для репутации своих финансовых организаций[8];

68% потребителей сообщают, что негативные новости о своих текущих финансовых организациях – вопросы, связанные с регулированием, незаконной деятельностью, штрафами и т.д., скорее всего приведут их к смене поставщика финансовых услуг[9].

широчайший оборот на открытом рынке. Розничные и коммерческие банки со своими филиалами, разбросанными по всему миру, компании по обработке кредитных карт, страховые и торговые компании – все они имеют такие данные, а также имеют связь с еще большим объемом данных у других компаний. Финансовые услуги не стоят первыми в списке целей для атак в 2015 году только потому, что усилия 2014 года по укреплению своей защиты сделали их более трудными для проникновения целями.

Финансовая кибербезопасность является глубоко сложной и многогранной экосистемой. Крупные финансовые институты стали более умными после 2014 года. Они начали инвестировать в интегрированные решения, а не в точечные продукты. Это дополнительно повысило защиту от наплыва сложных постоянных угроз и атак «нулевого дня».

Объем атак и точки их приложения требуют полного обзора для операций и централизованного управление безопасностью, но не полной прозрачности. Как и в случае государств, защищающих своих граждан, сотрудники службы безопасности в крупных финансовых учреждениях осторожны при обсуждении методов защиты или деталей атаки. Когда киберпреступники могут видеть, где атаки имеют успех, а где нет, они начинают соответственно приспосабливать свою тактику или ответные действия.

Восприятие защиты столь же, если не более, важно, чем фактическая защита. Инциденты, в которых не были потеряны никакие учетные записи или персональные данные, также могут подрывать доверие клиентов. Поэтому финансовые учреждения в настоящее время обмениваются информацией об атаках через общие каналы получения аналитической информации об угрозах. Наши партнерские программы по аналитической информации об угрозах предоставляют некоторые из таких каналов. Так как большинство хакеров используют те же самые успешные методы атак против нескольких жертв, данный подход может увеличить их расходы в случае, если метод взлома сработает только один раз. А чем дороже хакерство, тем меньше количество хакеров, что в свою очередь безопаснее для всех.

ЗДРАВООХРАНЕНИЕ

Записи о здоровье пациентов имеют самую высокую ценность на черном рынке: в десять раз больше, чем кредитные карты или другие финансовые данные[11]. В то время как номер кредитной карты или аутентификационные данные для банковской системы могут быть быстро переизданы, медицинские записи здравоохранения не могут. Они также открывают гораздо больше информации о человеке, в том числе чувствительные области, уязвимости и личные проблемы, что делает их ценным материалом для шпионажа. Медицинские компании являются главными целями киберпреступников.

9% ОРГАНИЗАЦИЙ ЗДРАВООХРАНЕНИЯ/ СТРАХОВАНИЯ СТАЛКИВАЛИСЬ С ПОТЕРЕЙ ДАННЫХ HIPAA

5.4 Источник: Check Point Software Technologies

В 2015 году и в начале 2016 года большое число организаций здравоохранения стали жертвами множества атак, в первую очередь «вымогательского» ПО. Традиционно отрасль здравоохранения отстает от главных целей хакеров, таких как финансовые организации с точки зрения надежности безопасности, но новые правила, касающиеся соблюдения требований защиты персональных данных, еще в большей степени осложнили ее модернизацию.

Показатели безопасности для здравоохранения в 2015 году

60%-й рост числа инцидентов безопасности в сегменте здравоохранения[12];

2% организаций здравоохранения в США сообщили по меньшей мере об одном случае кражи медицинских идентификационных данных[13];

282%-й скачок расходов на нарушения безопасности в отрасли здравоохранения по сравнению с предыдущими 12 месяцами[14];

89% медицинских учреждений США дают доступ к данным пациентов самим пациентам, их представителям и/или другим назначенных лицам[15];

11 типов – это среднее количество инструментов технической безопасности, которыми обладают организации здравоохранения в США[16];

21% организаций здравоохранения в США не используют технологию восстановления после сбоев (DR, Disaster Recovery), и 51.7% из них намерены приобрести такие средства в будущем[17];

54% организаций здравоохранения в США не имеют внедренной системы единого входа (SSO, Single Sign-On), и 49.3% из них намерены приобрести такую систему в будущем[18];

60% организаций здравоохранения в США не имеют внедренной двухфакторной аутентификации[19];

19% организаций здравоохранения в США сообщают о наличии взлома безопасности за последний год[20];

Только в 54% медицинских учреждений США специалисты IT и ИБ проверяли свои планы реагирования при взломе данных[21];

В сфере здравоохранения США первыми тремя мотивами предполагаемых угроз являлись:
(80%) работники, шпионящие за родственниками/друзьями,
(66%) кражи финансовых идентификационных данных,
(51%) кражи идентичности[22].

Такие программы, как HIPAA, устанавливают строгие правила в отношении преднамеренного или случайного открытия персональных данных, но такие меры могут обнаружить новые уязвимости в этом процессе. Медицинские учреждения любого масштаба должны соответствовать этим правилам относительно личной информации и ее безопасности. Средства защиты персональных данных иногда получают приоритет над контролем доступа. Интеграция устройств «Интернета вещей» (IoT) в среду здравоохранения значительно увеличивает область атак в этой отрасли, и эта область не масштабируется в соответствии с размером провайдера, что делает мелких операторов первыми целями. Также существенно усложняет защиту в области здравоохранения то, что при обновлении ОС системы, поддерживающие жизнедеятельность пациентов, не могут быть переведены в офлайн.

Соответствие регулирующим требованиям в области здравоохранения является доминирующей темой, но в первую очередь внимание здесь сосредоточено на механизмах внутреннего контроля, а не защиты информации. В то время как соответствие требованиям для врачей, медсестер и администраторов, имеющих доступ к данным, но обладающих ограниченным знанием методов киберпреступности, безусловно, является важной задачей, фокус должен быть смещен на IoT и защитные механизмы контроля доступа.

ПРОМЫШЛЕННЫЙ IoT

Промышленный Интернет Вещей (IIoT, Industrial Internet of Things) продолжал показывать значительный рост в 2015 году, что имело важные последствия для мировой экономики. В соответствии с Oxford Economics[23] этот сегмент включает в себя отрасли, которые создают 62% валового внутреннего продукта (ВВП) среди стран G20, в их числе предприятия коммунальных услуг, нефти и газа, сельского хозяйства и производства. Кроме того, сюда относятся и организации, обеспечивающие транспортировку, логистику и медицинские услуги для больниц, электростанции, а также железнодорожные и морские порты доставки.

Одной из самых больших привлекательных сторон IIoT является возможность повышения операционной эффективности. Дополнительные методы автоматизации и увеличения гибкости производства приводят к росту производительности на целых 30%[24]. Однако все эти устройства подключены к сети, как правило доступны и работают без присмотра, практически без защиты конечных станций.

Волновые эффекты от взломов IIoT трудно измеримы, но сосредоточены в основном вокруг нарушений нормальной работы. Критические сбои инфраструктуры имеют огромные последствия: одно выключение энергетической сети может повлиять на сотни или даже тысячи предприятий и, таким образом, не может быть легко выражено в количественных оценках.

Из всех нынешних достижений в области технологии IIoT имеет потенциал, чтобы создать наибольший положительный эффект и в тоже время быть причиной наибольшего ущерба. Например, производство автономных автомобилей компаниями Google и Tesla может, вероятно, повлиять на работу множества отраслей экономики, в том числе производство автомобилей, страхование автомобилей и лицензирование со стороны правительства и, возможно, обновление «по воздуху» программного обеспечения для определенных транспортных средств. HealthKit компании Apple является еще одним многообещающим примером IIoT. Если датчики здоровья и медицинские приложения внезапно станут локально доступны для пациентов, экосистема данных здравоохранения, которую в настоящее время формируют врачи, страховые организации и фармацевтические компании, будет смещаться в сторону частных лиц[25].

88% ОРГАНИЗАЦИЙ СТОЛКНУЛИСЬ С ИНЦИДЕНТОМ ПОТЕРИ ДАННЫХ

Главные способы обеспечения безопасности промышленного интернета вещей

Предотвращение. Если защита от вредоносного ПО не может быть реализована на каждом устройстве, она может находиться в точке, где IoT устройства обмениваются данными.

Сегментация. IoT устройства должны обмениваться данными с центральным контроллером, а не друг с другом.

Протоколы. Используйте средства безопасности, которые поддерживают специальные протоколы ICS/SCADA.

Управляющие команды. Системы IoT должны посылать информацию наружу. Однако, они же должны получать некоторые команды извне.

Преимущества, связанные с повышением эффективности, будут быстро омрачены их потерей в случае взлома.

ПОДСЧИТЫВАЯ УЩЕРБ ОТ ВОЛНЫ

Взлом данных может иметь краткосрочные финансовые последствия, но они бледнеют в сравнении с потенциально долгосрочным ущербом, нанесенным позиции организации на рынке. Как прямой результат взлома безопасности стоимость бренда в среднем может снизиться на 21%[26]. Восстановление вашей репутации может занять много времени и зависит от того, как проходит ваше аварийное восстановление после взлома.

Применяйте целостный подход к безопасности вместо комбинирования точечных решений. Делайте упор на предотвращении угроз как альтернативе их обнаружению и противодействию.

Для дальнейшего снижения риска включите решение по предотвращению потерь данных (DLP) в вашу систему защиты и используйте лучшие практики при конфигурировании безопасности.

> ***«Успех заключается не в том, чтобы никогда не делать ошибок, а в том, чтобы их не повторять».***
>
> Г. У. Шоу (Джош Биллингс), американский сатирик

Команда реагирования на инциденты Check Point доступна для расследования и решения сложных событий безопасности, охватывающих действия вредоносного ПО, вторжения или атаки «отказ в обслуживании».
Команда доступна в режиме 24x7x365 для связи по электронной почте emergency-response@checkpoint.com или по телефону 866.923.0907.

КОГДА ВЫ РАЗМЫШЛЯЕТЕ О ЦЕЛЯХ ВАШЕЙ КИБЕРБЕЗОПАСНОСТИ, ЗАДАЙТЕ СЕБЕ ЭТИ ВОПРОСЫ

1 ПОНИМАТЬ СИТУАЦИЮ

Насколько вы уверены в том, что ваша система кибербезопасности эффективна против угроз «нулевого дня»?

Насколько мои сотрудники осведомлены о киберугрозах и потенциальных последствиях своих действий?

2 ВИДЕТЬ ЧТО БУДЕТ

Есть ли у вас четкая видимость активности в журналах по всем сегментам вашей сети, или мониторинг является слишком сложной задачей, чтобы быть полезным ?

3 ЗАЩИЩАТЬ ЗАДАНИЯ, А НЕ СЕРВЕРА

Получают ли рабочие задания, которые я запустил в виртуальных, облачных и программно-определяемых средах, такую же защиту, как задания, исполняемые в моем ЦОД?

4 БЫТЬ ГОТОВЫМИ

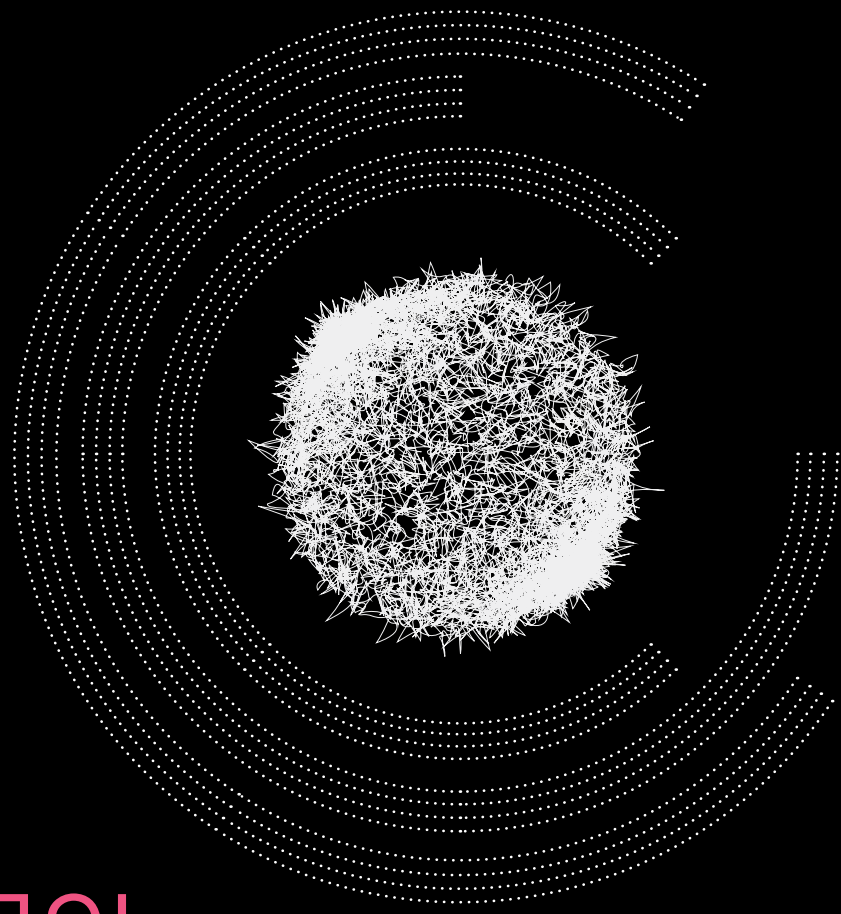
Защищают ли политики компании информацию и ресурсы во всех средах?

Насколько высшее руководство информировано о текущем уровне угроз и потенциальном ущербе бизнесу от кибератак на нашу компанию?

НАЧНИТЕ

Откройте для себя активные угрозы, которые в настоящее время действуют в вашей сети и слабые места в вашей защите, которые вы можете укрепить. Посетите страницу: checkpoint.com/resources/securitycheckup

6



НАХОДЯСЬ НА ШАГ ВПЕРЕДИ

«Предупрежден, значит вооружен; быть готовым – это половина победы».

Мигель де Сервантес,
писатель

Мобильность

3 — Среднее количество мобильных устройств, используемых на человека в США/Соединенном Королевстве[1].

Сотрудники смешивают бизнес и личное пользование. 1 из 5 мобильных устройств является зараженным[2].

IoT

Каждый день подключаются 5.5 миллиона новых вещей[3].

Облака

Расходы на корпоративные приложения в мировом масштабе выросли за 2015 год на 7.5% и составили 149.9 миллиардов долларов США[4].

Для того чтобы иметь эффективную стратегию безопасности, вы должны научиться понимать атакующих и провести инвентаризацию всего, что вы хотите защищать. Отчет этого года показывает, что сложность ландшафта угроз продолжает возрастать. Это связано с тем, что получить и развернуть вредоносное ПО стало проще чем когда-либо. В 2005 году был запущен один миллион новых образцов вредоносных программ. В 2015 году такое же количество могло быть запущено за один день[5]. Вредоносное ПО продолжает быть доступным и легким в использовании. Чтобы создать стратегию безопасности с учетом потребностей вашей организации внимательно изучите успешные атаки, последние уязвимости и тенденции атак.

Далее, оцените широту поверхности атаки в вашей организации. Границы предприятия продолжают растягиваться и размываться, еще более усложняя защиту. Серверы и корпоративные компьютеры больше не определяют эту границу. Вместо этого она была отодвинута рекордным количеством мобильных устройств, облачных приложений, а также растущим числом устройств Интернета Вещей (IoT), о подключении которых ваш департамент IT даже не подозревает. Эти инструменты повышают производительность, но каждое расширение границы предприятия должны быть защищено.

Мобильные устройства, IoT и облачные приложения предоставляют больше свободы, но эта свобода приносит абсолютно новые угрозы безопасности. На каждое прерывание бизнес-модели департамент IT ломает голову, думая о том, как защитить бизнес. Например, беспроводные соединения мобильных устройств, используемых для сканирования при инвентаризации на складе, не должны быть поставлены под угрозу или перехвачены. Устройства IoT, которые автоматизируют сбор медицинских данных, распределение мощности электротока высокого напряжения или воздушный поток в высотном офисном здании, должны быть надлежащим образом защищены от прерывания их работы с помощью удаленной команды. Приложения на основе облачных технологий не должны иметь непроверенных открытых интерфейсов, которые по незнанию предоставляют хакерам доступ в вашу сеть.

Управляя защитой для IoT как отдельной системой, вы усложните управление безопасностью. В идеале защита для IoT, будь то для потребительских товаров или промышленных систем SCADA, может быть реализована в рамках единой архитектуры безопасности и управляться с помощью той же консоли, что и другие сегменты сети.

Соответствие требованиям: лучший повод для лучших практик

Очень часто люди, которые пишут правила кибербезопасности, обнаруживают признаки группового поведения. Доказательством этого являются многочисленные общие требования регуляторов, записанные в правила кибербезопасности, которые создаются в организациях промышленного и государственного секторов. Когда вы сталкиваетесь со сложной сетью правил и законов, применение передового опыта может помочь вам использовать общие требования для упрощения и улучшения соблюдения регулирующих правил и совершенствования защиты.

Под лучшими практиками мы понимаем рекомендации по оптимизации настроек решений в области кибербезопасности. Основной причиной использования передового опыта является стремление исключить человеческие ошибки. Согласно Gartner «Вплоть до 2020 года 99% взломов МСЭ будет вызвано просто неправильной конфигурацией МСЭ, а не их недостатками»[6]. Описывая управление IT, Льюис Морган утверждает: «Человеческая ошибка является причиной большинства утечек данных. Ни для кого не секрет, что самой большой угрозой для данных организации являются ее собственные сотрудники – намеренно или нет»[7].

Учитывая то, что ошибки конфигурации могут иметь серьезное влияние на безопасность и соответствие требованиям, исследователи Check Point заинтересовались изучением того, насколько эффективно организации используют лучшие практики, а также их влиянием на соответствие требованиям. Чтобы выяснить это, наши исследователи мониторили конфигурации таких механизмов безопасности, как межсетевые экраны, системы обнаружения/предотвращения вторжений (IDS/IPS), антивирусы и других, и собрали метрики соответствия требованиям.

Наши исследователи были поражены тем, что только 53.3% параметров конфигурации были определены в соответствии с передовыми отраслевыми практиками. Уровни соответствия для различных отраслей промышленности и регулирующих стандартов приведены в следующей таблице:

Уровни соответствия 4 регулирующим стандартам по отраслям

ОТРАСЛЬ	РЕГУЛИРУЮЩЕЕ ПОЛОЖЕНИЕ	ОБЩИЙ СТАТУС СООТВЕТСТВИЯ
Здравоохранение	HIPAA Security	59%
Общая IT-безопасность	ISO 27001	64%
Большие энергосистемы	NERC CIP	67%
Платежные карты	PCI DSS 3.1	60%

Картина, которая возникла в ходе нашего исследования, показывает, что сегмент

IT-специалистов по широкому спектру отраслей не оптимизирует свои конфигурации безопасности для обеспечения защиты и соответствия требованиям. Чтобы понять это более подробно, в таблице 2 ниже показано соответствие наилучшим практикам с разбивкой по компаниям критически важной инфраструктуры и финансовым организациям.

Уровни соответствия по стандартам конфигураций по отраслям

ЛУЧШАЯ ПРАКТИКА	ВСЕ ОТРАСЛИ	КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА	ФИНАНСОВЫЕ ОРГАНИЗАЦИИ
Включить анти-спуфинг	70.0%	75.5%	65.0%
Убедиться, что правила МСЭ должным образом документированы	28.0%	30.0%	30.0%
Определить опции слежения для правил политики	20.0%	22.0%	30.0%
Блокировать приложения и вебсайты высокого риска	49.5%	54.0%	45.0%

Интересно отметить, что 3 из 10 предприятий не пользуются технологией антиспуфинга и одна из двух компаний не ограничивает доступ к приложениям с высокой степенью риска. Принимая во внимание риски, связанные с этими технологиями безопасности, эта статистика имеет эффект бомбы. Другим значимым результатом является то, что три из четырех политик МСЭ, которые были проанализированы, не были полностью документированы в базе правил.

Лучшие практики и отчетность

Лучшие практики также могут помочь вам с отчетностью и непрерывными аспектами мониторинга соблюдения требований в случае, если вы должны предстать перед «инквизицией аудиторов». Правило 11 PCI-DSS[8], HIPAA CFR 160-164[9], FISMA[10], FERPA 99.62[11], FINRA Правило 4530 и многие другие правила требуют мониторинга безопасности и отчетности по процедурам безопасности. После того как вы продвинулись вперед в деле конфигурации, ссылки на лучшие практики в отчетах являются эффективным способом для структурирования материалов для аудитов.

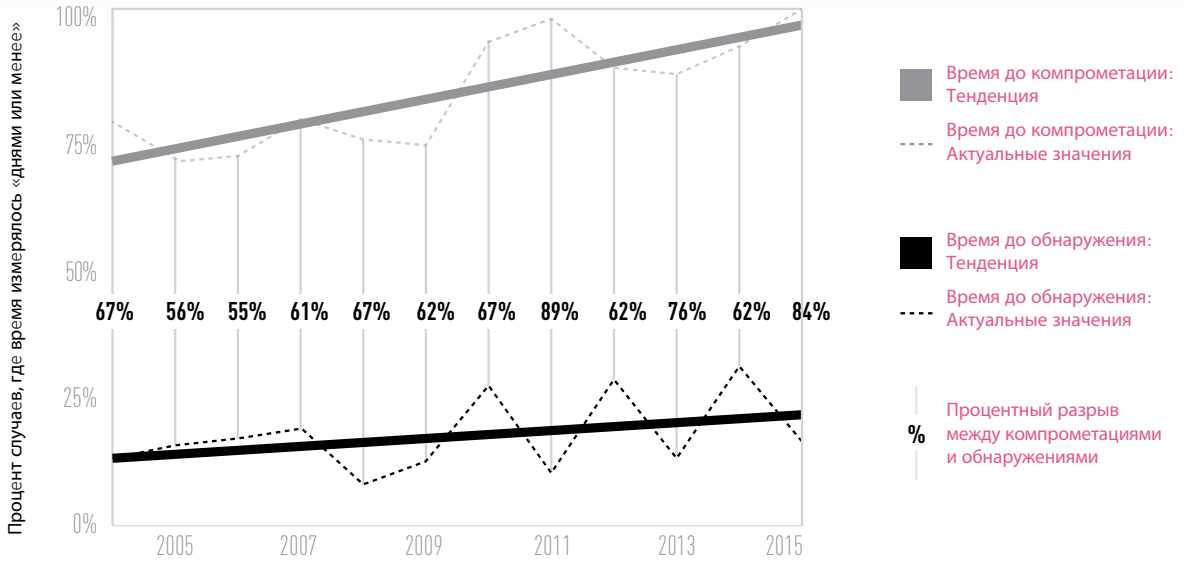
МНОГО ПОЖАРОВ, НО ОЧЕНЬ МАЛО ПОЖАРНЫХ

С таким большим числом вредоносных программ, с таким множеством векторов атак и таким количеством устройств, которые надо защищать, ни одна организация не может быть застрахована – ни маленькая, ни большая, ни коммерческая, ни промышленная, ни правительственная. Все мы рискуем. По мере того как угрозы и атаки возрастают, то же происходит и с количеством устройств безопасности и инструментов, которыми ваш департамент IT должен управлять. Даже если бюджеты IT были бы неограниченными, существует лишь ограниченное число подготовленного персонала IT.

Специалистов IT-безопасности не бывает достаточно для поддержки растущего спроса на управление и мониторинг систем IT. Те, кто есть в наличии, должны жонглировать комбинацией обычных запросов, смешанных со срочными оповещениями. Кроме того, они увязли в ручных процессах и разрозненных системах. И в этой ситуации ключом к успеху являются расширенные средства предотвращения угроз во всех точках, а также централизованное управление и методичное исполнение.

Традиционных подходов к безопасности уже не достаточно. Для того чтобы идти в ногу с постоянно расширяющимся периметром сети команды IT должны коренным образом изменить свой подход к безопасности. Традиционно представляемая как ряд индивидуально управляемых и индивидуально мониторируемых компонентов, безопасность теперь должна стать единой, лучшей в своем классе системой. Современная архитектура безопасности должна сочетать в себе управле-

ОКНО ОТКРЫТОСТИ ОТ КОМПРОМЕТАЦИИ ДО ОБНАРУЖЕНИЯ



6.1 Источник: 2016 Data Breach Investigations Report, Verizon, page 10

ние безопасностью для мобильных устройств, IoT и облачных систем в рамках одной архитектуры управления, обладающей гибкостью для поддержки нескольких распределенных сред облачных вычислений. Сегодня безопасность должна быть быстрой, открытой, интегрированной и самое главное – управляемой с одной консоли.

Чтобы попасть внутрь вашей сети, квалифицированному атакующему, имеющему точку входа, потребуется все несколько минут. Злоумышленники оказываются более эффективными при входе и выходе с данными, поэтому крайне важно сосредоточиться на предотвращении атак, а не только их обнаружении. Последние данные отчета по расследованию взломов за 2016 год компании Verizon показывают, что каждая минута на счету и каждый год атакующие компрометируют сети быстрее, чем их действия могут обнаружить.

БУДЬТЕ ОРГАНИЗОВАННЫ В ВАШИХ ДЕЙСТВИЯХ

Как было показано Главах 2 и 4, число неизвестных вредоносных программ увеличивается. Тем не менее большинство атак в 2015 году происходили с использованием известных вредоносных программ, которым уже больше года. Многих из этих атак можно было бы избежать. Для того чтобы идти в ногу с последними «заплатками» для ПО и быть уверенными, что все эти «заплатки» распространены на все устройства и компьютеры в сети, требуется организация и хорошая автоматизация. Быть организованными и методичными. Усильте строгую политику применения «заплаток» с помощью решений для предотвращения известных атак. Они должны включать традиционный антивирус, системы предотвращения вторжений и межсетевой экран нового поколения, каждый из которых постоянно обновляется, используя самую последнюю аналитическую информацию об угрозах.

Как видно из Главы 3, мобильные устройства размывают границы между личным и деловым их использованием. Одно устройство, содержащее необнаруженные вредоносные программы, ставит под угрозу всю сеть. Таким образом, жизненно важно создание безопасной, защищенной бизнес-среды на любом мобильном устройстве.

Глава 4 предоставила обзор постоянного роста неизвестных вредоносных программ – как реальных уязвимостей «нулевого дня», так и перепакованных вариантов уже существующего вредоносного ПО. Эти атаки гораздо труднее обнаружить. Кроме того, многие хакеры учатся обходить первое поколение «песочниц», которые были установлены в последние годы. К счастью, более современные решения сэндбоксинга обнаруживают атаки, прежде чем может быть развернут код уклонения.

Перспективная безопасность начинается с наличия лучшего в своем классе набора основных инструментов защиты. Усовершенствованная система предотвращения угроз, защита мобильных устройств и сегментация вашей сети таким образом, чтобы она могла находиться под пристальным контролем, имеют решающее значение для полной защиты вашей организации. Для максимизации производительности вашей команды IT всегда тщательно изучайте ваши затраты и поддерживайте высокую исполнительскую эффективность.

> ***«Лучший способ предсказать будущее – это изобрести его».***
>
> Алан Кэй, ученый в области теории вычислительных систем

Занимаетесь ли вы этим самостоятельно или командуете группой подчиненных, задачи по вкручиванию серверов в стойки или манипуляции кондиционированием серверной комнаты быстро становятся проблемами кого-то другого – того, кто работает в облачном вычислительном центре. По оценкам Cisco 83% трафика центров обработки данных (ЦОД) к 2019 году будет составлять облачный трафик[12]. Масштабные преобразования в облачных вычислениях знаменуют фундаментальный сдвиг от аппаратно-ориентированных инфраструктур, располагающихся в корпоративных центрах обработки данных, на программно-ориентированные инфраструктуры, работающие на динамических пулах вычислительных ресурсов и ресурсов хранения. Технологический переход на облачные вычисления предоставляет удобное время для пересмотра решений необходимых для защиты IT-ресурсов и сервисов вашей организации при их размещении на облачной платформе, а также того, что этот переход означает для вашей роли как специалиста IT.

Переосмысляя роли IT-безопасности

Облачные вычисления позволяют обеспечить расширяемые услуги дешевле и быстрее, так как облачные платформы, такие как Microsoft Azure, Amazon Web Services и Google Cloud Platform, как правило, более ресурсо-эффективные, чем их контрагенты из корпоративных ЦОД. Например, облачные вычислительные центры, как правило, имеют более высокие плотности гостевых виртуальных машин на хост-серверах, чем обычно можно наблюдать в виртуальных средах предприятия. Кроме того, мгновенная полоса пропускания облачных вычислений может обрабатывать всплески трафика, в то время как вычислительные ресурсы, предоставляемые по запросу, могут сделать услуги более надежными, масштабируемыми и экономически эффективными. Перекладывая заботу об аппаратных средствах и полосе пропускания на провайдеров услуг «Инфраструктура как сервис» (IaaS) и «Программное обеспечение как сервис» (SaaS), вы можете сосредоточиться на программных аспектах вашей деятельности: развертывании порталов приложений самообслуживания, архитектуре политик, внедрению лучших практик, а также мониторинге и отчетности по безопасности.

Переход к публичным и гибридным облачным сетям не означает, что услуги и меры безопасности, необходимые для их защиты, будут принципиально иными. В облаке вы по-прежнему нуждаетесь в широких возможностях по предотвращению угроз, а также безопасности электронной почты, веб-безопасности, безопасности приложений – всех тех мерах, которые вы в настоящее время используете для защиты сети, расположенной на территории вашей организации.

Несмотря на то, что безопасность должна быть непрерывной, переход в облако означает смену ролей. Вместо того, чтобы администраторы IT и безопасности ломали копья по вопросу зоны ответственности в управлении безопасностью и других инфраструктурных вопросах, эти решения будут принимать разработчики приложений. Администраторы и разработчики приложений должны изучить пути преодоления разрыва в знаниях, отделяющего администрирование IT, управление безопасностью и разработку приложений.

Для того чтобы взять верх, вам нужно начать согласовывать безопасность с рабочими процессами сервисных приложений и оркестровку процессов, что позволит вам защитить сервисы и данные, а также применять политики, независимо от того, где бы ни начинались ваши сервисы и где бы они ни завершались.

Сервер является сервером независимо от того, находится ли он в центре обработки данных или в облачном вычислительном центре. Тем не менее, когда серверы находятся в основном под чужой крышей, концентрация внимания на программных аспектах сетей и безопасности становится приоритетом, который вы должны начать применять прямо сейчас.

НАХОДИТЬСЯ НА ШАГ ВПЕРЕДИ В ВОПРОСАХ БЕЗОПАСНОСТИ

ДЕЙСТВУЙТЕ

Аксиома Бенджамина Франклина о том, что «унция профилактики стоит фунта лечения», особенно актуальна в эпоху неизвестного вредоносного ПО и уязвимостей «нулевого дня». В идеале скудные IT-ресурсы лучше вкладывать в предотвращение угроз, чем на погоню за предупреждениями и реагирование на инциденты безопасности.

ПРЕДОТВРАЩЕНИЕ

1 МНОГОСЛОЙНАЯ КИБЕРЗАЩИТА

Угрозы приходят в разных формах и объемах. Вот технологии для создания слоев вашего стека безопасности: система предотвращения угроз нового поколения, МСЭ, контроль приложений, антибот, антивирус, использование идентификационной информации, антиспам и система защиты электронной почты, системы предотвращения вторжений и фильтрации URL.

2 ПРЕДОТВРАЩАЙТЕ ВРЕДОНОСНОЕ ПО ПРИ ПЕРВОМ КОНТАКТЕ

Система предотвращения в реальном времени, которая прерывает работу вредоносного ПО при первом же контакте, является сегодня новым стандартом для эффективной защиты.

3 ВИРТУАЛЬНЫЕ «ЗАПЛАТКИ»

Виртуальные «заплатки» защищают от эксплоитов неопубликованных уязвимостей и покрывают временной разрыв до момента развертывания «заплаток» для известных уязвимостей.

АРХИТЕКТУРА

1 УПРОСТИТЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

Переключение между консолями для управления безопасностью для каждого сегмента сети является неэффективным, способствует возникновению ошибок конфигурации и несоответствий между слоями безопасности. Управление всеми функциями безопасности, сегментами и средами с помощью одной консоли помогает упростить процесс для достижения лучшей защиты, которой легко управлять.

2 УНИФИЦИРУЙТЕ УПРАВЛЕНИЕ

Внедряйте унифицированные элементы управления, которые распространяются на все сети, системы, конечные точки и среды, включая традиционные, облачные, виртуальные, мобильные, IoT и гибридные.

ПОЛУЧИТЕ ФАКТЫ

Изучите результаты независимого тестирования на коэффициент выявления вредоносного ПО, предотвращение угроз в режиме реального времени, масштабируемость управления и многое другое. Скачать документ «Факты против Слухов»: checkpoint.com/facts

ССЫЛКИ

Глава 2

1 Harrison, Virginia and Pagliery, Jose. "Nearly 1 million new malware threats released every day." CNN Money, April 14, 2015. http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

2 Chickowski, Ericka. "5 Exploit Trends Driving Attacks Today." Dark Reading, February 17, 2016. http://www.darkreading.com/perimeter/5-exploit-trends-driving-attacks-today/d/d-id/1324352

3 Cisco. "Cisco Global Cloud Index: Forecast and Methodology, 2014–2019 White Paper," April 21, 2016.

4 Weins, Kim. "Cloud Computing Trends: 2016 State of the Cloud Survey." RightScale, February 9, 2016. http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey

5 Malware Statistics. AV-TEST. https://www.av-test.org/en/statistics/malware/

6 Malware Statistics. AV-TEST. ibid.

Глава 3

1 comScore Whitepaper. "The U.S. Mobile App Report." August, 2014. http://www.comscore.com/Insights/Presentations-and-Whitepapers/2014/The-US-Mobile-App-Report

2 comScore Whitepaper. "The U.S. Mobile App Report." August, 2014. ibid.

3 comScore Whitepaper. "The U.S. Mobile App Report." August, 2014. ibid.

4 Information Security. "2016 BYOD & Mobile Security Spotlight Report." Scribd. https://www.scribd.com/doc/309703246/BYOD-and-Mobile-Security-Report-2016

Глава 4

1 Internet World Stats, "Internet Users in the World by Region 2015." http://www.internetworldstats.com/stats.htm

2 Internet World Stats, "Internet World Penetration Rates by Geographic Regions, November 2015 Update." http://www.internetworldstats.com/stats.htm

3 Kerner, Sean Michael. "Heartbleed Remains a Risk 2 Years After It Was Reported," eWeek, April 7, 2016. http://www.eweek.com/security/heartbleed-remains-a-risk-2-years-after-it-was-reported.html

4 US Cert Alert TA15-051A, "Lenovo Superfish Adware Vulnerable to HTTPS Spoofing." US-CERT, February 24, 2015. https://www.us-cert.gov/ncas/alerts/TA15-051A

Глава 5

1 Korolov, Maria. "Ponemon: Data Breach Costs Now Average $154 per Record." CSO, May 27, 2015. http://www.csoonline.com/article/2926727/data-protection/ponemon-data-breach-costs-now-average-154-per-record.html

2 Gemalto. "Gemalto releases findings of 2015 Breach Level Index," February 23, 2016. http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-2015-Breach-Level-Index.aspx

3 Makovsky. "Data Breaches and Failure to Protect Personal Info Further Damage Wall Street's Reputation and Business," May 28, 2015. http://www.makovsky.com/news/data-breaches-and-failure-to-protect-personal-info-further-damage-wall-streets-reputation-and-business-2/

4 PwC. "The Global State of Information Security Survey 2015 - Managing cyber risks in an interconnected world," 2015. http://www.pwccn.com/home/eng/rcs_info_security_2015.html

5 Makovsky Wall Street Reputation Study op. cit.

6 Makovsky Wall Street Reputation Study ibid.

7 Makovsky Wall Street Reputation Study ibid.

8 Global State Information Security Survey op. cit.

9 Makovsky Wall Street Reputation Study op. cit.

10 Raytheon Websense. "2015 Drill-Down Report – Financial Services," June, 2015.

11 Wagstaff, Jeremy. "Medical data, cybercriminals' holy grail, now espionage target," Reuters, June 2015. http://www.reuters.com/article/cybersecurity-usa-targets-idUSL3N0YR30R20150605

12 Global State of Information Security Survey op. cit.

13 6th Annual HIMSS Security Survey. http://www.himss.org/2013-himss-security-survey?ItemNumber=28270

14 6th Annual HIMSS Security Survey ibid.

15 6th Annual HIMSS Security Survey ibid.

16 6th Annual HIMSS Security Survey ibid.

17 6th Annual HIMSS Security Survey ibid.

18 6th Annual HIMSS Security Survey ibid.

19 6th Annual HIMSS Security Survey ibid.

20 6th Annual HIMSS Security Survey ibid.

21 6th Annual HIMSS Security Survey ibid.

22 6th Annual HIMSS Security Survey ibid.

23 Copyright Oxford Economics, Ltd. Global Industry Databank. http://www.oxfordeconomics.com/forecasts-and-models/industries/data-and-forecasts/global-industry-databank/overview

24 Heng, Stefan. "Industry 4.0: Huge potential for value creation waiting to be tapped," Deutsche Bank Research, May, 2014. http://www.dbresearch.com/servlet/reweb2.ReWEB?rwsite=DBR_INTERNET_EN-PROD&rwobj=ReDisplay.Start.class&document=PROD

25 Boulton, Clint. "Apple's New Health Focus Comes at Propitious Time," The Wall Street Journal, June 10, 2014. http://blogs.wsj.com/cio/2014/06/10/apples-new-health-focus-comes-at-propitious-time/

26 Experian. "Reputation Impact of a Data Breach." https://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf

Глава 6

1 Statista. "Average number of connected devices used per person in selected countries in 2014." http://www.statista.com/statistics/333861/connected-devices-per-person-in-selected-countries/

2 Information Security. "2016 BYOD & Mobile Security Spotlight Report." Scribd. https://www.scribd.com/doc/309703246/BYOD-and-Mobile-Security-Report-2016

3 Gartner. "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," November 10, 2015. http://www.gartner.com/newsroom/id/3165317

4 Gartner. "Gartner Says Modernization and Digital Transformation Projects Are Behind Growth in Enterprise Application Software Market," August 27, 2015. http://www.gartner.com/newsroom/id/3119717

5 AV-TEST. "Malware Statistics." https://www.av-test.org/en/statistics/malware/

6 Gartner. "One Brand of Firewall Is a Best Practice for Most Enterprises," February 18, 2016. https://www.gartner.com/doc/3215918?ref=SiteSearch&sthkw=One%20Brand%20of%20Firewall%20is%20a%20Best%20Practice%20for%20Most%20Enterprises&fnl=search&srcId=1-3478922254

7 Morgan, Lewis. "Five damanging data breaches caused by human error," IT Governance Blog, February 17, 2016. https://www.itgovernance.co.uk/blog/five-damaging-data-breaches-caused-by-human-error/

8 PCI Security Standards Council. "Maintaining Payment Security." https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

9 U.S. Department of Health & Human Services. "Summary of the HIPAA Security Rule." http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/

10 National Institute of Standards and Technology. "Federal Information Security Management Act (FISMA) Implementation Project." http://csrc.nist.gov/groups/SMA/fisma/

11 U.S. Department of Education. "Family Educational Rights and Privacy Act (FERPA)." http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

12 Cisco. "Cisco Global Cloud Index: Forecast and Methodology, 2014–2019 White Paper," page 5, April 21, 2016.

О компании Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) является крупнейшим мировым производителем в области сетевой кибербезопасности, поставляющий передовые решения и защищающий своих клиентов от кибератак, используя беспрецедентный коэффициент обнаружения вредоносного ПО и других типов угроз. Check Point предлагает всеобъемлющую архитектуру безопасности для защиты предприятий — от сетей до мобильных устройств — в дополнение к наиболее полной и интуитивной системе управления безопасностью. Check Point защищает свыше 100 000 организаций любых масштабов.