CHECK POINT
МИФЫ МОБИЛЬНОЙ БЕЗОПАСНОСТИ

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ - ЭТО БОЛЬШЕ, ЧЕМ ОБЕСПЕЧЕНИЕ ДОВЕРЕННЫХ ПРИЛОЖЕНИЙ И ПРАВИЛ УКЛОНЕНИЯ ОТ ВРЕДОНОСНОГО ПО

Мобильность изменила облик рабочего места. Ноутбуки, смартфоны и планшеты являются теперь не только рабочими инструментами часто путешествующих работников, но также дают возможность всем сотрудникам оставаться на связи, где бы они ни были – присутствуя на конференции, работая из дома или сидя в терминале аэропорта.

Когда дело доходит до обеспечения безопасности мобильных устройств, наиболее популярными вариантами являются решения по управлению мобильными устройствами (MDM – Mobile Device Management) и менеджменту мобильности на предприятии (EMM – Enterprise Mobility Management). Однако не совсем ясно, могут ли эти решения обеспечить защиту в реальных ситуациях. Например, что произойдет, если устройство, содержащее как рабочую, так и личную информацию утеряно, и существует необходимость стереть на нем данные? Обеспечивают ли эти решения защиту от вредоносного ПО? Насколько хорошо защищены корпоративные документы?

Мы решили развенчать миф о том, как хорошо существующие решения защищают реальные данные в реальных ситуациях. Мы попросили наших внутренних экспертов создать несколько типовых сценариев и произвести оценку механизмов обеспечения безопасности различных производителей. Сценарии охватывали различные вопросы – от «что делать с потерянными устройствами», до «что делать с вредоносным ПО» и «как защитить документы».

РЕЗУЛЬТАТЫ РАЗВЕНЧАНИЯ МИФА МОБИЛЬНОЙ БЕЗОПАСНОСТИ

Мы рассмотрели четыре базовых сценария, с которыми регулярно сталкиваются пользователи, и в рамках которых тестировали возможность каждого решения по:

1. Поддержке потерянных устройств – удаленном стирании корпоративных данных, но не личных данных сотрудника;
2. Действиям до заражения – защите мобильного устройства от заражения вредоносным ПО;
3. Действиям после заражения – мерам, принимаемым по отношению к вредоносному ПО, найденному на мобильном устройстве;
4. Защите документов и контента – защите документов и предотвращению намеренных и ненамеренных утечек данных.

MDM И EMM
НЕ ОБНАРУЖИВАЮТ
ВРЕДОНОСНОЕ ПО
И НЕ ЗАЩИЩАЮТ ОТ УГРОЗ
ПРИ ИСПОЛЬЗОВАНИИ
НЕЛЕГИТИМНЫХ
ПРИЛОЖЕНИЙ

РЕШЕНИЯ MDM И EMM
ТАКЖЕ НИЧЕГО
НЕ ДЕЛАЮТ ДЛЯ ТОГО,
ЧТОБЫ ОСТАНОВИТЬ
ШПИОНСКОЕ ПО,
ЕСЛИ ОНО ПОПАЛО
НА УСТРОЙСТВО

Результаты тестов приведены ниже, в Таблице 1.

	Check Point Capsule	Good For Enterprise	MobileIron Mobile@work	AirWatch Workspace	Citrix XenMobile
Стирание рабочих данных на устройстве	ПРОЙДЕН	ПРОЙДЕН	НЕ ПРОЙДЕН	ПРОЙДЕН	ПРОЙДЕН
Действия до заражения	ПРОЙДЕН	НЕ ПРОЙДЕН	НЕ ПРОЙДЕН	НЕ ПРОЙДЕН	НЕ ПРОЙДЕН
Действия после заражения	ПРОЙДЕН	НЕ ПРОЙДЕН	НЕ ПРОЙДЕН	НЕ ПРОЙДЕН	НЕ ПРОЙДЕН
Защита документа	ПРОЙДЕН	ПРОЙДЕН	ПРОЙДЕН	ПРОЙДЕН	ПРОЙДЕН
Защита контента	ПРОЙДЕН	НЕ ПРОЙДЕН	НЕ ПРОЙДЕН	НЕ ПРОЙДЕН	НЕ ПРОЙДЕН

Таблица 1.

Когда необходимо избежать очевидного враждебного поведения, решения большинства производителей справляются достаточно хорошо. Множество решений по обеспечению мобильной безопасности пытаются решить проблему возможного заражения мобильного устройства путем его блокировки, исходя из предположения, что они смогут с этим справиться в 100% случаев. Но что произойдет, если они пропустят хотя бы один вредоносный файл? Что они будут делать в случае заражения мобильного устройства? Какие действия они предпримут для защиты сети организации в целом? Далее в документе мы опишем детали наших испытаний, настройки тестов и наблюдения за производительностью решений каждого производителя.

MDM И EMM: ИСТОРИЯ ВОПРОСА

MDM и EMM традиционно являлись способами обеспечения мобильной безопасности. Однако, безопасность никогда не была главной целью при создании этих решений. MDM представлял собой раннюю попытку обеспечить мобильную безопасность, которую давал компаниям функционал блокировки доступа к определенным функциям мобильного устройства, предотвращая таким образом возможность совершения пользователем определенных действий. Хотя с точки зрения IT безопасности это было резонным, такой подход не был популярным у пользователей, так как он ограничивал их свободу. Еще менее привлекательными выглядели ограничение свобод пользователей и угроза стирания данных на их собственных устройствах в концепции BYOD (Bring Your Own Device).

Более новые решения EMM предоставляют гораздо большую свободу сотрудникам за счет использования «допущенных» приложений. Решения EMM обеспечивают безопасность индивидуальных приложений путем ограничения их возможностей через использование слоя безопасности, который встраивается либо на уровне исходного кода приложения, либо с помощью внешней оболочки безопасности. Допущенные приложения могут распространяться, мониториться и управляться с помощью централизованной станции мониторинга EMM. Как MDM, так и EMM обеспечивают безопасность сетей в основном за счет уклонения от вредоносного ПО, обеспечивая защиту только корпоративных данных и приложений, оставляя незащищенными личные данные и приложения. MDM и EMM не обнаруживают вредоносное ПО и не защищают от угроз при использовании «недопущенных» приложений. Также решения MDM и EMM не могут остановить шпионское ПО, если оно уже попало на устройство.

МИФЫ МОБИЛЬНОЙ БЕЗОПАСНОСТИ

Когда мы рассматриваем расширение периметра сети организации при включении в нее мобильных устройств, то ее защита требует учета нескольких факторов. Для любого мобильного устройства, будь то ноутбук, планшет или смартфон, существуют различные пути обеспечения защиты самого устройства, сетевых соединений и контента как на устройстве, так и в корпоративной сети.

Большинство организаций защищает соединение с помощью виртуальных частных сетей, VPN (Virtual Private Network). Соединение VPN создает защищенный доверенный канал между удаленным устройством и организацией. Это не обеспечивает безопасность самого устройства или его содержимого, но защищает транспорт от устройства до корпоративной сети. Некоторые опции VPN поддерживают концепцию разделенного туннелирования, при котором только корпоративный трафик идет в сеть организации. Доступ в Интернет с удаленного устройства, например, в этом случает реализуется напрямую. Хотя это экономит полосу пропускания, такое новое соединение более не является зашифрованным или безопасным.

ЗАЩИТА ДОКУМЕНТА ЧАСТО ЯВЛЯЕТСЯ НЕДООЦЕНЕННЫМ АСПЕКТОМ МОБИЛЬНОЙ БЕЗОПАСНОСТИ

МИФ №1 – РЕШЕНИЕ MDM БЕЗОПАСНО

Решение по управлению мобильными устройствами MDM (Mobile Device Management) представляет собой систему, которая позволяет отделу IT администрировать мобильные устройства и контролировать действия пользователей. Используя MDM, IT может определить разрешенные для пользователя операции. При этом существуют два главных недостатка MDM. С точки зрения пользователя, политики MDM могут быть слишком строгими, в зависимости от отдела IT. А когда пользователи чувствуют себя ущемленным, они склонны искать пути обхода систем безопасности. С точки зрения организации, MDM не обеспечивает реальной защиты устройств, так как решения MDM не включают в себя механизмы защиты от вредоносного ПО. И хотя решения MDM могут контролировать настройки и приложения, они не могут контролировать входящий и исходящий потоки данных. Также решения MDM могут быть дорогими в эксплуатации, так как мобильные устройства требуют постоянного мониторинга на предмет недопустимого поведения.

МИФ №2 – МОБИЛЬНЫЕ КОНТЕЙНЕРЫ ПРЕДОХРАНЯЮТ МОБИЛЬНЫЕ УСТРОЙСТВА ОТ ВРЕДОНОСНОГО ПО

МОБИЛЬНОСТЬ ПОЗВОЛЯЕТ ЛЮДЯМ РАБОТАТЬ «НА ХОДУ», А СПЕШАЩИЕ ЛЮДИ ИМЕЮТ ТЕНДЕНЦИЮ СОВЕРШАТЬ БОЛЬШЕ ОШИБОК

Мобильные контейнеры являются более гибким решением, позволяющим пользователям получать доступ к корпоративным данным на своих устройствах, отдельно от их собственных личных данных. Контейнер представляет собой защищенную область на устройстве с независимым контролем доступа. Такое безопасное зашифрованное рабочее пространство защищает корпоративные данные путем отделения их от других данных и приложений на устройстве. В то время как контейнеры защищают корпоративные данные на мобильном устройстве, личные данные и приложения часто остаются незащищенными. Запуск контейнера на скомпрометированном устройстве приведет к компрометации данных при их использовании.

МИФ №3 – НА МОБИЛЬНЫХ УСТРОЙСТВАХ ДОКУМЕНТЫ ЗАЩИЩЕНЫ ПРИ ИХ ПРИЕМЕ/ОТПРАВКЕ

Защиту документов зачастую игнорируют, При рассмотрении вопросов мобильной безопасности зачастую игнорируется проблема защиты документа. Мобильность позволяет людям работать «на ходу», а спешащие люди имеют тенденцию совершать больше ошибок, будь то потеря устройства, или отсылка документа не тому получателю. Контроль доступа к документу

находящемуся на устройстве является одним из вариантов организации защиты. Другим вариантом может быть парольная защита самого документа, хотя, к сожалению, как только документ открыт, он может быть распечатан, скопирован или к нему может быть организован разделяемый доступ. Лучшим вариантом могло бы быть ограничение доступа только определенным набором получателей, определение действий, которые они могут совершать с документом, и возможность отзыва прав доступа в любое время.

Полнценное решение мобильной безопасности должно обеспечивать безопасность соединения, устройства, корпоративных данных на устройстве, личных данных и не относящихся к бизнесу приложений, и, конечно, предоставлять наивысший уровень защиты документов. Такая планка производительности была задана нашей командой для сценариев испытаний.

ПРОИЗВОДИТЕЛИ РЕШЕНИЙ МОБИЛЬНОЙ БЕЗОПАСНОСТИ – СПИСОК УЧАСТНИКОВ

Мы сравнивали решение Check Point Capsule с решениями четырех лидеров рынка систем менеджмента мобильности предприятий EMM, в которых сделан наиболее сильный упор на безопасность мобильных устройств. Конфигурации этих решений приведены в Таблице 2.

ПРОИЗВОДИТЕЛЬ	ВЕРСИЯ СЕРВЕРА	ВЕРСИЯ КЛИЕНТА
Check Point	Check Point R77.20	Capsule Workspace (1.643.34) Capsule Connect (2.38)
Good Technology	Good Mobile Messaging (8.3.0.12)	Good for Enterprise (2.8.1.402)
MobileIron	Core 7.5 (Cloud)	Mobile@Work (7.5.0.2)
AirWatch	AirWatch MDM Cloud (7.3.6.0)	Workspace (1.5.3.394) Inbox (2.2.2.2194)
Citrix	XenMobile 9.0	Worx (10.0.1) With WorxMail

Таблица 2.

ОЦЕНКА МОБИЛЬНЫХ РЕШЕНИЙ: СЦЕНАРИИ И РЕЗУЛЬТАТЫ

Решения каждого производителя были загружены на мобильный телефон LG G3 с операционной системой Android 4.4. Мы сконфигурировали на решении Office 365 inbox и разрешили разделенный доступ к файлам и вебдоступ как с устройства, так и на него. Для корректности результатов испытаний мы использовали последние версии решений каждого производителя, по состоянию на февраль 2015 года.

СЦЕНАРИЙ ИСПЫТАНИЙ 1 – ПОДДЕРЖКА ПОТЕРЯННЫХ УСТРОЙСТВ

1. Сотрудник использует планшет как для личного, так и корпоративного доступа. Во время путешествия сотрудник теряет устройство. Сотрудник звонит в отдел IT и сообщает о потере. IT инициирует процедуру стирания всех корпоративных данных и доступа.
2. Спустя два часа сотрудник находит свое устройство и открывает его, чтобы посмотреть результаты действий IT. Тест получает оценку ПРОЙДЕН, если IT отдел смог осуществить стирание данных и блокировать доступ за данный период.

Цель испытания: определить, насколько хорошо каждое решение способно защитить сети и данные организации в случае потери устройства,

и определить, насколько точно это может быть осуществлено при сохранении неприкосновенности личных данных.

РЕЗУЛЬТАТЫ ИСПЫТАНИЯ

- Check Point: Check Point Capsule продемонстрировала возможность удаленного стирания корпоративных данных и отключения корпоративного доступа с устройства. При этом личные фото, хранившееся на этом устройстве, никак не были затронуты.
- Good: Good поддерживает удаленное стирание корпоративных данных из приложения «Good For Enterprise App».
- MobileIron: MobileIron имеет ограниченный выборочный функционал по стиранию только данных электронной почты. Другие данные на устройстве, такие как корпоративные файлы, могут быть удалены только используя полное стирание устройства.
- AirWatch: AirWatch поддерживет функцию стирания корпоративных данных на устройстве Enterprise Wipe.
- Citrix: Citrix XenMobile поддерживает функцию выборочного стирания корпоративных данных на устройстве Selective Wipe.

СЦЕНАРИЙ ИСПЫТАНИЙ 2 – ОТСЫЛКА ПО ЭЛЕКТРОННОЙ ПОЧТЕ ЗАРАЖЕННЫХ ССЫЛОК

ТОЛЬКО CHECK POINT ПУТЕМ ИСПОЛЬЗОВАНИЯ МЕХАНИЗМА ПРЕДОТВРАЩЕНИЯ УГРОЗ ПРЕДОТВРАЩАЕТ ЗАГРУЗКУ ВРЕДОНОСНОГО ПО НА МОБИЛЬНОЕ УСТРОЙСТВО. ВСЕ ОСТАЛЬНЫЕ ПРОИЗВОДИТЕЛИ ПОЗВОЛИЛИ ЗАГРУЗКУ ВРЕДОНОСНОГО ПО

Все высшее руководство компании получает сообщение электронной почты от известного кандидата на высокую должность. Сообщение содержит краткое изложения квалификации кандидата, а также ссылки на его профиль в социальной сети LinkedIn в формате PDF и на его личный вебсайт. Как файл, так и ссылка содержат вредоносный контент, который при его открытии может заразить устройство. Так как 9% получателей обычно переходят по фишинговым ссылкам, существует высокая вероятность, что кто-то перейдет и по этим ссылкам.

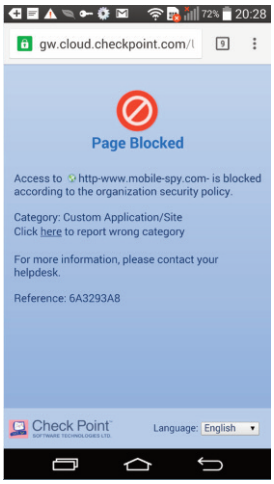
1. Посылаем сообщение электронной почты на мобильное устройство через корпоративную почту, защищенную одним из тестируемых решений.
2. Открываем электронную почту и находим две ссылки, которые ведут к:
   a. Загрузке вредоносного PDF файла на устройство;
   b. Доступу к вредоносному вебсайту, заражающему устройство. Для корректности теста ссылка с вредоносным контентом в почте должна быть доступна извне контейнера. Мобильные контейнеры не могут открывать внешний контент изнутри защищенного рабочего пространства и должны перенаправлять его в нативный браузер устройства.
3. Загружаем вредоносный pdf и проверяем заражение устройства вредоносным ПО;
4. Переходим по вредоносной ссылке и проверяем заражение устройства вредоносным ПО.

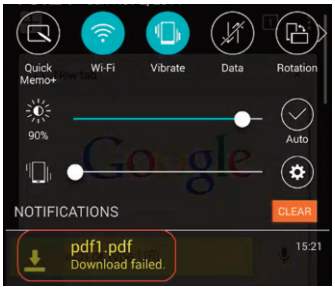
Цель испытания: проверить, может ли каждое из решений обеспечить защиту мобильного устройства от возможного заражения путем распознавания и блокировки вредоносного контента.

РЕЗУЛЬТАТЫ ИСПЫТАНИЯ

- Check Point: решение Check Point обеспечило защиту устройства, не позволив открыть PDF файл или получить доступ к вредоносному сайту. При попытке пользователя загрузить вредоносный PDF файл, загрузка была блокирована и ее процесс прерывался.

При попытке пользователя открыть ссылку на вредоносный веб-сайт, Check Point Capsule блокирует доступ к вебсайту и оповещает об этом пользователя.





- Good: при попытке открыть ссылку из внешнего домена Good перенаправляет запрос на родной браузер устройства, где она будет открыта, позволив вредоносному контенту заразить устройство.
- MobileIron: MobileIron позволяет пользователю открывать ссылку, принятую по электронной почте в браузере устройства. Это позволяет вредоносному контенту получить доступ к устройству.
- AirWatch: AirWatch по умолчанию открывает все ссылки в браузере AirWatch Browser. Однако, если эта опция выключена, нативный браузер устройства открывает ссылки и позволяет вредоносному контенту заразить устройство.
- Citrix:Citrix Worxmail позволяет открывать ссылки на устройстве, открывая его таким образом к заражению вредоносным ПО.

Необходимо отметить, что только решение Check Point, путем использования механизма предотвращения угроз, предотвращает загрузку вредоносного ПО на мобильное устройство. Ни одно из тестируемых решений не смогло защитить мобильные устройства от вредоносного контента при его открытии вне защищенного контейнера.

GOOD, MOBILEIRON, AIRWATCH, CITRIX: ЭТИ ПРОИЗВОДИТЕЛИ НЕ СПОСОБНЫ ПРЕДОТВРАТИТЬ ОТСЫЛКУ ДАННЫХ НА СЕРВЕР УПРАВЛЕНИЯ ШПИОНСКИМ ПРИЛОЖЕНИЕМ, УСТАНОВЛЕННЫМ НА УСТРОЙСТВЕ

СЦЕНАРИЙ ИСПЫТАНИЙ 3 – РАБОТА ПОСЛЕ ЗАРАЖЕНИЯ

Наше мобильное устройство случайно было оставлено залогиненым без присмотра. Некто находит его, загружает мобильное шпионское приложение, негласно в фоновом режиме сохраняющее все нажатия клавиш, и отсылающее все напечатанное на сервер управления. Затем он закрывает устройство и оставляет его на том месте, где оно будет найдено пользователем.

Мобильные шпионские приложения обладают возможностью собирать действия пользователя, такие как местоположение устройства, список звонков и контекст сообщений, снимки экрана и камеры, и иногда даже получать полный контроль над мобильным устройством. Адекватное решение безопасности должно изолировать защищенную область от такого рода шпионских программ.

1. Заражаем мобильное устройство шпионской программой. Активируем приложение. Это действие приводит к отсылке собранных на мобильном устройстве данных на сервер управления, контролируемый хакерами.

2. Пользователь открывает свое приложение электронной почты на устройстве, пишет сообщение внутри защищенного контейнера каждого производителя, и нажимает кнопку «послать». Если шпионское приложение может это видеть, копия этого контента будет отослана на контролируемый хакерами сервер управления.
3. Следим за сервером управления мобильного шпионского приложения, чтобы увидеть, получит ли он данный контент.

Вы можете найти дополнительную информацию о шпионских приложениях, мобильных троянских программах и защите мобильных устройств в следующих исследованиях, проведенных Check Point и Lacoon Security:

https://media.blackhat.com/eu-13/briefings/Brodie/bh-eu-13-lacoon-attacks-mdm-brodie-wp.pdf

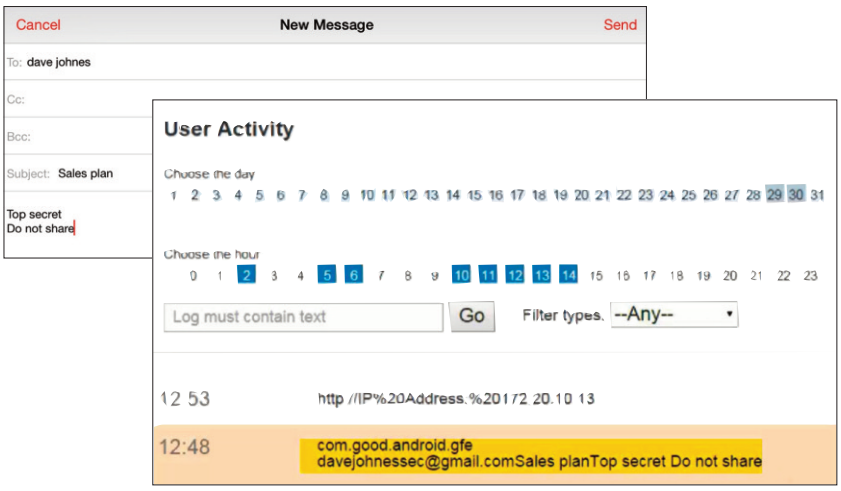
https://www.blackhat.com/docs/eu-14/materials/eu-14-Koretsky-A-Practical-Attack-Against-VDI-Solutions.pdf

Цель испытания: определить, до какой степени контейнеры разных производителей могут защитить мобильные устройства после заражения шпионским приложением.

РЕЗУЛЬТАТЫ ИСПЫТАНИЯ

- Check Point Capsule: все назначенные получатели получили тестовое сообщение электронной почты. Сервер управления шпионского приложения не был информирован о факте отсылки сообщения электронной почты, равно как и не произошло передачи контента письма на сервер управления.
- Good: «Good for Enterprise» не способен предотвратить отсылку данных установленным на устройстве шпионским приложением на сервер управления.

Ниже приведен пример написания сообщения электронной почты пользователем «Good for Enterprise» на устройстве, зараженном вредоносным ПО.



- MobileIron, AirWatch, Citrix: решения этих производителей не способны предотвратить отсылку данных на сервер управления шпионским приложением, установленным на устройстве.

СЦЕНАРИЙ ИСПЫТАНИЙ 4 – ЗАЩИТА ДОКУМЕНТА И КОНТЕНТА

Отсылка сообщений электронной почты с прикрепленными конфиденциальными документами компании является часто распространенной рабочей практикой. Оценка состоит из двух частей: в первой части оценивается, насколько хорошо защищен контент исходного документа, а во второй части – насколько хорошо защищен исходный документ от случайной отсылки не тому получателю.

1. Зашифровываем конфиденциальный документ компании, используя подход к защите документов, реализованный каждым производителем.
2. Прикрепляем зашифрованный документ к сообщению электронной почты и посылаем получателю внутри компании, который открывает его на мобильном устройстве, защищенном решением производителя.
3. Проверяем, допускает ли система защиты документов скопировать содержимое документа в буфер обмена мобильного устройства или в новое сообщение электронной почты внутри мобильного контейнера.

Во второй части руководителю необходимо получить дополнительную информацию от своей команды, и он пересылает исходный документ со своими заметками другим шестерым сотрудника. К сожалению, он случайно выбирает ошибочного адресата, и в результате отсылает сообщение конкуренту. Этот тест позволит определить, сможет ли конкурент открыть и прочитать исходный документ.

1. Зашифровываем конфиденциальный документ компании, используя подход к защите документов, реализованный каждым производителем.
2. Прикрепляем зашифрованный документ к сообщению электронной почты и посылаем получателю внутри компании, который открывает его на мобильном устройстве, защищенном решением производителя.
3. Получатель открывает приложенный файл на устройстве и сохраняет его внутри защищенного контейнера.
4. Затем, пользователь прикрепляет расшифрованный документ к другому сообщению электронной почты, и отсылает его конкуренту вне корпоративной сети.
5. Проверяем, доступен ли расшифрованный документ вне контейнера.
6. Проверяем, сможет ли конкурент получить доступ к полученному документу.

Цель испытания: первой целью этого испытания является оценка возможности решений мобильной безопасности предотвратить передачу данных из защищенного документа другому приложению или его копирование вне мобильного контейнера. Второй целью данного испытания является определение возможности применения тех же механизмов защиты в ситуации случайной отсылки документа за пределы защищенной сети.

РЕЗУЛЬТАТЫ ИСПЫТАНИЯ

- Check Point Capsule: документы, защищенные механизмами защиты документов Capsule, обладают атрибутами, специфическими для получателя. Все документы защищаются с использованием атрибутов, определяющих возможные действия пользователя в отношении документа. Существует лог и контрольный журнал для любого

вида активности, отражающие все действия, произведенные над документом. Защищенные документы могут быть открыты только внутри защищенного контейнера на устройстве. Capsule блокирует возможность открытия документа конкурентом.

- Good, MobileIron, AirWatch, Citrix: эти производители шифруют и защищают документ до тех пор, пока он находится внутри защищенного контейнера. Как только документы отсылаются с устройства внешнему получателю, они становятся незащищенными и могут быть открыты и просмотрены кем угодно.

БЕЗОПАСНОСТЬ: ПОЛУЧЕННЫЕ ДАННЫЕ

Большинство пользователей не любит носить с собой много устройств и склонно сочетать рабочую с личной информацией. Попытки ограничить это через политики MDM мотивируют сотрудников к поиску путей обхода механизмов безопасности устройства и операционной системы. Это может оказаться более опасным, чем отсутствие таких политик, так как многие из обходных путей сами по себе могут содержать вредоносное ПО.

- **Все производители оказались способны удаленно стирать данные со скомпрометированных устройств**, хотя некоторые из них предлагают только механизмы стирания почты или полного стирания устройства, так что надо внимательно читать все, что написано мелким шрифтом.
- **Check Point является единственным решением, способным обнаруживать и блокировать вредоносное ПО на мобильных устройствах.** Никто из производителей решений MDM/мобильных контейнеров кроме Check Point не смог определить, является ли загруженный на мобильное устройство контент вредоносным. Check Point Capsule является единственным решением, способным обнаружить вредоносное ПО и защитить мобильные устройства от заражения им.
- **Check Point является единственным решением, способным предотвратить кражу данных с устройств, зараженных вредоносным ПО.** Никто из производителей решений MDM/мобильных контейнеров кроме Check Point не смог защитить устройство, уже зараженное вредоносным ПО. Check Point Capsule является единственным решением, обнаруживающим и блокирующим шпионское приложение от экспорта данных за пределы контейнера.
- **Check Point является единственным решением, способным защитить документы за пределами контейнера.** В то время как все производители могут предотвращать копирование данных документа внутри контейнера, решение Check Point является единственным, способным отслеживать и защищать документы после того, как они покинули защищенную сеть.

ВЫВОДЫ

Управление парком мобильных устройств и поддержание единообразия их конфигураций являются важными задачами. Однако, главной задачей является обеспечение безопасности. Поддержание мобильных устройств в безопасном состоянии большую часть времени только за счет защиты приложений, или решения некоторого другого подмножества задач, не создает состояния мобильной безопасности. И хотя на рынке существует много решений мобильной безопасности, они обычно решают только часть задач по защите мобильных устройств. Таким образом, важно разрушить миф о мобильной безопасности и ложное чувство защищенности, созданное существующими решениями.

Первым разрушен миф о MDM, как решении по безопасности. В то время как MDM предоставляет контроль над устройством и приложениями, это решает только часть проблемы безопасности и работает только для корпоративных устройств. Вторым разрушенным мифом является утверждение о том, что мобильные контейнеры обеспечивают защиту от угроз. Мобильные контейнеры защищают и отделяют корпоративные данные на мобильных устройствах, но оставляют устройство, личные данные и приложения открытыми для всех видов угроз, таких как возможность загрузки нежелательных приложений (шпионских программ) и вредоносного контента на устройство. И, наконец, разрушен миф о защите документов и данных. Документы должны защищаться не только на самом устройстве, но и в процессе пересылки с или на устройство. Это должно достигаться путем наличия возможностей ограничения получателей, ограничения действий и отзыва доступа к документу в любое время.

Раскрытие мифов мобильной безопасности доказывает, что для поддержания безопасности мобильных устройств необходим другой, целостный подход. Check Point Capsule является единственным решением, которое предлагает полную безопасность мобильных устройств посредством:

- обеспечения защищенной бизнес-среды с помощью шифрования и сегрегации корпоративных данных от личных данных и приложений;
- полноценной защиты мобильных устройств от угроз. Оно распространяет корпоративные политики безопасности на мобильные устройства для предотвращения доступа к киберугрозам;
- шифрования и защиты корпоративных документов, куда бы они ни перемещались. Это позволяет быть уверенным, что получить к ним доступ смогут только авторизованные пользователи, как внутри контейнера, так и вне защищенной сети организации.

MDM, мобильные контейнеры и даже EMM обеспечивают лишь частичное решение по защите мобильных устройств. Только Check Point Capsule обеспечивает как безопасность самого устройства и данных внутри него, так и сети, к которой он подключен, обеспечивая одинаково надежную степень защиты. Мы приглашаем Вас самим попробовать Check Point Capsule и самим увидеть разницу – capsule.checkpoint.com.

НАШИ КОНТАКТЫ

Международная штаб-квартира | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Телефон: 972-3-753-4555 | Факс: 972-3-575-9256 | Эл. почта: info@checkpoint.com

Представительство в России и СНГ | Check Point Software Technologies (Russia) ООО | 109240, Москва, ул. Николоямская, д. 13, стр. 17 | Тел./факс: +7 495 967 7444 | http://rus.checkpoint.com