Целенаправленные атаки на мобильные устройства

ДиалогНаука

План презентации

1. Целевые атаки – общая информация
2. Целевые атаки на мобильные устройства
3. Пример решения для защиты
4. Советы по обеспечению безопасности

Продолжительность 20 мин

Особенности APT

APT - целенаправленная атака, при которой злоумышленник получает неавторизованный доступ в сеть и остается необнаруженным в течении длительного времени

Термин APT введен U.S. Air Force в 2006

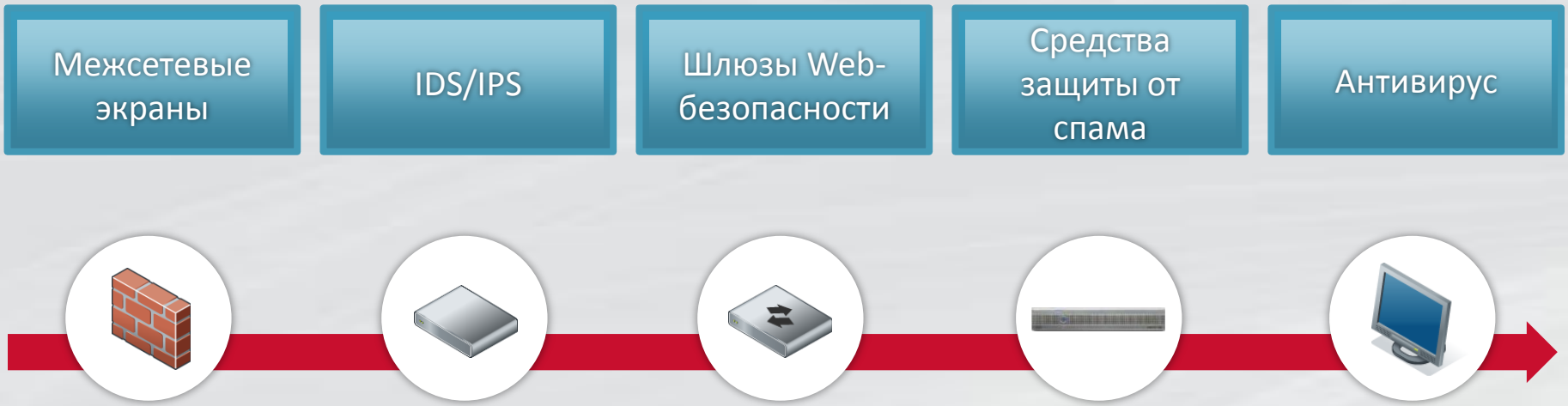
- **Advanced:** Атакующий является экспертом и использует свои собственные, неизвестные другим инструменты для эксплуатации уязвимостей
- **Persistent:** Атакующий не ограничен во времени, т. е. он будет тратить столько времени, сколько нужно, чтобы получить доступ и остаться незамеченным
- **Threat:** Атакующий организован, мотивирован, обладает необходимыми финансовыми ресурсами

APT

- считается наиболее опасным типом атак
- Характерные признаки целевых атак – использование социальной инженерии, применение эксплойтов «нулевого дня»
- спланированная атака, мотивированная деньгами, политикой/национальными интересами и направленная для достижения определенной цели (как получение доступа в проектах тестов на проникновение)

Типичный сценарий атаки

Особенности APT



Традиционные технологии не могут остановить APT

Особенности APT

Обход защиты основанной на анализе сигнатур

- Традиционные продукты, такие как IDS/IPS, межсетевые экраны следующего поколения (NGFW), шлюзы Web-безопасности (secure Web gateways), антивирусное ПО— анализируют сигнатуры для обнаружения известным им атак, и в некоторых случаях, неизвестных атак, которые используют известные им уязвимости

Обход защиты основанной на анализе аномалий

- Продвинутые IDS/IPS и решения анализирующие сетевые аномалии могут обнаруживать APT. Они собирают траффик (e.g., NetFlow, sFlow, cFlow) с сетевых устройств и сравнивают его с “обычным” сетевым трафиком в имевшем место в течении дня, недели, месяца
- Однако такие решения подвержены ошибкам 1-го и 2-го рода. False positives – когда нормальный трафик принимается за атаку, и наоборот, false negatives – когда атака воспринимается как нормальный трафик

Известные атаки

2014 Атакованы 100 банков из 30 стран

Известные атаки

2016

Пострадали

- Металлинвестбанк
- Алтынбанк
- Русский Международный Банк
- Система денежных переводов Рапида

- Swift

Известные атаки

2015

Топ-5 банк РФ – атака на мобильные устройства клиентов

Телефон все время находился в руках абонента. По его словам, он ничего не делал, никакие смс не отправлял, но деньги с банковского счета все равно исчезли

Анатомия атаки

- Клиент устанавливает проигрыватель Flash злоумышленника
- Вредоносный код посылает СМС на короткий номер «Баланс»
- Если получен ответ, значит телефонный номер привязан к банковскому счету
- Осуществляется перевод денежных средств
- Весь СМС обмен с банком стирается, включая СМС подтверждения операций

Известные атаки

В феврале 2015 года, Google удалил 3 вредоносных приложения из Google Play, которые были скачаны 15 миллионов раз!

Malicious Google Play apps (may have) hosed millions of Android handsets

"After a week, you might start to feel there is something wrong with your device."

by **Dan Goodin** - Feb 3 2015, 8:05pm MSK

Share Tweet 171

Известные атаки

Вот эти приложения:

- «Durak» – предназначенное для англоговорящих пользователей
- «IQ Test»
- «Russian History» – для русскоговорящих пользователей

Вредоносное ПО начало действовать, когда после его инсталляции прошло 30 дней

Когда пользователь обращался к устройству, ему выводилось сообщение о проблеме, например, устройство заражено, ПО устарело или выводилась порно-картинка на весь экран, которую нельзя было убрать.

После этого предлагалось совершить определенные действия: посетить фальшивый сайт, скачать новую версию приложения, отправить платный СМС, провести оплату с помощью банковской карты

Решение FireEye

- Компания FireEye с 2004 г в США
- Поставляет продукты с 2006 г
- Мировой лидер – FireEye используют 40% компаний Fortune 100

Решение FireEye

1

Аппаратный гипервизор FireEye

- Специализированный гипервизор
- Разработан для анализа угроз

2

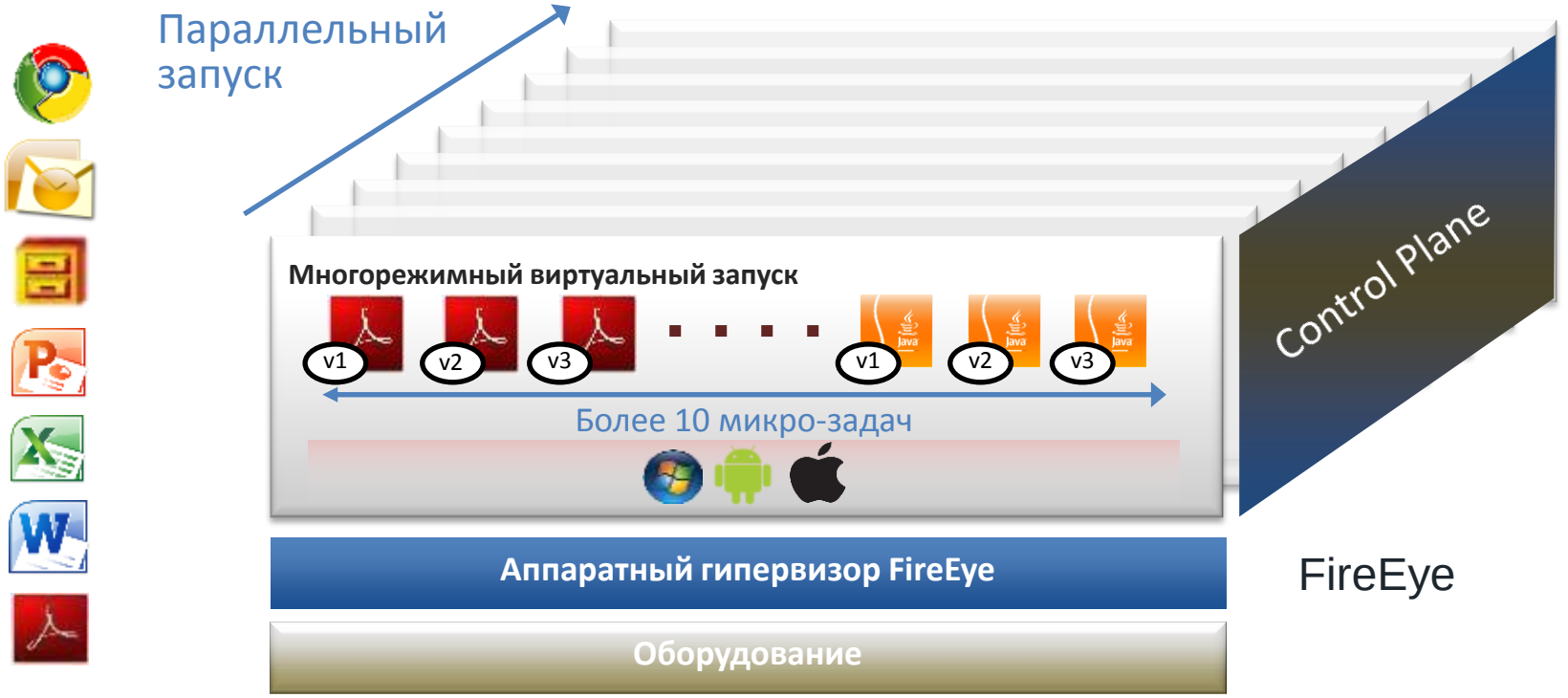
Многопоточный виртуальный запуск

- Разные ОС
- Разные сервис-паки
- Разные приложения
- Разные типы файлов

3

Защита от угроз в масштабе

- Параллельный запуск
- Многоуровневый анализ



Решение FireEye

FireEye Mobile Threat Prevention поддерживают Android и iOS

На мобильное устройство устанавливается пассивный агент FireEye Mobile Threat Prevention, который можно загрузить из Google Play или AppStore

Управление агентами осуществляется с помощью сервера управления, размещаемого в корпоративной сети.

Виртуальная машина, используемая для анализа приложений, находится в Облаке FireEye.

Проанализировать приложение можно несколькими способами:

- Самостоятельно загрузить его в облако FireEye
- Передать URL ссылку на его файл
- Или указать, что для анализа нужно использовать версию, находящуюся в Google Play или AppStore.

Решение FireEye

Работа агента заключается в инвентаризации установленных приложений. Для того, чтобы отличать установленные версии приложений, агент использует криптографические хеши.

Решение обнаруживает:

- неизвестное вредоносное ПО, которое пропускают антивирусы
- библиотеки, используемые для рекламы (adware)
- уязвимости в приложениях
- подозрительное/нестандартное поведение приложений

Решение FireEye

Если анализ приложения уже проводился, то FireEye оповещает пользователя об опасном приложении до того, как оно будет установлено.

FireEye Mobile Threat Prevention интегрируется с MDM решениями

- MobileIron
- AirWatch
- Samsung Knox

Использование MDM решений позволяет блокировать и удалять вредоносное ПО, уничтожать корпоративную информацию или блокировать устройство в случае потери или кражи.

Советы

- Не отвечайте на запросы содержащие персональную информацию, в том числе пароли.
- Для контакта с банком используйте номера с ваших банковских карт
- Если вам приходит СМС или звонок – будьте осторожны, не доверяйте
- Ограничьте сумму доступную на ваших банковских картах
- Установите СМС и e-mail оповещения
- Посетите офис вашего мобильного оператора. Запретите обращение по доверенности
- Регулярно отслеживайте состояние ваших счетов

Дополнительная информация – наши статьи

«Защищаемся от целенаправленных атак»
Национальный Банковский Журнал, №2 февраль 2014

«Целенаправленные атаки – обнаружение и защита»
Информационная безопасность, №2 май 2014

«Расследование целевых атак»
Безопасность Деловой Информации, №06 II квартал 2014

«Защита от вредоносного кода на мобильных устройствах»
Информационная безопасность банков, №3 / 2015

«Защита банков от незаконного вывода денежных средств»
Информационная безопасность банков, №2 / 2016

Вопросы?

info@dialognauka.ru
8(495)980-67-76
www.DialogNauka.ru

ДиалогНаука