Новое в защите от целенаправленных атак

Николай Петров, CISSP
Заместитель Генерального директора

АО «ДиалогНаука»

ДиалогНаука

План презентации

- Целенаправленные атаки – общая информация
- Эволюция систем защиты за последние 3 года
- Советы по обеспечению безопасности

Особенности APT

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

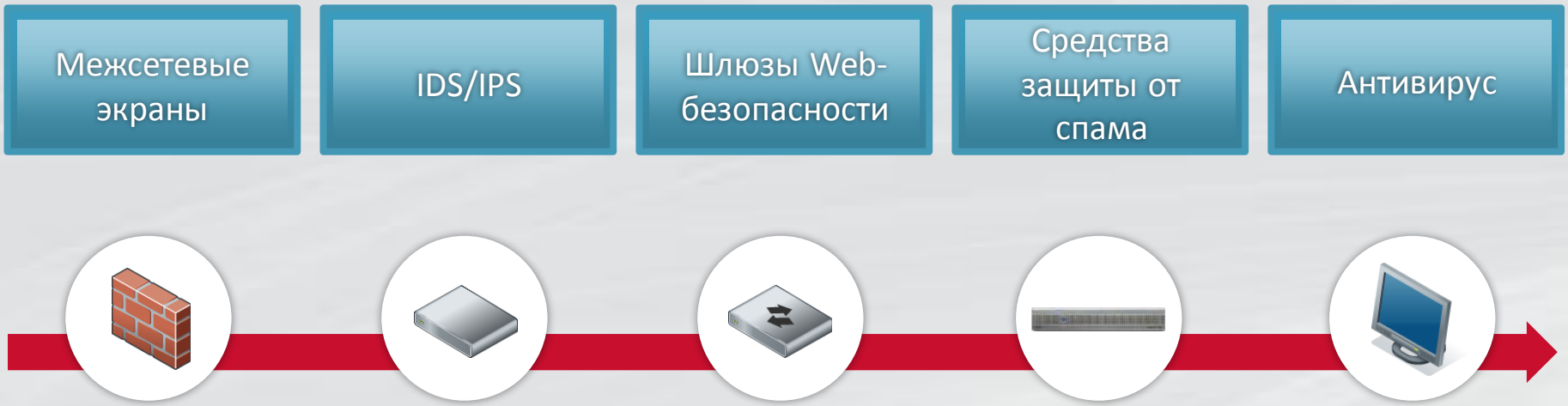
Термин APT введен U.S. Air Force в 2006

- **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)

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 2017 г

InterContinental Hotels

В апреле компания, владеющая такими известными брендами, как Holiday Inn и Crowne Plaza объявила, что злоумышленники установили вредоносное ПО в 1,200 отелей и собирали данные кредитных карт

Google

В мае злоумышленики совершили фишинговую рассылку направленную на Gmail пользователей, вынуждая их кликнуть на Google Doc link. Google остановил атаку в тот же день, но миллион пользователей уже были заражены.

Deloitte

В сентябре, Deloitte, одна из компаний большой 4-ки, объявила, что злоумышленники получили доступ к конфиденциальной информации ее 350 клиентов.

Известные атаки 2017 г

Uber

В ноябре Uber объявил, что заплатил злоумышленникам $100,000 для удаления похищенной информации о 57 миллионах клиентов и сотрудников компании

Yahoo!

В октябре Yahoo объявил, что 3 млрд ее пользователей электронной почты были скомпрометированы еще в 2013 г

Equifax

В сентябре кредитное агентство Equifax объявило о том, что злоумышленники похитили информацию о 143 млн американцев, включая даты рождения, адреса, номера социального страхования. Это почти половина населения США

Известные атаки 2017 г

WannaCry

В мае вредоносное ПО WannaCry атаковало тысячи компаний, включая FedEx и Nissan. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (FinCERT) сообщил, что вирус WannaCry затронул ресурсы нескольких российских банков. Атака затронула деятельность серверов российских телекоммуникационных компаний и силовых ведомств. Среди них оказались «МегаФон», «ВымпелКом», компьютеры МВД

Petya Virus

В июне тысячи компаний атаковало вредоносное ПО Petya. В нашей стране о заражении сообщили российские филиалы производителей Mars, Nivea, металлургическая компания ЕВРАЗ и гиганты энергорынка «Башнефть» и «Роснефть»

Обнаружение взлома

Источник: Mandiant M-Trends Report

63%

Компаний узнали, что их взломали от сторонних организаций

100%

У всех потерпевших антивирус был обновлен и содержал последние сигнатуры

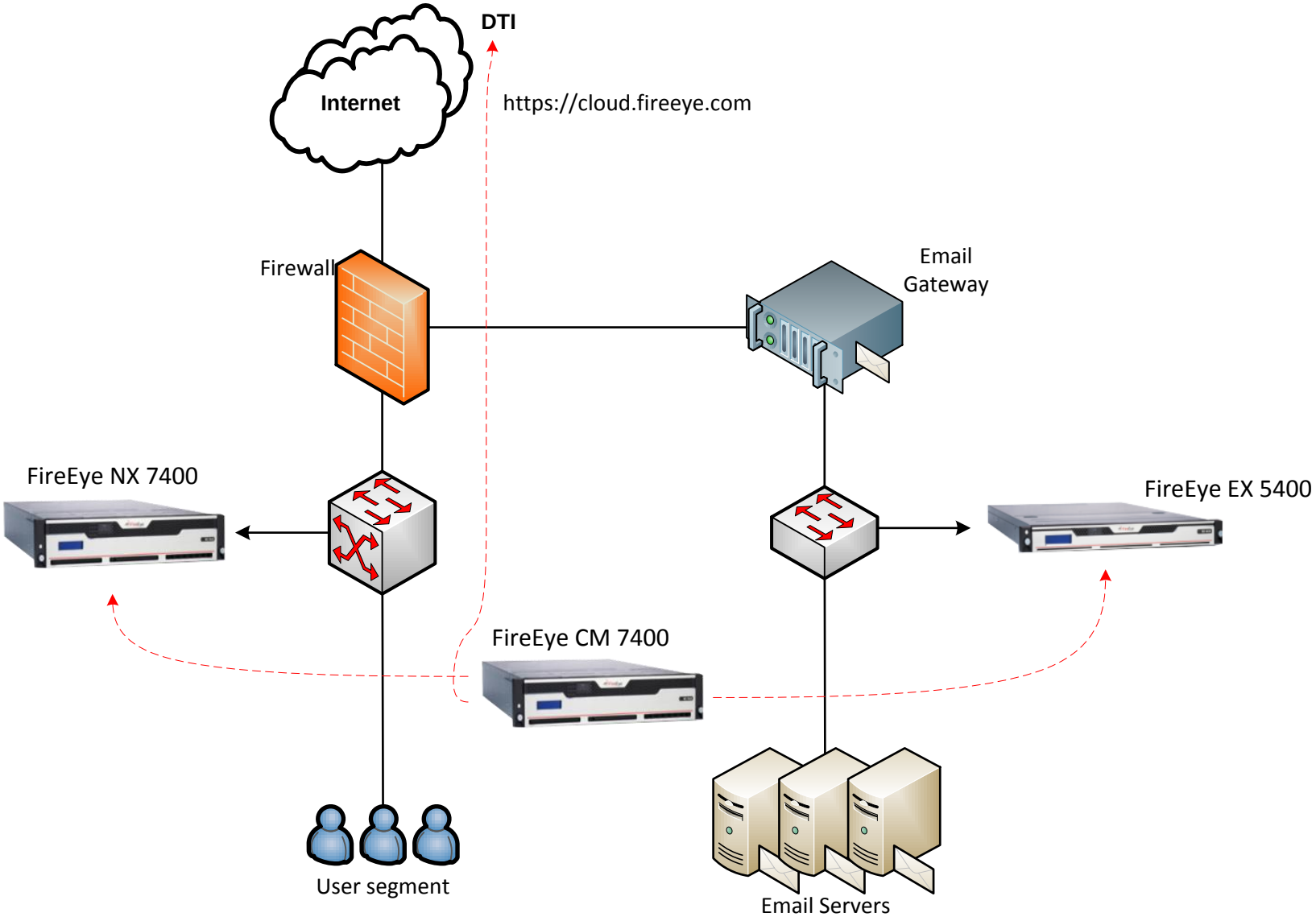
Наш опыт 2014-2015

Мы начали поставлять системы защиты от целенаправленных атак в 2014 г выбрав решения мирового лидера FireEye

Стандартная поставка включала устройства защиты

- Web
- E-mail
- И устройство управления

Схема решения



Как работает FireEye

1

Аппаратный гипервизор FireEye

- Специализированный гипервизор
- Разработан для анализа угроз

2

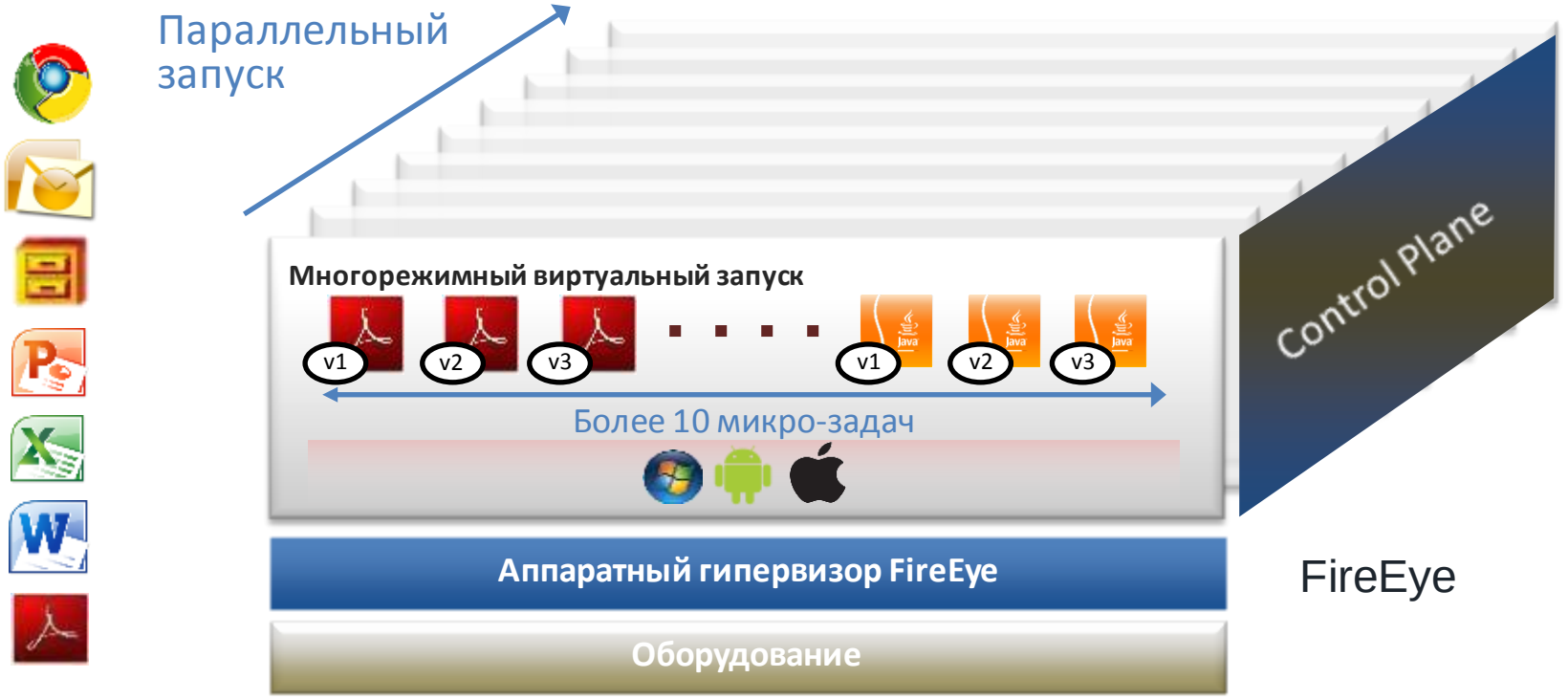
Многопоточный виртуальный запуск

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

3

Защита от угроз в масштабе

- Параллельный запуск
- Многоуровневый анализ



Передача информации об атаках

Передача информации об атаках

- Файлы из вашей сети не передаются в Облако (Персональные данные, конфиденциальная информация)
- Идентификаторы вредоносного ПО со всего мира
- Возможность выбрать вариант обмена информацией

Наш опыт 2015-2016

Мы стали дополнительно поставлять решение TDS (Threat Detection Service) компании Group-IB

Несколько наших клиентов поставили сразу 2 решения

- FireEye
- TDS

В конце 2016 в наш портфель решений добавлен продукт Kaspersky Anti Targeted Attack (KATA)

Наш опыт 2017

В 2017 г целый ряд клиентов покупает решения для защиты конечных точек. До этого времени, только один банк внедряя сетевую защиту FireEye, приобрел решение для защиты хостов.

Эта тенденция продолжается и в 2018 г

Мы предполагаем, что это закономерный результат развития систем защиты.

- Что делать, если несколько рабочих станций из парка в 2000 или 10000 заражены?
- Какие именно заражены?
- Вредоносный код может не проявлять себя
- А что, если это шифровальщик?
- Как эти рабочие станции найти и очистить?

Описание FireEye HX

Появился после слияния с компанией Mandiant (на основе продукта Mandiant Intelligence Response)

2 типа устройства

- поддерживает 15К агентов
- поддерживает 100К агентов

Агенты устанавливаются на Windows, Linux, Mac OS

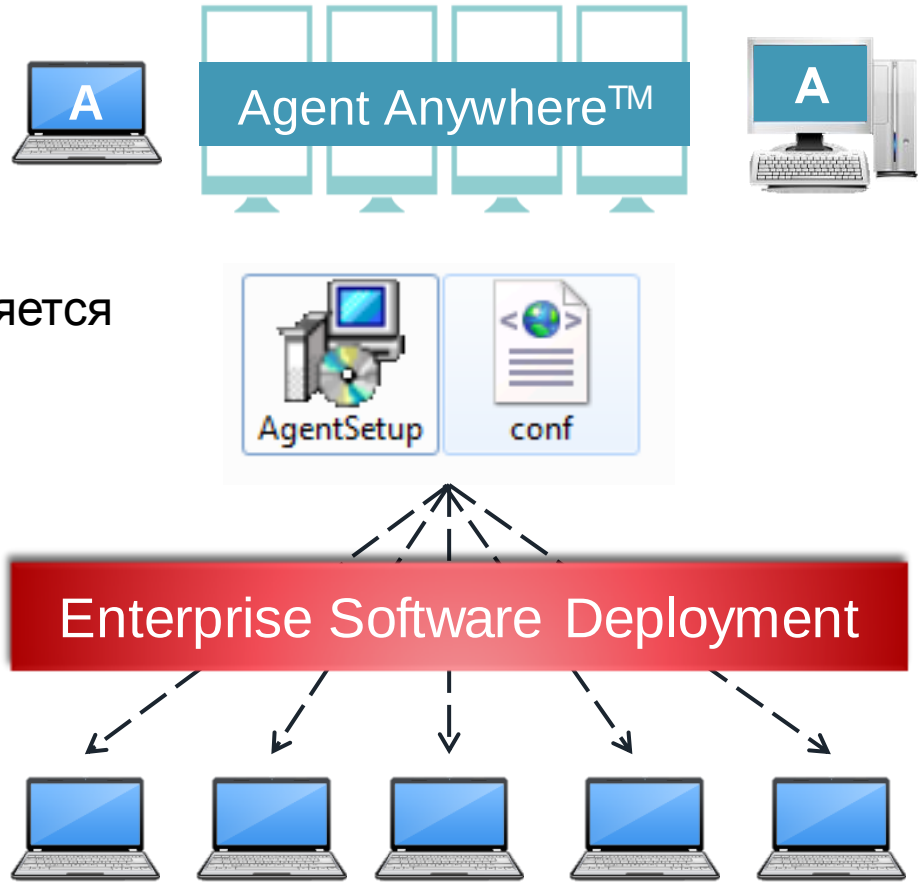
Могут быть использованы как отдельно, так и вместе с FireEye NX и EX

Описание FireEye HX

- Легкий агент
- Создает мало траффика
- Скрывает себя
- Не требует подтверждения
- Легко инсталлируется и обновляется
- Может легко обнаружить

скомпрометированные рабочие станции, где бы они не находились

- И изолировать их от сети



Kaspersky EDR

В феврале 2018 компания анонсировала решение по защите конечных точек Kaspersky Endpoint Detection & Response.

Советы по обеспечению безопасности

Использование эшелонированной защиты, путем использования:

- и правильной настройки межсетевых экранов
- антивирусного ПО
- ограничений запуска программ («белых списков»)
- веб фильтрации
- систем защиты от целенаправленных атак
- программ повышения информированности сотрудников

Вопросы?

ДиалОгНаука