SolidLab

Professional services. Development. Research

# Защита корпоративных ресурсов в эпоху недоверенных клиентских устройств

**Андрей Петухов**
CEO @ SolidLab
7 июня 2017

# ПРЕАМБУЛА

- Мы занимаемся практической безопасностью
- Основная специализация – анализ защищенности
  - пентесты
  - «боевые учения» в режиме red team vs blue team
  - анализ кода
- Видим варианты реализации ИТ и ИБ в крупных организациях в финансовой сфере и не только
- Данный рассказ – итог аналитической обработки опыта, полученного за последние 5 лет

# ТЕНДЕНЦИИ И СЛЕДСТВИЯ

- Мобильность
- Интеграция систем
- Централизация управления
- Виртуализация и облака

Было

- ЛВС-DMZ-Интернет



Стало

# НАЧАЛЬНЫЕ ШАГИ АТАКИ НА КОМПАНИЮ

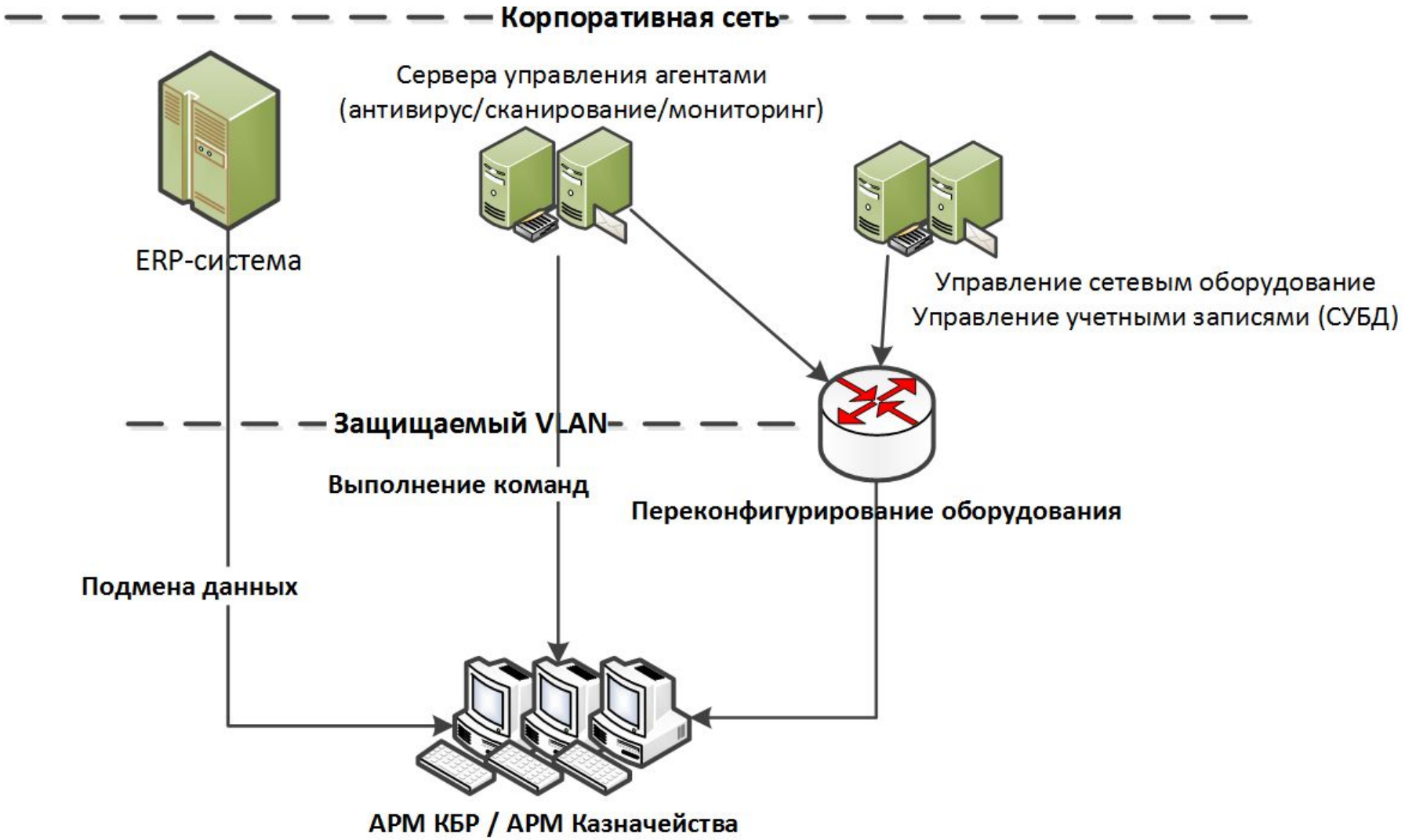
- Первый шаг – получение доступа в корпоративную сеть
  - социальная инженерия с вредоносным вложением
  - личные и/или мобильные устройства сотрудников
  - ethernet-гость, взлом корпоративной WiFi
  - пробив периметра через публичные приложения
- Второй шаг – повышение прав в AD
- Третий шаг – начало пути по доступу к цели
  - доступ к серверам, интегрированным в домен
  - доступ к рабочим станциям администраторов и разработчиков

- Наша статистика:
  - при получении прав пользователя домена дойти до доменного администратора удавалось в 100% случаях

# РАЗВИТИЕ АТАКИ - УДОБНЫЕ РЕШЕНИЯ

- Single Sign On
  - без второго фактора на критичных системах – конец игры
- Централизованное управление ресурсами ИТ/ИБ
  - антивирусами на узлах
  - сетевыми устройствами и учетными данными
  - агентами сканирования/мониторинга
- ERP-системы, с которыми интегрируются другие бизнес-приложения
  - захват системы => контроль бизнес-процессов
- Виртуализация
  - захват платформы => захват гостевых машин

# ПРИМЕР ВЕКТОРОВ АТАК НА КРИТИЧНЫЙ СЕГМЕНТ



# ВЫВОДЫ

- Любое пользовательское устройство в сети в любой момент может оказаться недоверенным
- При поглощениях и слияниях недоверенные – целые инфраструктуры
- Сегментация не так эффективна, как раньше
  - централизация управления/интеграция систем
  - поддерживать строгий least privilege на уровне сети нереально
- Рациональная стратегия: перестать наводить порядок в хаосе и сосредоточиться на защите самого ценного

# ЗАЩИТА САМОГО ЦЕННОГО

- Повышение стоимости атаки на защищаемый сегмент
  - правильный второй фактор
  - контроль публикации и исполнения собственного кода
- Мониторинг
  - мониторинг в эпоху миллиона событий и фокусы
- «Боевые учения» или read team vs blue team
  - как узнать, что мониторинг работает

SolidLab

Professional services. Development. Research

# Спасибо за внимание!
# Пожалуйста, вопросы!

**Андрей Петухов**

andrew.petukhov@solidlab.ru

mob: +7 916 360-52-49

tel: +7 499 705-76-57