Мобильный офис глазами пентестера

Дмитрий Евтеев (Positive Technologies)

Предисловие

- **Бизнес требует доступности всех ИТ-сервисов из любой точки земного шара и с любых мобильных устройств…**

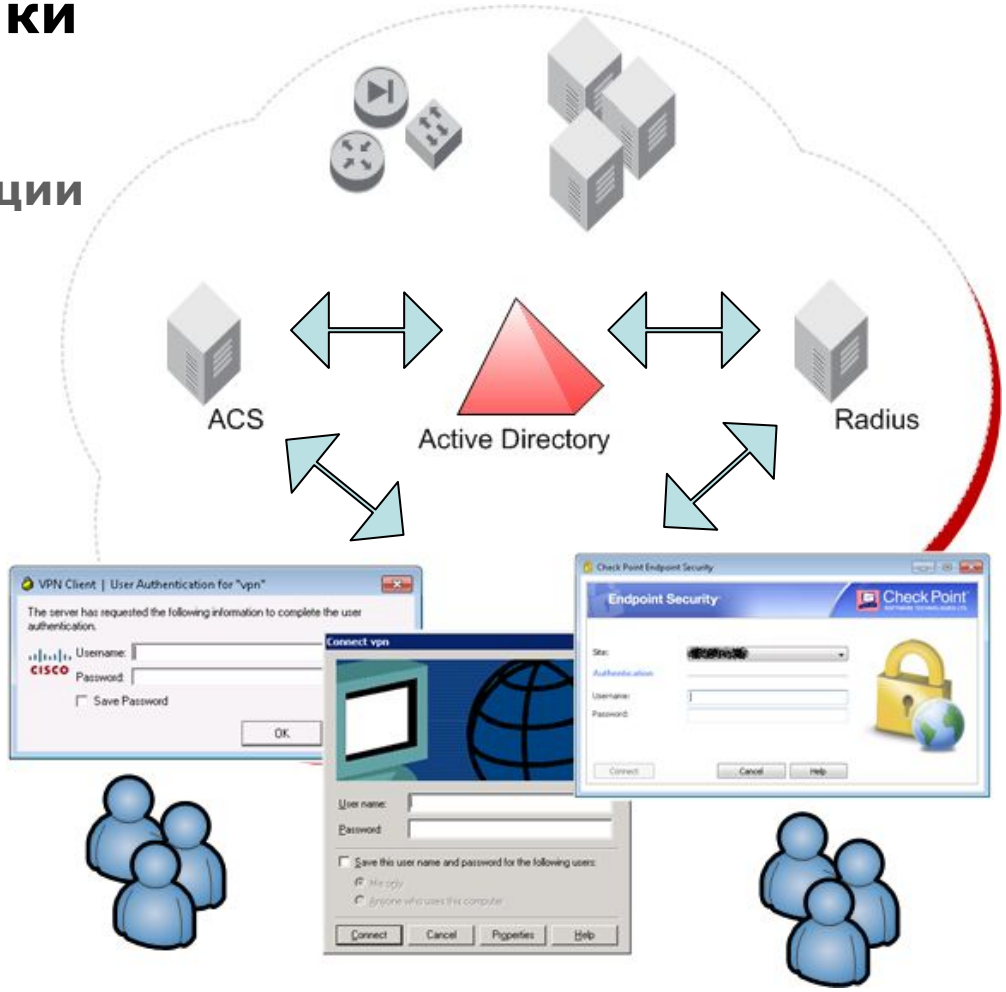
- **Чем это может обернуться?**

Основные точки входа в корпоративные сети

- **веб-приложения**
- **интерфейсы удаленного администрирования**
- **удаленный доступ к сети**
  - **VPN-шлюзы**
  - **Доставка приложений через веб-сервисы**
- **рабочие станции пользователей**
- **беспроводные сети**
- **сервисы инфраструктуры (базы данных, сторонние приложения и т.п.)**

Стандартная схема построения корпоративной ИС

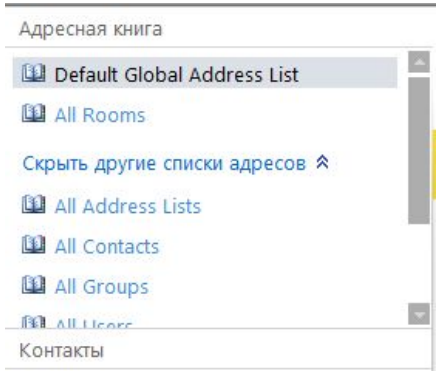
- **Типовые сценарии атаки**
  - **На Active Directory**
  - **На сервера аутентификации**
  - **На оборудование**
  - **На каналы связи**
  - **На VPN-шлюзы**
  - **На пользователя**



Как действует атакующий

- **Атакующий идет по пути наименьшего сопротивления!**

3. Список действующих (!) идентификаторов



1. Список идентификаторов

2. Перебор

3. Верификация доступа;
перебор действующих идентификаторов

Проблема парольной защиты

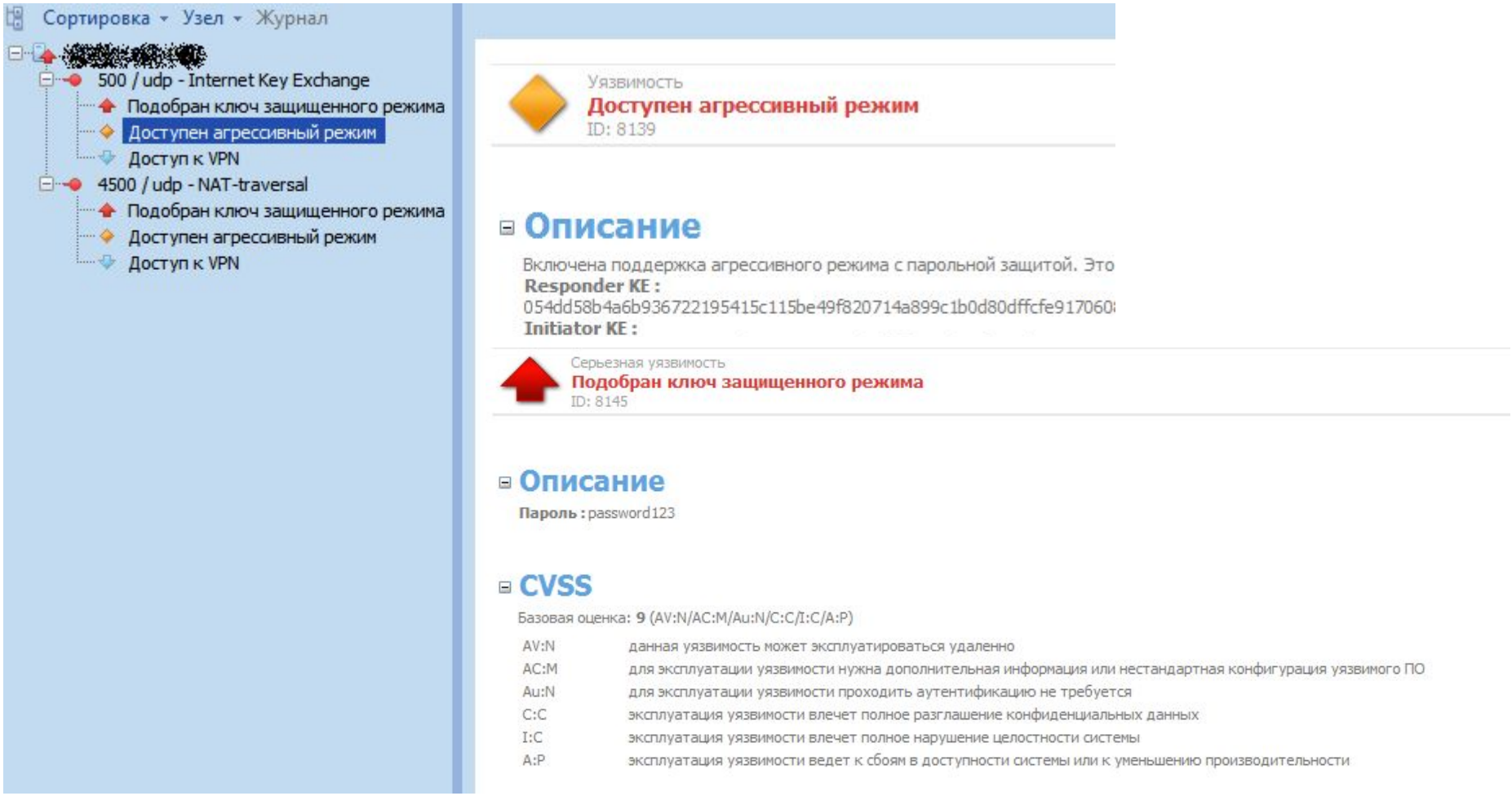
- **Более половины пользователей в Российских компаниях используют цифровые пароли**
  http://www.ptsecurity.ru/download/PT-Metrics-Passwords-2009.pdf

  - **Политика сложности используемых паролей в сетях Microsoft имеет известные недостатки**

  - **Чем больше сотрудников в компании, тем выше вероятность успешной атаки**

  - **За последние три года (!) в ходе проведения тестирований на проникновение не было ни одного случая, когда не удавалось получить список всех идентификаторов Active Directory с использованием указанной атаки**

Агрессивный режим IPSEC



Основной режим IPSEC

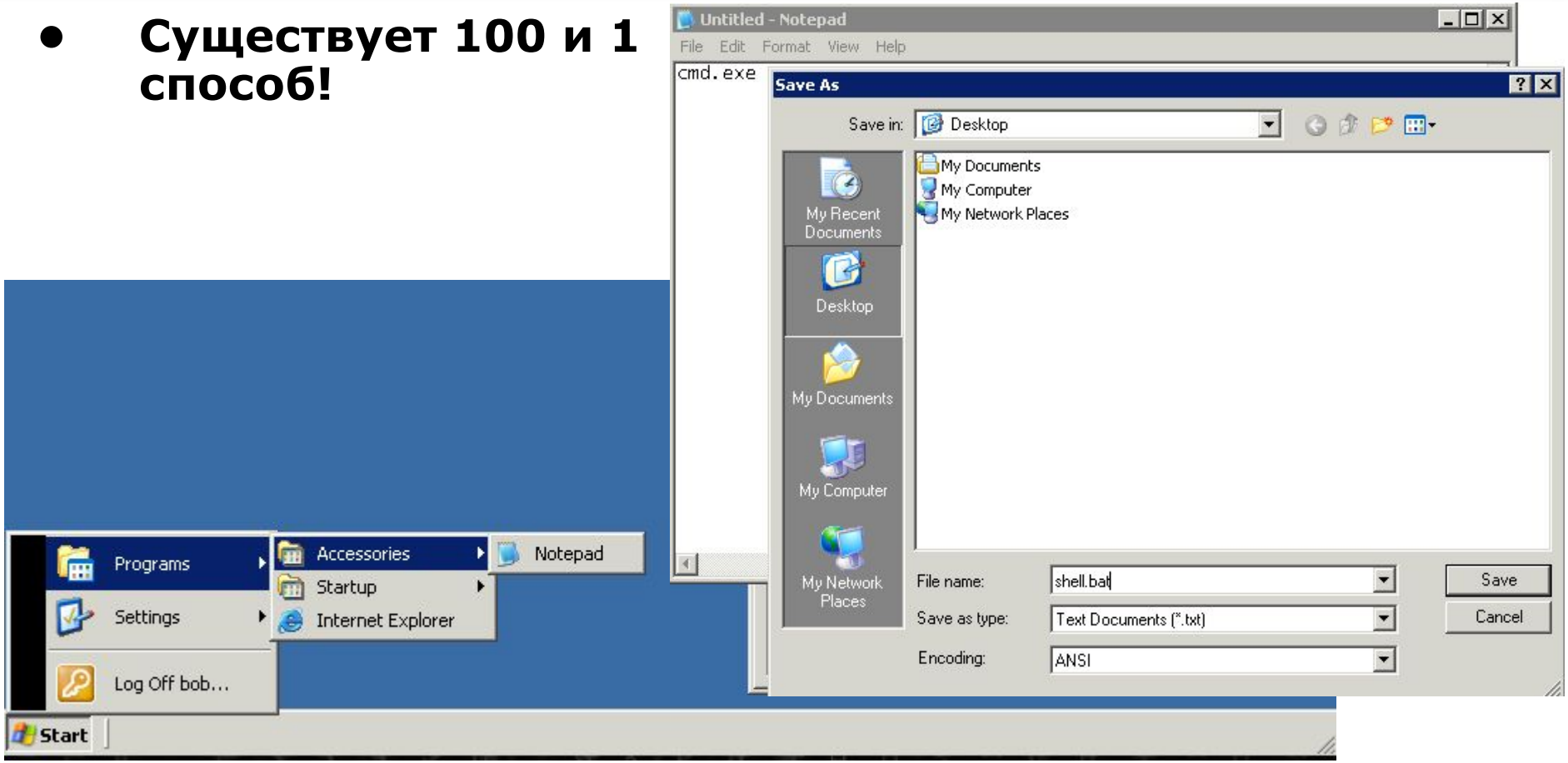
- **Pre-shared key и GroupName могут быть восстановлены путем перебора**
- **Могут быть найдены в свободном корпоративном доступе**
  - **Подробные инструкции по настройке**
  - **Сохраненные конфигурации**
- **Могут быть получены с использованием других сценариев атак**

Чем опасен удаленный доступ к сети

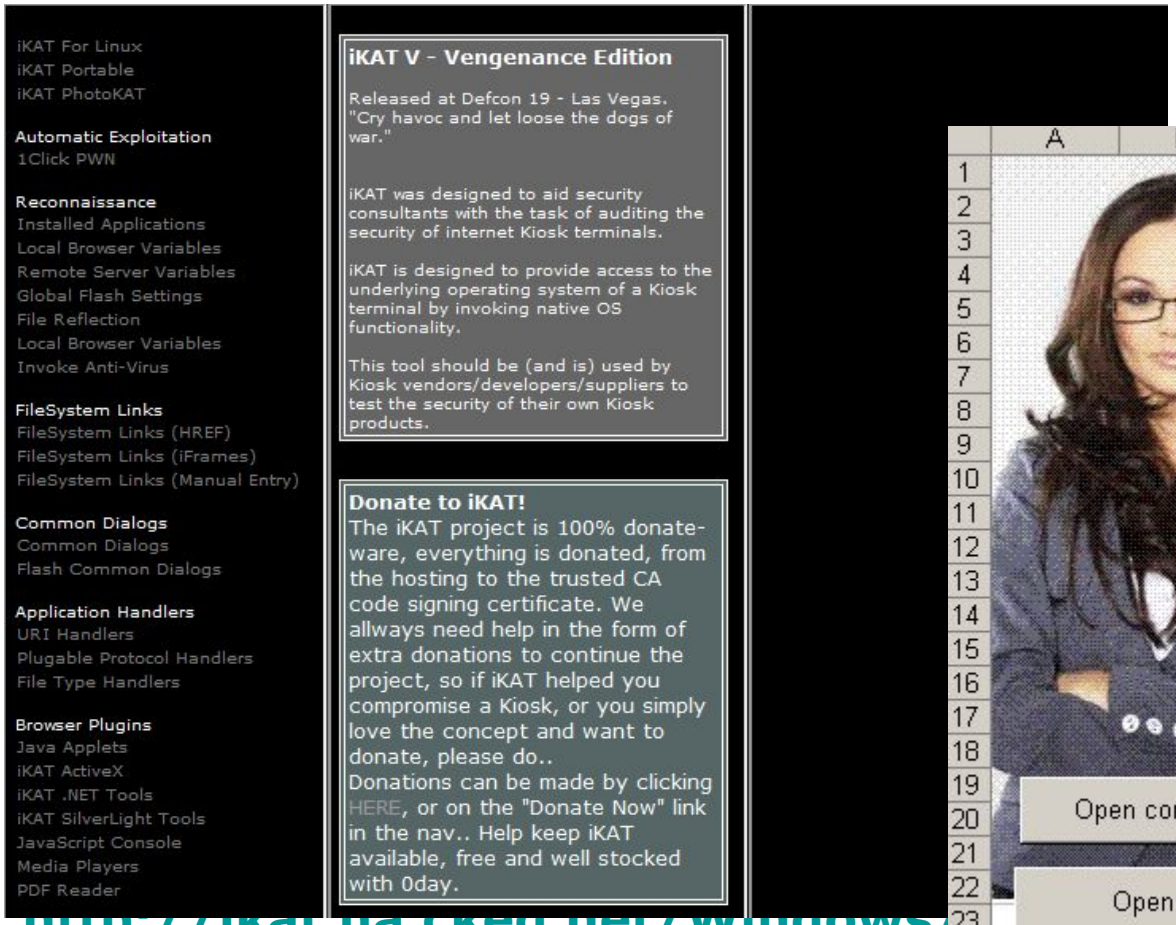
- **Классический удаленный доступ к сети (IPSEC/PPTP)**
  - **Пользователь обладает административными привилегиями в своей системе**
- **Доставка приложений через веб-сервисы (eq Citrix)**
  - **Пользователь обладает локальным доступом к ОС**
  - **Пользователь может расширить свои знания о существовании всех опубликованных приложениях**
  - **Пользователь из одной точки может получить сетевой доступ к любым опубликованным приложениям (в случае отсутствия правильной фильтрации)**

Citrix Jailbreak (1/2)

- **Существует 100 и 1 способ!**



Citrix Jailbreak (2/2)



http://ikat.ha.cked.net/Windows/

Резюме

- **Удаленный доступ к корпоративной сети через легитимный канал очень привлекателен с позиций атакующего**
- **Основные недостатки при организации удаленного доступа к корпоративной сети**
  - **Использование паролей, вместо цифровых сертификатов**
  - **Повсеместное использование нестойких паролей (!)**
  - **Отсутствие безопасной сегментации сети**
  - **Недостаточное разграничение сетевого доступа**
  - **Отсутствие мониторинга аномалий и начала атаки**

Спасибо за внимание!
Вопросы?

devteev@ptsecurity.ru
http://devteev.blogspot.com/

POSITIVE TECHNOLOGIES