Безопасность данных

Информационная безопасность

Информационная безопасность

- Процесс обеспечения основных свойств информации
  - Конфиденциальность
  - Целостность
  - Доступность

ИБ как процесс

- Обеспечение ИБ требует постоянного выполнения определенного набора мероприятий
  - Постоянные затраты
- Достижение “разумной защищенности”
  - Затраты < Потери

Угроза ИБ

- Совокупность условий и факторов, создающих опасность нарушения информационной безопасности
  - Классифицируются по различным признакам
- Модель угроз
  - Перечень угроз ИБ данной ИС с их характеристиками

Корпоративная информационная безопасность

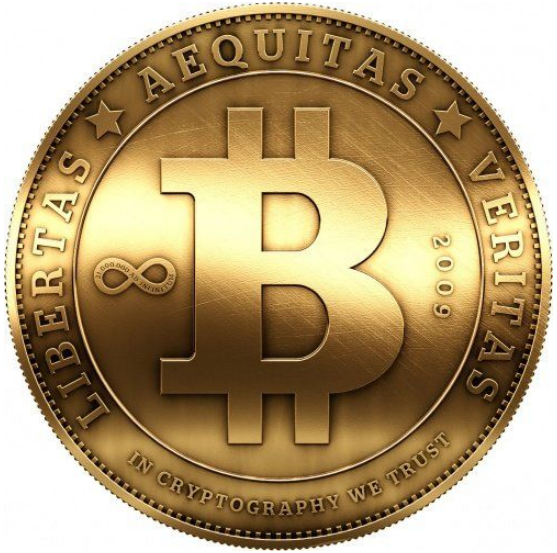
- Обеспечение непрерывности бизнеса
- Построение системы защиты информации
  - Организационно
  - Технически
- “Культура постоянного совершенствования”
- Снижение расходов на менеджмент инцидентов
- “Государство как угроза”

Личная информационная безопасность

- “Цифровая гигиена”
- Реализация несложных принципов информационного самосохранения
- Основной ресурс - время
- Основной нарушитель - мошенник
- Комфорт как актив

Угрозы данным на современном этапе

Тенденции, влияющие на развитие угроз ИБ

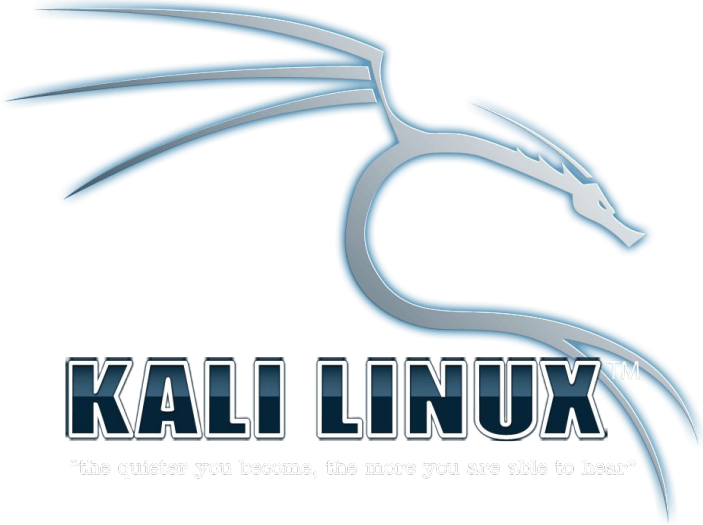


- Распространенность криптовалют
  - Наличие безопасного метода перевода денег от жертвы к вымогателю
- Рост популярности анонимных сетей
  - Tor, i2p
  - Защищенная площадка для встречи заказчика и исполнителя

Тенденции, влияющие на развитие угроз ИБ

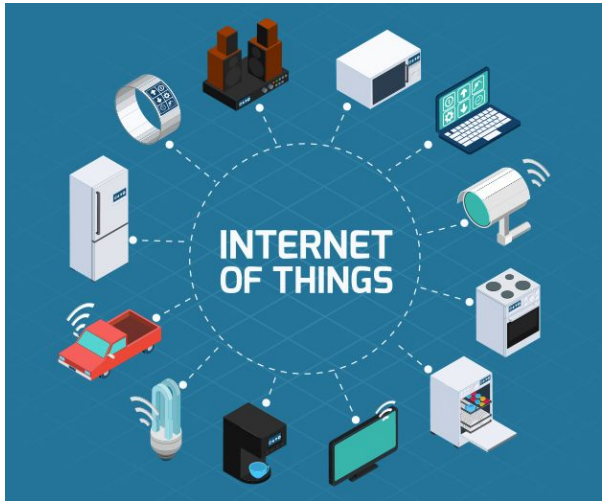
- Обнаружение “запрограммированных” уязвимостей
  - Утечка инструментария спецслужб в открытый доступ
  - Сложность в реагировании на угрозу
  - Широчайший спектр “зараженных” устройств и программ

Тенденции, влияющие на развитие угроз ИБ



- Высокая степень автоматизации средств нападения
  - Автоматизация поиска, сканирования и применения средств
- Падение требуемого уровня квалификации для выполнения хакерских атак

Тенденции, влияющие на развитие угроз ИБ



- Интеграция широкого класса устройств в единое информационное поле
  - Компрометация одного устройства ведет к ослаблению защиты остальных
  - Доступ к данным возможен с нескольких точек
  - Расширение списка способов “доставить неудобство”

Отечественная проблематика ИБ

- Кадры
  - Наличие определенного уровня подготовки в вопросах ИБ обязательно для всех сотрудников
- Государственный “формальный” подход
  - “Информационная безопасность как борьба с проверяющим”
  - Формальный подход порождает формальное отношение

Актуальные реализации угроз ИБ

Эволюция угроз

- Львиная доля концепций угроз ИБ сформировалась достаточно давно
  - На фоне зарождения информационных систем и начала их распространения
- Угрозы мутируют и эволюционируют, опираясь на существующие тренды и достижения в ИТ

Вредоносные программы

Вредоносные программы

- “malware”, “malicious software”
- Атака с использованием специального ПО, выполняющего задачу и имеющего механизмы распространения
- Существуют разные виды вредоносных программ
  - Червь, вирус, “троянский конь” и т.п.
- Разработка программ поддается автоматизации

Неизбирательные вирусные атаки

- “Вирусная эпидемия”
- Распространение через уязвимости в ПО, социальную инженерию и халатность жертв
  - Распространение программы может иметь сложный паттерн

Потенциальные цели

- Кража “хорошо известных” данных
  - Файлы популярных форматов, данные банк-клиентов и т.п.
- Разрушение ИТ-инфраструктуры
- Блокирование доступа к данным с целью выкупа
- Захват компьютеров под свое управление
  - Майнер & Кликер

Непосредственный заработок

- Майнеры
  - Зловредные программы, генерирующие криптовалюту с помощью вычислительных мощностей компьютера
- “За все надо платить”
  - Зачастую маскируются в “взломанных” нелицензионных программах
  - Популярны в игровых сборках

Мобильная специфика

- Реклама - популярная модель монетизации мобильных приложений
  - Накрутка “кликов” - способ конвертации рабочего времени мобильного телефона в деньги
- “Кликер”
  - Программа, без ведома пользователя осуществляющая “клики” по рекламе

Точечная атака с применением malware

- Используется для атаки определенной ИС
- Распространяется в окружении жертвы
- Может использовать сложные схемы обхода защит
- Создается с учетом характеристик и “портрета” жертвы

Точечная атака с применением malware

- Требует серьезных инвестиций в ИБ
  - Проведение полноценного комплекса организационно-технических мероприятий
- Наличие точечной атаки говорит о серьезности намерений злоумышленника

Эксплуатация уязвимостей

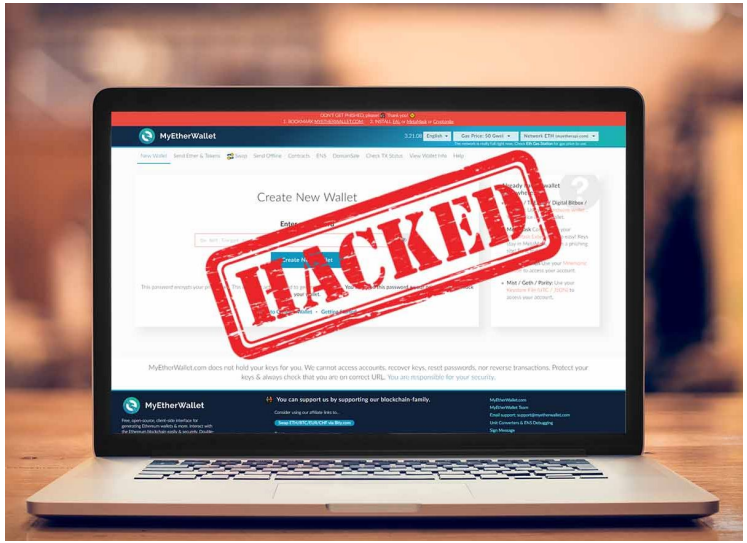
Эксплуатация уязвимостей

- Уязвимость программы
  - Особенность реализации программы, допускающая незапланированное поведение
- Эксплойт
  - Программа, эксплуатирующая уязвимость другой программы
- “Шеллкод”
  - Внедряемый в жертву программный код

Эксплуатация уязвимостей

- Выполняется как точечно\вручную, так и автоматизировано и на большой аудитории
  - С учетом задач, стоящих перед атакующим
- Один из основных рабочих инструментов проникновения в компьютерные системы

Точечные атаки



- Направлены на решение конкретных, зачастую специфичных задач
- Выполняются вручную квалифицированными специалистами
- Характеризуются упорством атакующего, адаптивным планом действий, применением нестандартных решений

Цель точечных атак

- Кража\уничтожение данных
- Ограничение доступа с последующим требованием выкупа
- Организация скрытого наблюдения за ИС
- Фабрикация улик, загрузка компрометирующей информации

Реализация атаки

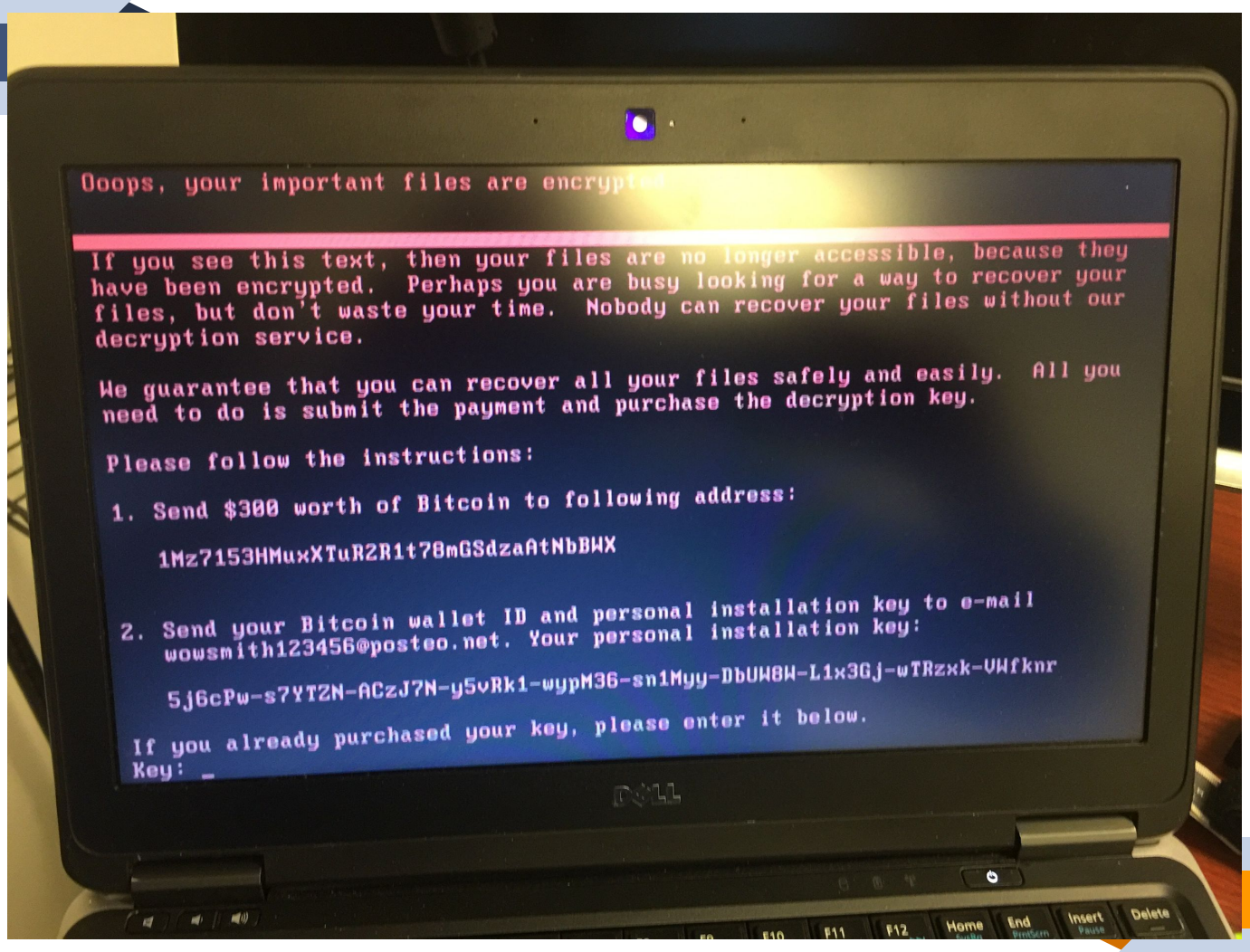
- Поиск
- Исследование
- Эксплуатация уязвимостей
- Закрепление результата
- Выполнение задачи
- Уничтожение следов

Атаки широкого охвата

- Выполняются автоматическими распределенными системами
  - Работают по плану с четким условием отказа
- Работают на большом количестве компьютеров
- В случае, если план не приводит к успеху - теряют интерес к жертве

Цели атак широкого охвата

- Захват компьютеров под контроль
  - Установка ПО для выполнения нужных злоумышленнику задач
- Поиск потенциально ценных данных
  - Данные интернет-банков, пароли, документы
  - Данные прочих уязвимых предложений
- Ограничение доступа к данным с последующим требованием выкупа


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
5j6cPw-s7YTZN-ACzJ7N-y5vRk1-wypM36-sn1Myy-DbUW8W-L1x3Gj-wTRzxk-VWfknr
If you already purchased your key, please enter it below.
Key: _

EternalBlue

- Уязвимость протокола сетевого окружения Windows
- Использовалась вирусами Petya и WannaCry
- Существовала незамеченной 16 лет
- Один из первых эксплойтов связывают с подразделением АНБ

Особенности эксплуатации уязвимостей широкого охвата

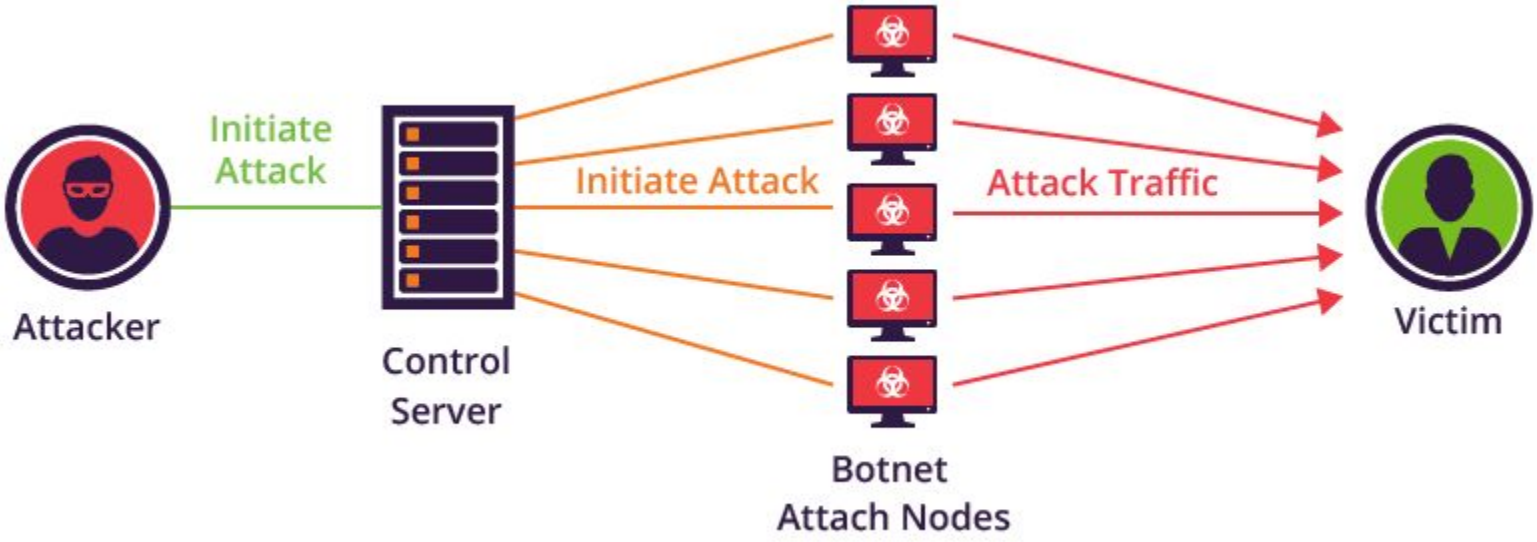
- Действие по сценарию
  - Сценарий может быть нетривиальным
- Отсутствие “человеческого” принятия решения
  - Действие строго по плану
- Низкий порог срыва атаки
  - Время - ценный ресурс для подобных систем

Отказ в обслуживании

Распределенный отказ в обслуживании

- Distributed Denial of Service
- Хакерская атака на компьютерную систему, имеющая целью исчерпание ресурсов жертвы
  - Добросовестные пользователи не смогут получить доступ к системе
- Может включать в себя эксплуатацию возможных уязвимостей

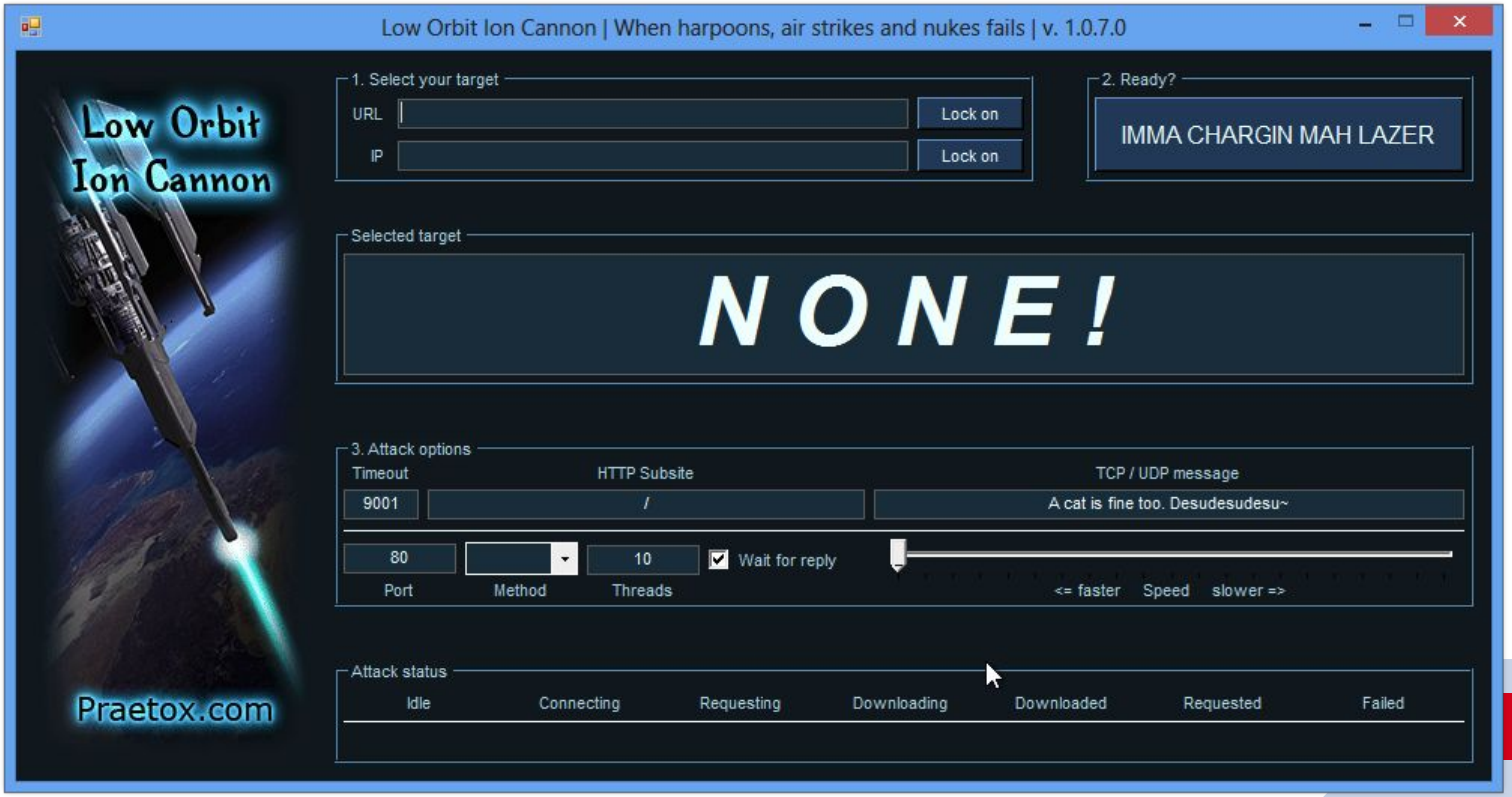
Распределенный отказ в обслуживании



Цели атаки

- Месть\развлечение
- Недобросовестная конкуренция
- Вымогательство
  - Выполнение определенных требований
  - Плата за остановку атаки
- Протест

DDOS как протест



“Цифровая травля”

- Реализация DDOS против человека
  - Программные телефонные звонки
  - Рассылка сообщений SMS и т.п.
  - Спам-атака на электронную почту
- Месть, шантаж, лишения доступа к привычным средствам связи

“Посредник”

Атака посредника

- Man in the Middle - “Человек посередине”
- Угроза, основанная на внедрении злоумышленника в цепочку передачи данных
  - Может быть пассивным и активным
- Многие среды передачи данных допускают MitM по своей природе
  - Радиоэфир один для всех

WiFi как среда передачи данных

- Одна из популярнейших технологий беспроводной передачи данных
- Представлена широчайшим спектром оборудования для организации сетей
- Настройка технологии обычно автоматизирована и имеет крайне низкий порог вхождения

Распространение сигнала

WiFi как небезопасная среда

- Ложная точка доступа
  - Большинство устройств настроено автоматически подключаться к знакомым сетям
  - Злоумышленник создает сеть с таким же именем
  - Весь сетевой трафик жертвы проходит через злоумышленника

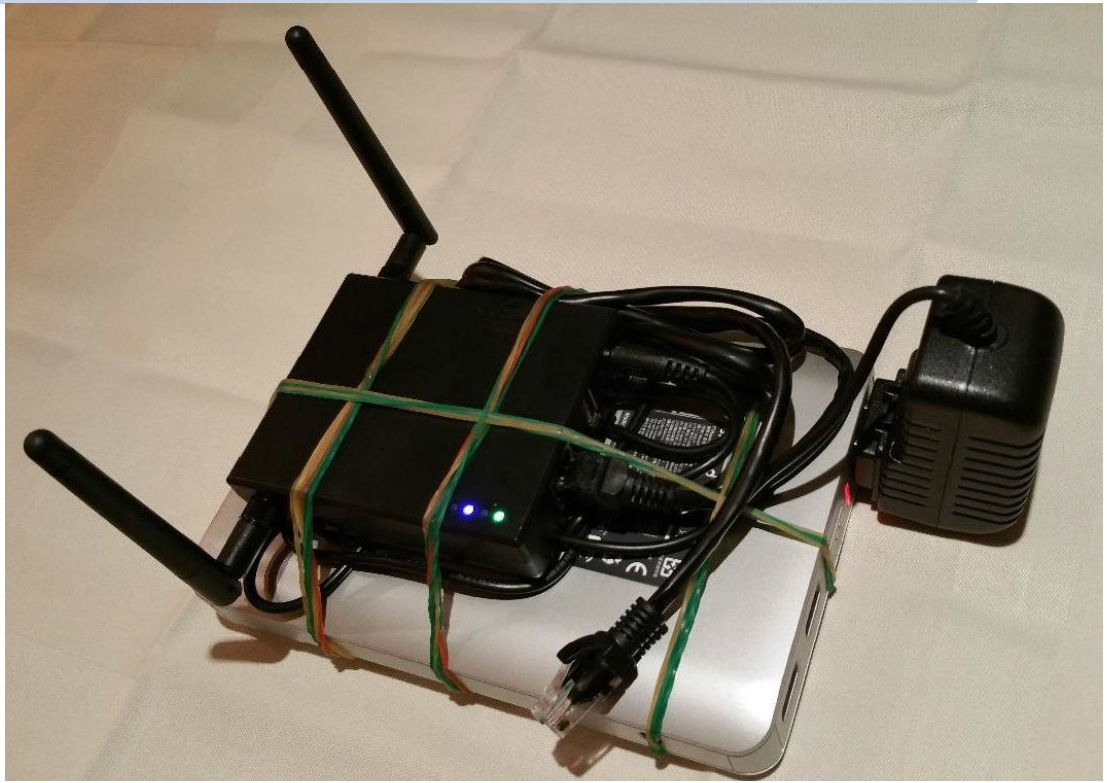
WiFi как среда передачи данных

- Ложная точка доступа может подавлять настоящую, переключать клиентов с реальной точки на ложную
- Анализ передаваемых данных
  - Кража паролей, учетных и т.п.
- Модификация трафика
  - Реклама, вирусы в скачиваемых файлах
- Прямые атаки на устройство клиента

Мобильные точки доступа

- В рамках бюджета в 5-6 тыс. рублей доступны как самодельные, так и промышленно изготовленные решения
- Решения могут иметь 4G-модемы для предоставления доступа в интернет
- Большинство сопутствующего ПО распространяется свободно

Самодельная автономная точка доступа



Эксперименты

- Компания Avast в рамках Mobile World Congress 2016 реализовала эксперимент
  - В аэропорту г. Барселона было развернуто несколько фальшивых WiFi-точек доступа с именами “AirportFreeWIFI”, “Starbucks” и т.п.
- За 4 часа перехвачено 8 миллионов пакетов от более чем двух тысяч пользователей

Эксперименты

- В рамках “некоей” конференции по ИБ была развернута фальшивая WiFi-точка
- Точка была снабжена широчайшим набором автоматизированных средств анализа трафика
- Перехвачено большое количество паролей от электронной почты и iCloud

Большие Данные и Большой Брат

Синьцзян-Уйгурский автономный район

СУАР

- Регион, пребывающий в состоянии перманентной контртеррористической операции
- Драйвер развития китайских(и мировых) технических средств наблюдения и контроля за обеспечением безопасности

Тотальный контроль

- В ходе осложнения ситуации в СУАР было принято решение перевести регион в режим полного и тотального контроля
- Комбинация человеческих и технических ресурсов
  - Традиционные полицейские меры
  - Меры, основанные на данных

Оценка задач

- Все виды коммуникаций с применением сети Интернет
  - Текст, голос, видео
  - Традиционные мессенджеры, игровые чаты и т.п.
- Огромный массив материалов, получаемых с видеокамер и прочих источников


© Alexander Belenkiy | macos.livejournal.com | www.macos.ms

Работа с видеопотоком

- Распознавание образов становится приоритетным направлением
  - Лица, автомобильные номера
- Видеокамера становится главным рабочим инструментом в обеспечении порядка
  - В определенные периоды большая часть видеокамер в КНР была установлена в СУАР

Первые успехи

- Массовое открытие профильных R&D-центров в СУАР
- Огромные инвестиции как в добычу данных, так и в обработку
- Регион превращен в гигантский тестовый полигон профильных технологий
- Время реакции полиции на преступления сокращено до 2-3 минут


SUV
非机动车
白色
轿车
黑色
轿车
灰色
轿车
白色
轿车
成人
长裤
男
上身蓝色
下身深蓝色
灰色
面包车
红色
轿车
成人
短袖
非机动车
裤
女
上身灰色
下身黑色
非机动车
非机动车
成人
短袖
长裤
男
上身灰色
下身灰色
非机动车
轿车
津BZ2697

Масштабирование

- в 2016 году в КНР было зарегистрировано 176 миллионов видеокамер
  - План подразумевает установку более четырехсот миллионов камер к 2020 год
- Минимум четыре человека стали миллиардерами благодаря росту рынка видеонаблюдения

Применение достижений микроэлектроники

Аппетит приходит во время еды

- К 2020 году система распознавания сможет за 3 секунды узнать в лицо любого гражданина КНР
- Распространение технологий биометрической идентификации
- Вычислительные и алгоритмические возможности для анализа всего массива информации

Социальный рейтинг

- “Система социальных кредитов”
- Система оценки поведения гражданина
- Баллы начисляются за общественно полезные дела и снимаются за общественно неприемлемые
- Используется максимально возможный массив информации

“Хороший гражданин”

- Получает скидки на кредитные и страховые продукты
- Арендует авто без депозита
- Скидки на коммунальные услуги
- Продвижение на сайтах знакомств

“Плохой гражданин”

- Отказ в выездных документах
- Отказ в доступе к самолетному и железнодорожному сообщению
- Невозможность пройти конкурс на государственную должность
- Отчисление из учебных заведений