«Эффективная оценка защищенности распределенной информационной системы»

Алексей Качалин

ЗАО «Перспективный мониторинг»

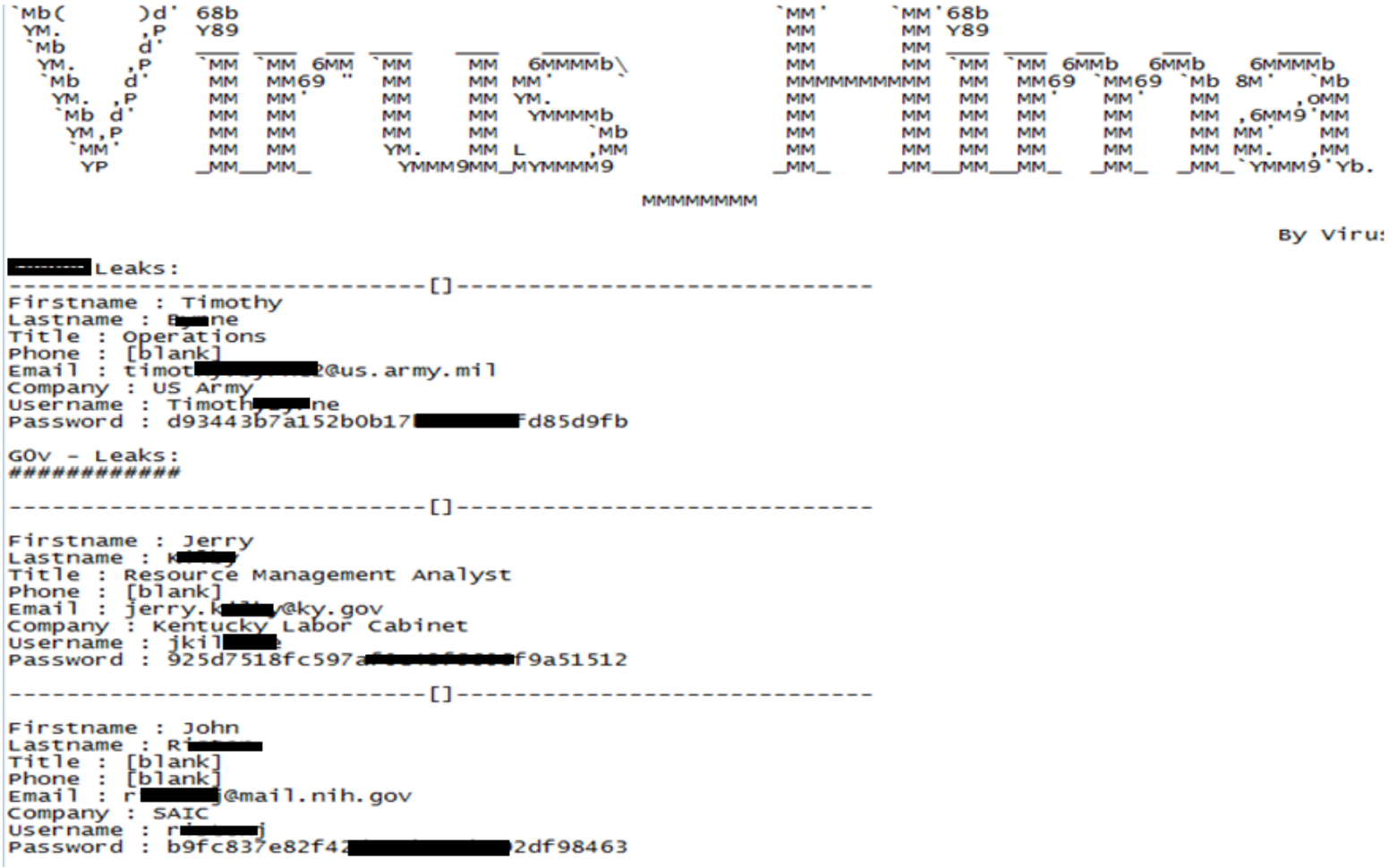
О компании

- Специализация:
  - Исследовательские работы в области ИБ
  - Инструментальный анализ ИБ, методы и средства атак на информационные системы
- Услуги ЗАО «ПМ»
  - Инструментальный анализ ИБ, тесты на проникновение
  - Анализ продуктов (ПО, ПАК)
  - Расследование инцидентов

«Стандартный» сценарий работ

- Ограничения по срокам – в течение года, следующий год
- Информационная система (ИС)
  - Распределенная, разнородная
  - Содержит ~~архаичное~~ необходимое ~~самописное~~ удобное для БП ПО
  - Дублирующие компоненты и ресурсы
- Текущее состояние ИС – неизвестно
  - Нет консистентного описания
  - Инкрементальные описания – не полны
  - Интервьюирование решает часть проблем
- Профиль угроз – не полон
- Внедрены системы контроля ИБ. Эффективность – неизвестна
- Потребность в работах
  - Требования регулятора
  - Инциденты
  - **Отсутствие ощущения безопасности**

Инциденты случаются



Предпосылки «тревожности»

- Неизвестен профиль угроз, отсутствие целостной информации
  - Подозрение на альтернативные/теневые БП
  - Заказное ПО
  - Географически-распределенные ИС с различным уровнем обеспечения ИБ
  - Облачные сервисы, сопряжение облака и «классической» инфраструктуры
  - Мобильные устройства и BYOD
- Динамика – сотрудники, клиенты, партнеры, реорганизация
- Необходимость доверять – например разработчик заказного ПО
  - Располагает вашей интеллектуальной собственностью, конфиденциальной информацией
  - Обладает доступом (доверием) на ресурсах (ИБ) вашей ИС
  - Интегрирован в вашу ИС, обладает возможностью модификации компонентов вашей ИС

Ок! Быстро делаем … что?

- Соответствие требованиям регулятора
  - Есть практика, требования
- Управление рисками
  - Процесс внедрение системы
- Анализ и противодействие актуальным угрозам (2012top10 и т.д.)
- Первичный анализ
  - Новый компонент/технология ИС
  - Объединение ИС

Первый шаг – границы исследования

- Ограничения по времени
- Ограничения по объектам исследований
  - Когда? (всегда кроме, в выделенное время, никогда→стенд)
  - Какие объекты не трогать
- Объем и порядок привлечения специалистов Заказчика
  - Интервьюирование
  - Сопровождение работ
  - Ревью/экспертная оценка результатов

Необходимо согласование и координации исследования со стороны Заказчика → нужен язык общения

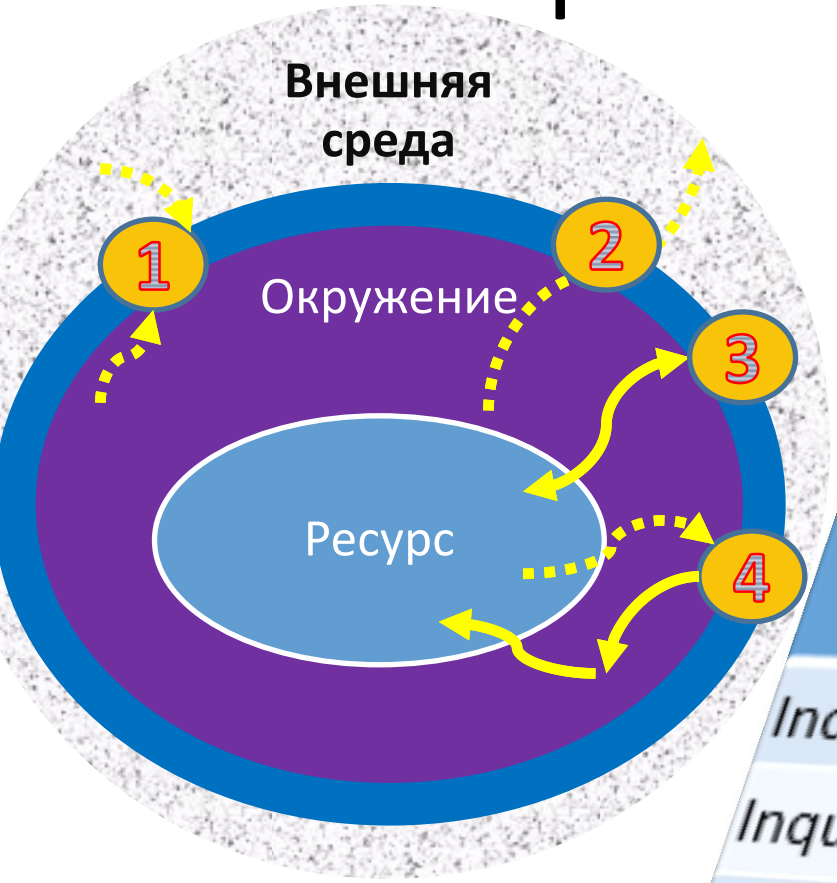
Потребность в модели

- Цели использования моделей в ходе исследования
  - Снизить зависимость описания методики от технологий
  - Разговор на одном языке исследователей, аналитиков, специалистов ИТ, специалистов по ИБ, менеджмента
  - Верификация и улучшение методик
- Объект исследования может быть описан в виде:
  - Ресурсов и возможностей взаимодействия
  - Каналов взаимодействия: человек, физический доступ, беспроводной доступ, телеком, сети передачи данных
  - Уровень взаимодействия: видимость, доступ, доверие

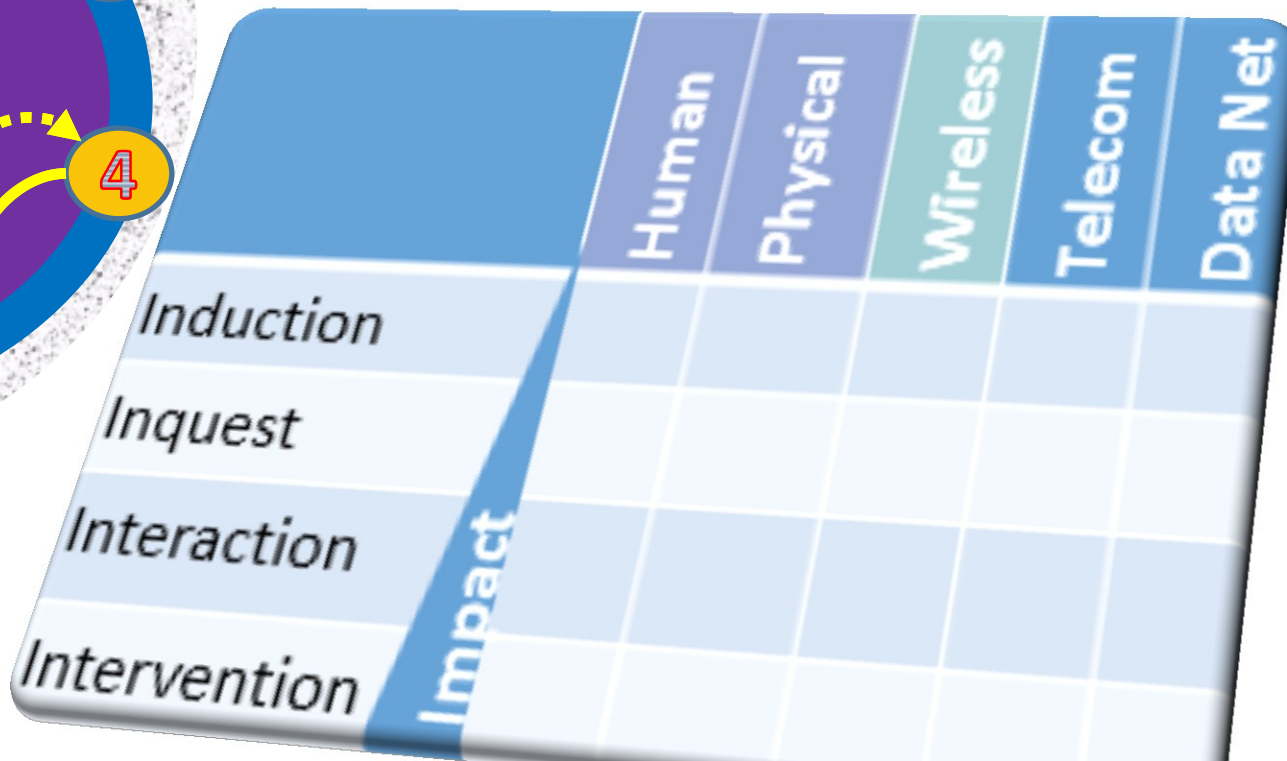
Пример модели анализа ИБ

- Контроль – **интерактивный, процессный**: идентификация/авторизация, подотчетность, достоверность,– конфиденциальность, целостность, доступность, неотказуемость
- Методы ограничения взаимодействия
  - Разделение – убрать/устранить ресурс
  - Устранить последствия угрозы
  - Устранить угрозу
- Количественная оценка контроля менее 100% - недостаточная, 100% - баланс, более 100% ИБ – избыточные
- Ограничения
  - Конфликты средств ИБ
  - Средства ИБ как ресурс ИС и возможность взаимодействия - дополнительные вектора атак

Планирование исследования



МетодыИсследования *
КаналыВзаимодействия →
Методики, Инструменты



По мотивам OSSTMM v3.0

Анализ угроз: ПО для мобильных устройств

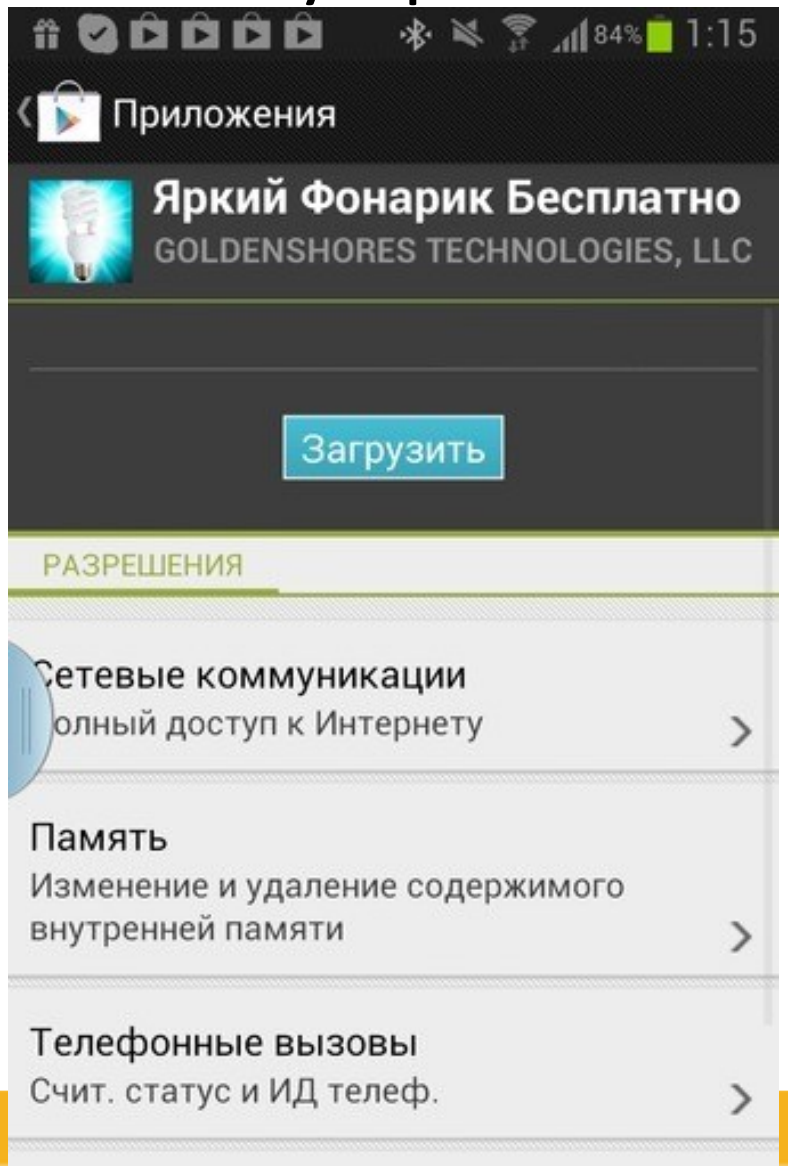
Функции ПО:

1. Включить светодиод

Запрашиваемы разрешения:

- Полный доступ к Интернет
- Полный доступ к памяти устройства
- Доступ к гео-позиционированию
- Полный доступ к истор звонков и СМС

Новинка!!!

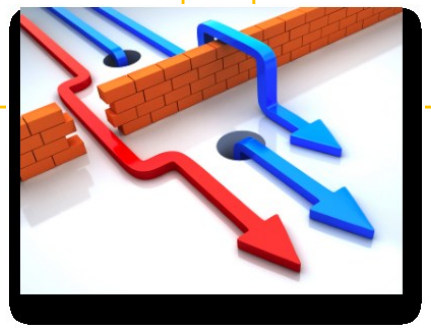


Скачиваний: более 1 000 000

Пример: систематизации векторов атак (human, physical)

- Japan
  - Mixi
- Korea
  - CyWorld
- Poland
  - Grono
  - Nasza-klasa
- Russia
  - Odnoklassniki
  - Vkontakte
- Sweden
  - LunarStorm
- UK
  - FriendsReunited et al
  - Badoo
  - FaceParty
- US
  - Classmates
  - Facebook
  - Friendster

- Physical Security
  - Building Security
    - Meeting Rooms
      - Check for active network jacks.
      - Check for any information in room.
    - Lobby
      - Check for active network jacks.
      - Does receptionist/guard leave lobby?
      - Accessbile printers? Print test page.
      - Obtain phone/personnel listing.
    - Communal Areas
      - Check for active network jacks.
      - Check for any information in room.
      - Listen for employee conversations.
    - Room Security
      - Resistance of lock to picking.
        - What type of locks are used in building?



Penetration Test Framework 0.59

Пример сценария – DDoS 2.0

«Низкоорбитальная Ионная Пушка»

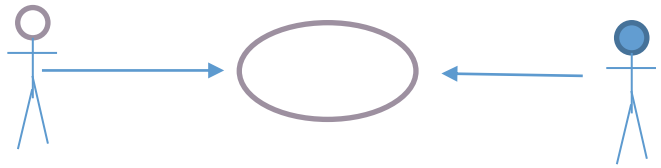
- Инструмент координации DDoS-атак на ИС правительства и гос. корпораций
- Сайт позволяет (добровольно) подключить компьютер посетителя к DDoS атаке
- Хостинг вне юрисдикции РФ

Владелец ресурса может без ведома активистов направить их ресурс на любую ИС

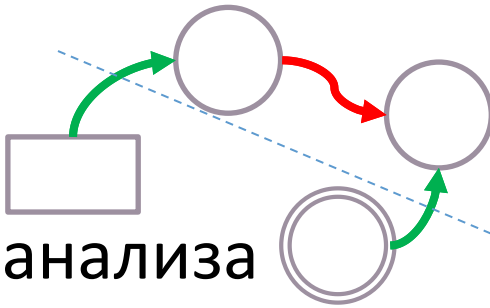
Типичные проблемы в ходе исследования

- Сбор информации
  - Предвзятое отношение: «Здесь проблем точно нет!»
  - Трудности перевода: «Наш ЕТС обеспечивает БРПС через ЗУД»
- «Подмена» исследования применением или внедрением инструмента
  - Сканер, система инвентаризации
- «Ограничения» исследователя
  - Вероятностный процесс – часть объектов исследования может быть недоступна в момент исследования
  - Возможность сопоставления информации от разных инструментов, отказ в пользу единого инструмента
- Реакция на исследование объектов – отключение
- Быстрая победа. Более сложные вектора остаются.

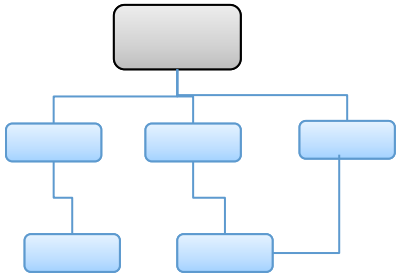
Аналитические инструменты



- Сценарии, MisUsecases
  - Рабочий инструмент аналитика – интервью, презентация результатов
- Диаграмма потоков данных (DFD)



  - Подход ориентирован на ПО
  - Возможность автоматизированного анализа
- Деревья атак/отказов (FTA)



  - Трассировка на причины и следствия

Мониторинг угроз и трендов

- «Классика» - уязвимости
  - Продукты
  - Сервисы
  - Библиотеки и компоненты
- Рост потенциального ущерб
  - Интеграция ИС в сети общего пользования
  - Штрафы и репутация
- Инновации в угрозах
  - Рынок blackhat-сервисов (0-day)
  - АСУ ТП (SCADA) вирусы
  - Advanced persistent threats (APT)
  - Хактивизм

Тренды ИБ
Information Security →
Information Assurance

IS Management →
IS Governance

Security →
Offensive security →
Information Security Intelligence

Представление результатов исследования

- Отчет – с учетом целей, методики, инструментов
  - Зафиксированы (уточнены) цели, границы, ограничения исследования
  - Несколько форм отчета, различающихся по детализации – для руководства, ИБ, ИТ
- Принятие ограничений результата– «из 2 зол»
  - Статус – «не определен» – приемлемый результат
  - Фиксация аномалий – отклонений в поведении, причины и последствия которых вне границ исследования
- Учет и управления динамикой
  - Анализ Было-Стало
  - План действий
  - План на следующую итерацию

Итого…

- Нет готового решения проблем ИБ в виде …

  (Продукта, Процесса, Шаблона, Стандарта, Рекомендованной практики)
- Методики исследования ИБ должна разрабатываться и обновляться с учетом динамики системы
- Проведение исследований и анализ результатов не возможно без аналитиков – в связи с наличием аномалий, ограничений наблюдаемости
- Нужен мониторинг актуальных угроз и трендов ИБ
  - Возможностей и ограничений средств защиты
  - Новых методов атак
  - Анализ инцидентов

Спасибо за внимание!

Алексей Качалин
kachalin@advancedmonitoring.ru
@kchln

info@advancedmonitoring.ru
http://advancedmonitoring.ru/
Twitter: @am_rnd