Направленные атаки социальной инженерии

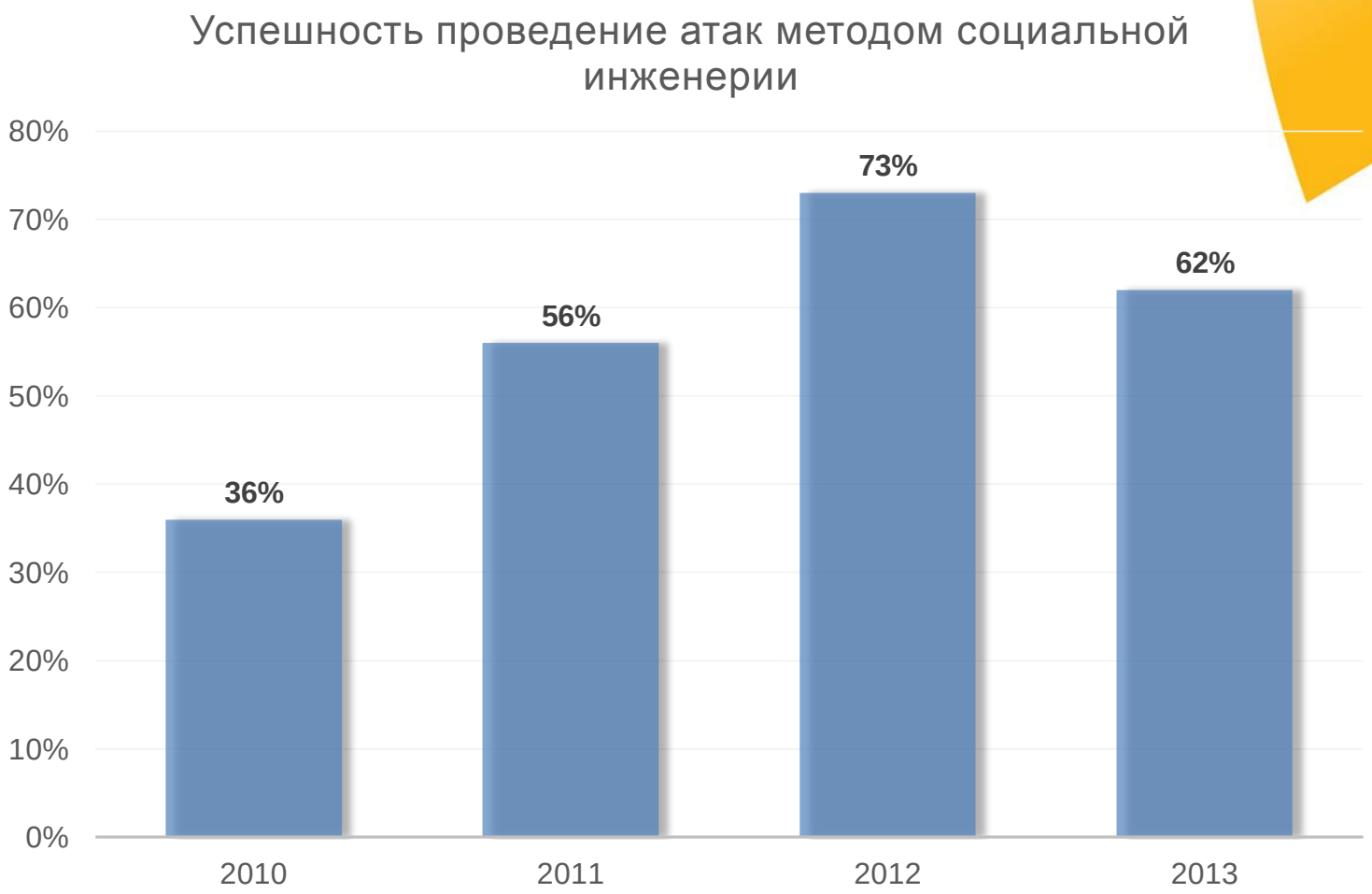
Юрий Омельяненко
Специалист отдела анализа защищенности

Социальная инженерия

- Слабое звено – человек
- Социальная инженерия – метод несанкционированного доступа к информации/системам хранения информации основанный на использовании слабостей человеческого фактора:
  - Любопытство
  - Страх
  - Беспечность
  - Желание помочь
- Социальная инженерия = обман

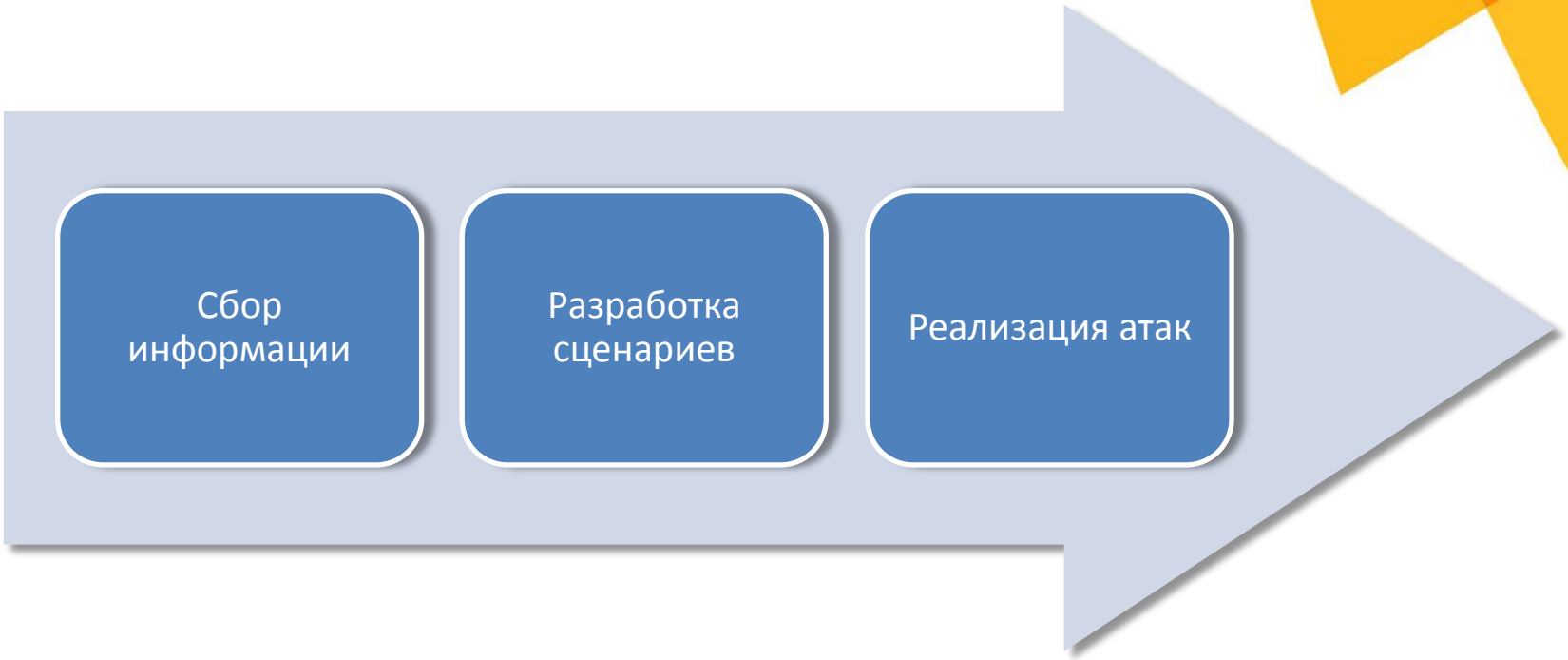
Информзащита
Системный интегратор

Статистика Информзащиты



Информзащита
Системный интегратор

Как это происходит?



Информзащита
Системный интегратор

Сбор информации: что искать ?

- Профиль индивидуума
  - Круг общения
  - Интересы, хобби
  - Публикации на форумах, блогах
  - Резюме

- Профиль компании
  - Деятельность на рынке
  - Партнеры
  - Общедоступная информация
    - Файлы на сайте
    - Список сотрудников
    - Адреса электронной почты, телефоны и др.

Информзащита
Системный интегратор

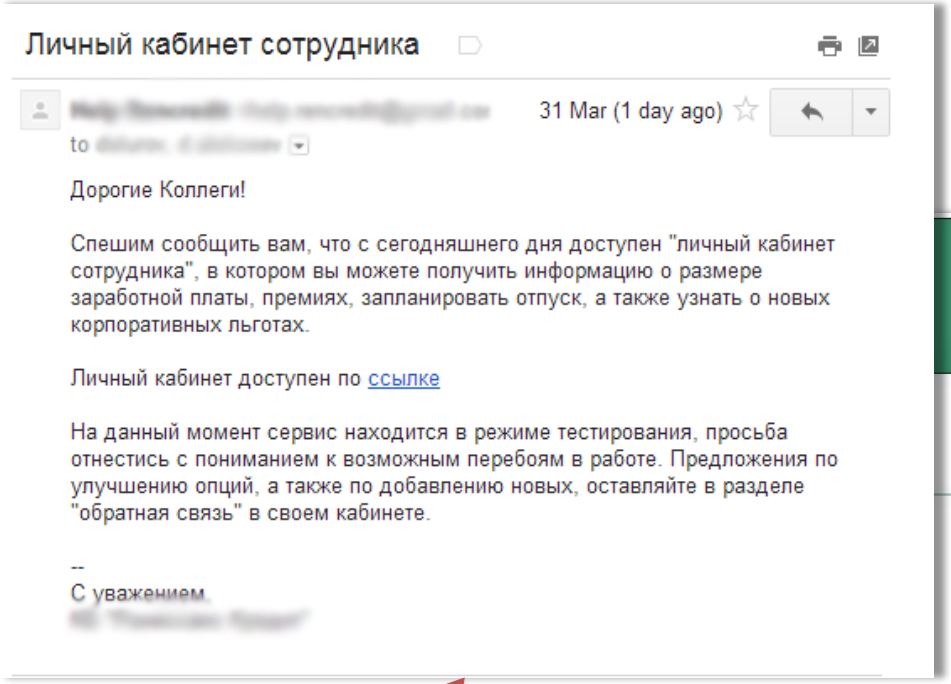
Разработка сценариев

- **Социальные сети** – формирование дружественных отношений
- **Почтовая рассылка** – реиндексация зарплат, web-интерфейс портала, настойчивая просьба
- **Физические носители** – потерянная флешка, посылка начальнику
- **Телефонная сеть** – техническая поддержка, забытый пароль, ограбленный клиент

Информзащита
Системный интегратор

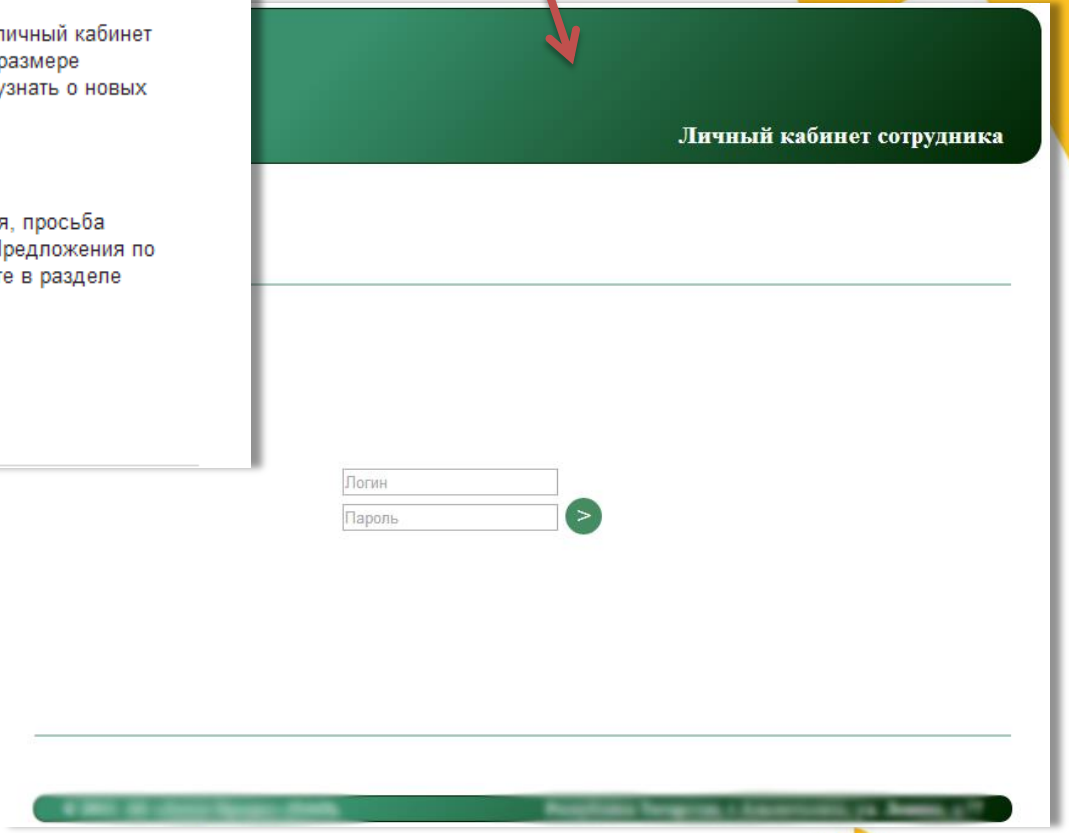
Информзащита
Системный интегратор

Пример реализации атаки



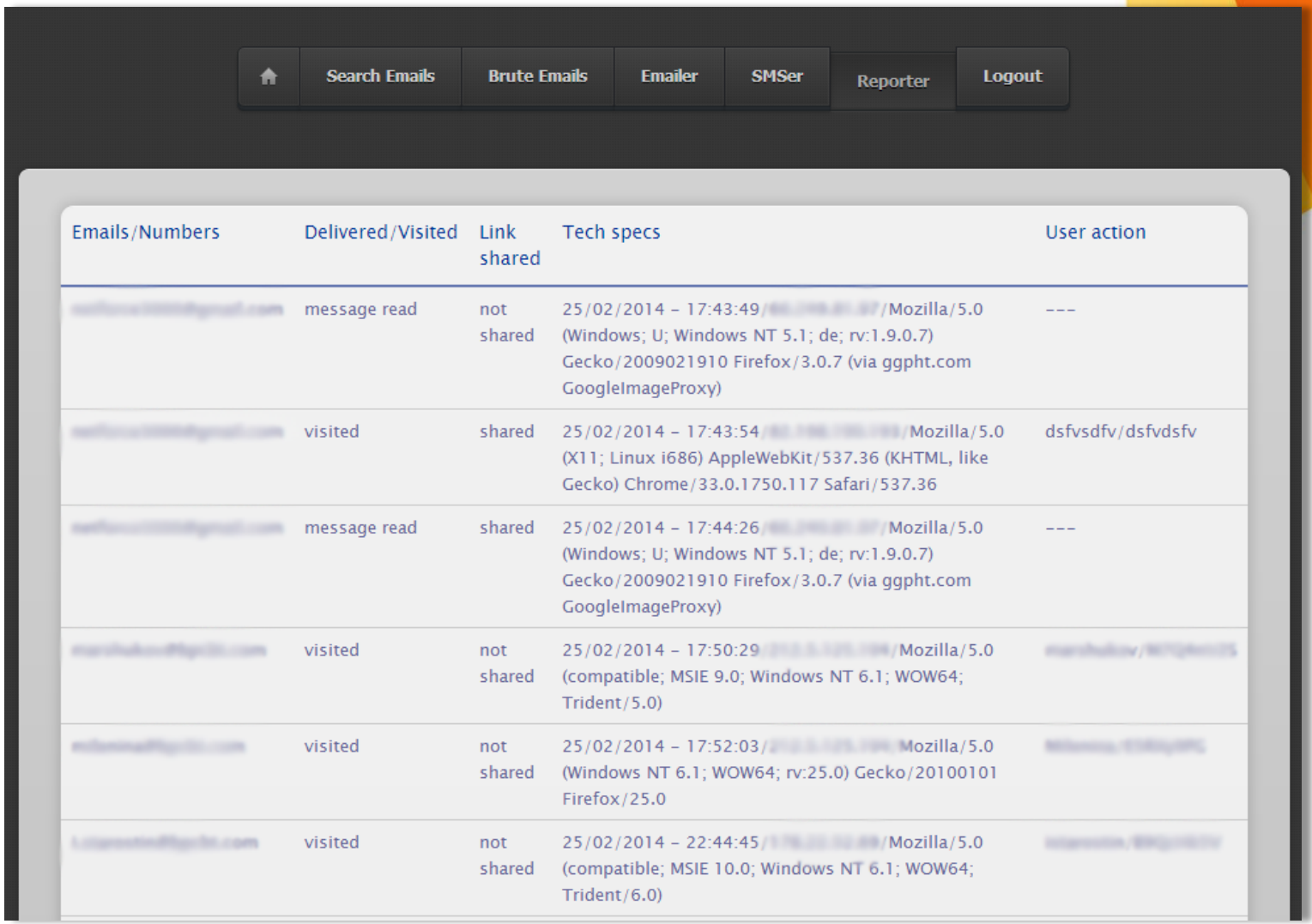
Письмо для массовой рассылки

Фишинговый сайт



Информзащита
Системный интегратор

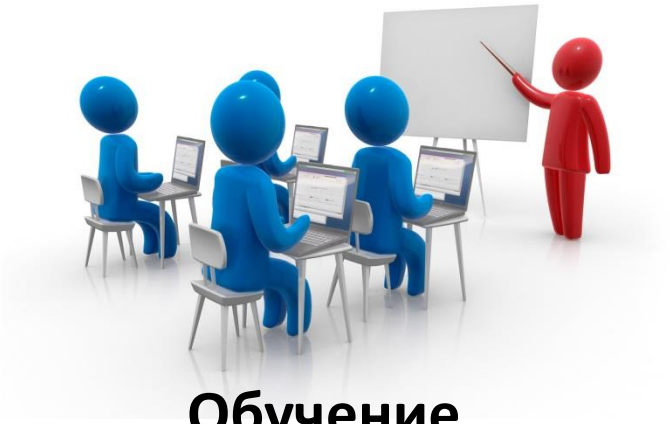
Результаты



Emails/Numbers	Delivered/Visited	Link shared	Tech specs	User action
[redacted]	message read	not shared	25/02/2014 – 17:43:49 [redacted] /Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7 (via ggpht.com GoogleImageProxy)	---
[redacted]	visited	shared	25/02/2014 – 17:43:54 [redacted] /Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.117 Safari/537.36	dsfvsdfv/dsfvdsfv
[redacted]	message read	shared	25/02/2014 – 17:44:26 [redacted] /Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7 (via ggpht.com GoogleImageProxy)	---
[redacted]	visited	not shared	25/02/2014 – 17:50:29 [redacted] /Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)	[redacted]
[redacted]	visited	not shared	25/02/2014 – 17:52:03 [redacted] /Mozilla/5.0 (Windows NT 6.1; WOW64; rv:25.0) Gecko/20100101 Firefox/25.0	[redacted]
[redacted]	visited	not shared	25/02/2014 – 22:44:45 [redacted] /Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)	[redacted]

Информзащита
Системный интегратор

Методы противодействия



Обучение

Отладка процессов

Тестирование

Разбор полетов

Информзащита
Системный интегратор

Повышение осведомлённости

- **Знать** > **уметь** > **выполнять**
- Разные формы обучения:
  - Ознакомление с документацией
  - Рассылки по e-mail
  - Плакаты/ заставки
  - Внутренние семинары
  - Внешнее обучение
- Контроль знаний
- Направленное обучение

Информзащита
Системный интегратор

Разделение обязанностей

- Снижает риск «человеческого фактора»
- Для намеренного выполнения неправомерного действия требуется сговор
- Деление ответственности (не всегда в пользу)
- Двойной контроль ≠ двойная работа

Информзащита
Системный интегратор

Тестирование и разбор полетов

- «Учебные тревоги»
- Тестирование на проникновение
- Плановое vs внезапное vs непрерывное
- Недостатки это хорошо (когда их нашли раньше злоумышленников)
- По результатам тестирования:
  - Доведение результатов до руководства с вариантами коррекции
  - Разбор полетов с сотрудниками
  - Коррекция внутренних контролей, процессов, программы обучения

Информзащита
Системный интегратор

Сухой остаток

- Любая система может быть взломана
- Системы защиты с каждым годом все совершеннее, сотрудники – неизменны.
- Самое слабое звено – человек, но можно максимально сократить риски:
  - Объяснив сотрудникам, что их могут обмануть и как
  - Внеся корректировки в существующие процессы
  - Проводя периодические тестирования и делая выводы из результатов
  - Лучшая проверка – независимая, максимально приближенная к реальности

Информзащита
Системный интегратор

ВОПРОСЫ?

Юрий Омельяненко
Специалист отдела анализа защищенности, CEH

y.omelyanenko@infosec.ru
+ 7 (495) 980-23-45 #685

Twitter: @netforce3000
www.infosec.ru

Информзащита
Системный интегратор

Полезные ссылки

Социальная инженерия:

- http://www.social-engineer.org

Обучение:

- http://itsecurity.ru
- http://itsecurity.ru/awareness/

Тестирование на проникновение:

- http://www.isecom.org/research/osstmm.html
- http://www.infosec.ru/katalog/bezopasnost-it-infrastrukturyi/obespechenie-bezopasnosti-setevoy-infrastrukturyi

Информзащита
Системный интегратор