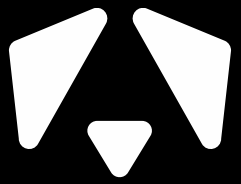


ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Социальная инженерия на практике

Проектный опыт ЗАО «ПМ»

Новиченко Александр

Деятельность ЗАО «ПМ»

Мониторинг инцидентов ИБ

Тестирование на проникновение

Анализ защищённости ПО

Разработка ПО

Расследование инцидентов ИБ

OSINT & SE

Что такое социальная инженерия?

Социальная инженерия (СИ) / Social engineering (SE)

Определение: совокупность приёмов, методов и технологий формирования условий и обстоятельств, которые максимально эффективно приводят к необходимому результату с использованием социологии и психологии.

Социальная инженерия в контексте информационной безопасности — использование человеческого фактора с целью нарушения информационной безопасности системы.

Связанные области: HUMINT, OSINT, тестирование на проникновение, продажи, маркетинг, противоправная деятельность.

Базовая идея

**Понимаем,
как люди думают**

**Ломаем не систему,
а человека**

Физическая безопасность и социальная инженерия

Цель: аудит физической защищённости

Мероприятия:

- Экспертная оценка нормативных и методических документов (план повышения защищённости объекта, паспорт антитеррористической защищённости и т.п.)
- Анализ контроля доступа и внутренних правил
- Аудит технических средств (систем контроля и управления доступом, видеонаблюдения, периметральной охраны и сигнализации)
- Аудит физической охраны объектов

Физическая безопасность и социальная инженерия

Максимальные размеры заготовки (ДхШхВ)	420x280x120 мм
Максимальный угол наклона проволоки (в зависимости от толщины заготовки)	14…30 градусов
Диапазон диаметров применяемой проволоки	0.05….0.3 мм
Точность координатных перемещений по осям X и Y	±1.5 мкм

Образцы наших изделий:

Более подробную информацию об услугах, профессиональные консультации можно получить специалистов по телефону:

Экономическая безопасность и социальная инженерия

Цель: противодействие мошеннической деятельности

Методология: симуляция действий злоумышленника / жертвы

Приёмы:

- Обман
- Обман
- Обман

Мероприятия:

- Контрольная закупка
- Контрольная поставка
- Тайный покупатель

Цель: получение конкурентного преимущества

Методология: конкурентная разведка

Информационная безопасность и социальная инженерия

Аудит информационной безопасности:

- Проверка возможности получения доступа к конфиденциальной информации
- Проверка возможности получения доступа к информационным системам (в том числе, физического)
- Проверка эффективности работы IDS/IPS, DLP и прочих СЗИ
- Проверка работы служб информационной и внутренней безопасности
- Проверка осведомлённости сотрудников в вопросах ИБ

Договорные и юридические аспекты СИ

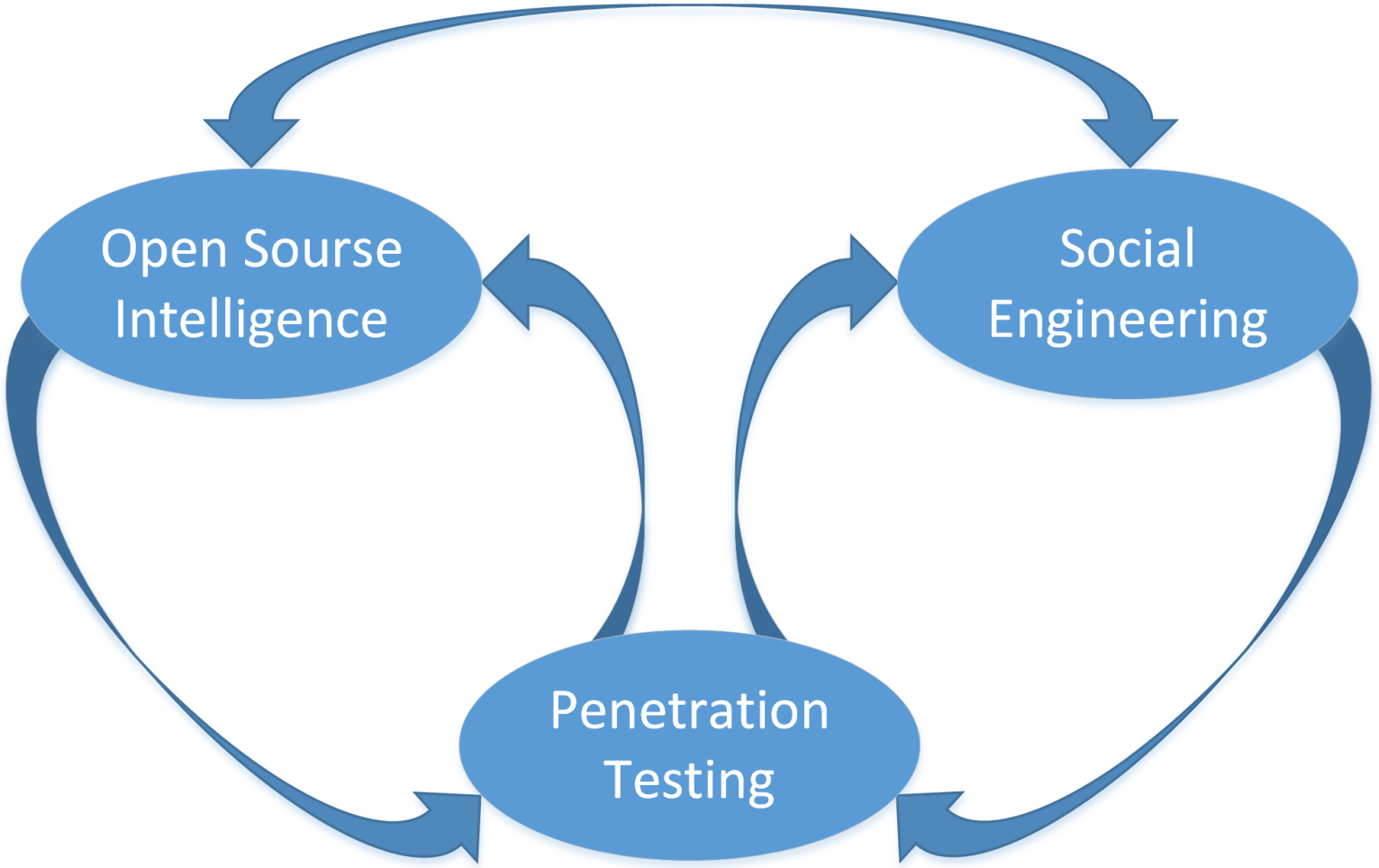
Rules of engagement и scope of work

- Цели СИ-исследования
- Используемые типы атак
- Категории сотрудников
- Время проведения работ

Правовые аспекты

- Нарушение Rules of engagement
- Нарушение прав третьих лиц
- Нарушение права на неприкосновенность частной жизни
- Обработка персональных данных

OSINT, Pentest, SE — лучшие друзья



OSINT

Мероприятия:

- Reconnaissance / Footprinting
- Enumeration
- Information Gathering

Приёмы:

- DNS-разведка
- Shodan, Censys, Google dorks и т.п.
- Поиск директорий / поддоменов
- Сетевое сканирование
- Поиск информации в социальных сетях, СМИ, на сайтах подбора персонала
- Поиск информации об утечках
- И т.д.

Результаты:

- Сведения об атакуемой инфраструктуре
- Конфиденциальная информация
- Потенциальные вектора для SE-атак

Pentest

Мероприятия:

- Enumeration & vulnerability analysis
- Weaponization & exploitation
- Post exploitation

Результаты:

- Вложения, зеркала сайтов и т.д.
- Конфиденциальная информация
- Потенциальные вектора для SE-атак

Social Engineering и гуманитарная составляющая

Психологические аспекты:

- Уверенность
- Знание контекста
- Обращение к авторитету
- Обращение к эмоциям
- Эксплуатация эмоций (страх, лень, жадность)
- Контроль внимания
- Заторапливание
- Сенсорная перегрузка
- Использование когнитивных искажений (феномен «дверь в лицо», феномен «нога в двери» и др.)

Социальная инженерия на практике

Методы:

- Создание вспомогательных материалов
- Претекстинг и легендирование
- Итеративный сбор информации
- Фишинг-рассылка
  - с целью сбора аутентификационных данных
  - с целью запуска вредоносных (или контрольных) вложений
- Спирфишинг
- Вишинг
- Кликджекинг
- “Road apple”
- Обратная социальная инженерия

Кейсы:

- Кейс 1 «Безответственный админ»
- Кейс 2 «Ненадёжный форум»
- Кейс 3 «Торговцы оружием»
- Кейс 4 «Массовая рассылка»
- Кейс 5 «Insurance, от слова Sure»
- Кейс 6 «Тысячи продавцов»

Кейс 1 «Безответственный админ»

Тип работ:

- Проверка осведомлённости сотрудников

Методы (SE):

- Претекстинг и легендирование
- Итеративный сбор информации
- Вишинг

Результаты:

- Получена информация для продолжения атаки (отсылки на НПА, название отдела, ФИО трёх уполномоченных сотрудников, IP-адрес)
- Не получена конфиденциальная информация

Кейс 2 «Ненадёжный форум»

Тип работ:

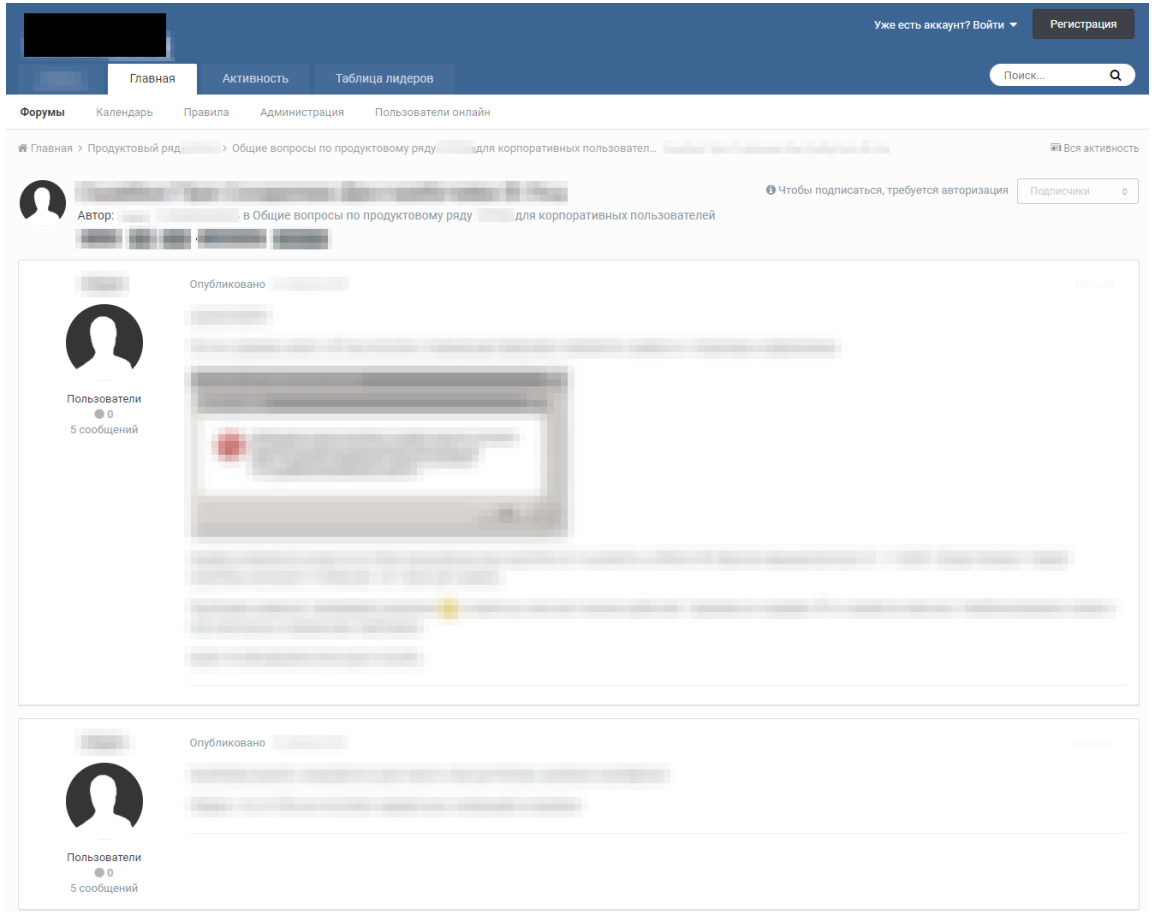
- Проверка осведомлённости сотрудников

Методы (SE + Pentest):

- Претекстинг и легендирование
- Создание вспомогательных материалов
- Кликджекинг

Результаты:

- Получен полный доступ к форуму
- Получен доступ к АРМ администратора форума



Кейс 3 «Торговцы оружием»

Тип работ:

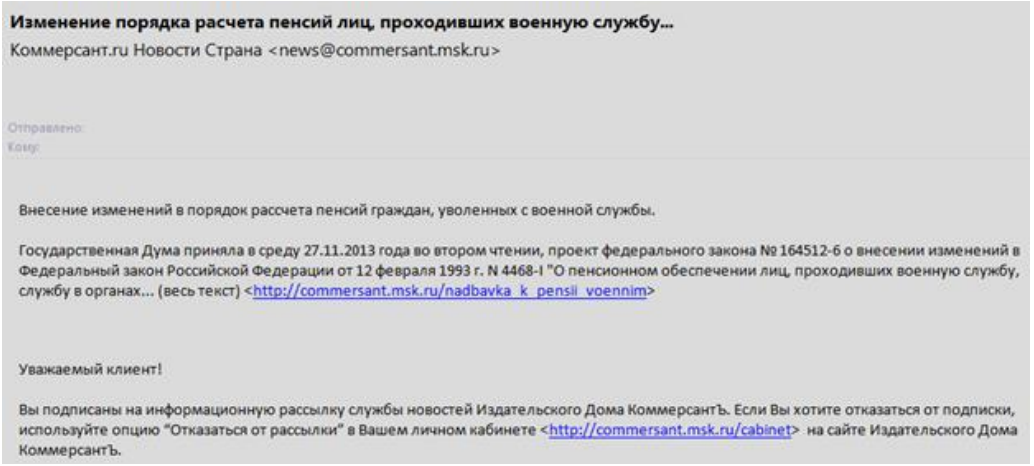
- Аудит защищённости ИС, проверка осведомлённости сотрудников, проверка работы службы ИБ Заказчика

Методы (SE + Pentest):

- Поиск и эксплуатация уязвимостей
- Создание вспомогательных материалов
- Спирфишинг
- Кликджекинг

Результаты:

- Из 44-х 17 адресатов активировали ссылку. Из них 3 попытались отказаться от вызвавшей недоверие рассылки, что также привело к активации вредоносного кода, а 14 активировали вредоносный код без попытки проверки или отказа.
- В результате атаки был получен доступ к АРМ и.о. генерального директора, АРМ ведущего бухгалтера, АРМ начальника управления, АРМ руководителя проекта
- Служба ИБ заказчика не обнаружила атаку



Изменение порядка расчета пенсий лиц, проходивших военную службу...

Коммерсант.ru Новости Страна <news@commersant.msk.ru>

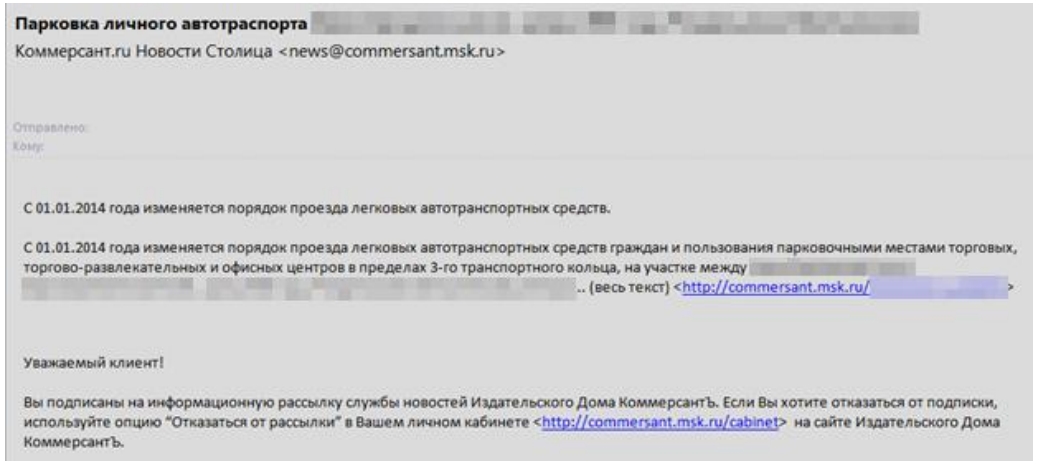
Отправлено:
Кому:

Внесение изменений в порядок рассчета пенсий граждан, уволенных с военной службы.

Государственная Дума приняла в среду 27.11.2013 года во втором чтении, проект федерального закона № 164512-6 о внесении изменений в Федеральный закон Российской Федерации от 12 февраля 1993 г. N 4468-I "О пенсионном обеспечении лиц, проходивших военную службу, службу в органах... (весь текст) <http://commersant.msk.ru/nadbavka_k_pensii_voennim>

Уважаемый клиент!

Вы подписаны на информационную рассылку службы новостей Издательского Дома КоммерсантЪ. Если Вы хотите отказаться от подписки, используйте опцию "Отказаться от рассылки" в Вашем личном кабинете <http://commersant.msk.ru/cabinet> на сайте Издательского Дома КоммерсантЪ.



Парковка личного автотраспорта

Коммерсант.ru Новости Столица <news@commersant.msk.ru>

Отправлено:
Кому:

С 01.01.2014 года изменяется порядок проезда легковых автотранспортных средств.

С 01.01.2014 года изменяется порядок проезда легковых автотранспортных средств граждан и пользования парковочными местами торговых, торгово-развлекательных и офисных центров в пределах 3-го транспортного кольца, на участке между ... (весь текст) <http://commersant.msk.ru/>

Уважаемый клиент!

Вы подписаны на информационную рассылку службы новостей Издательского Дома КоммерсантЪ. Если Вы хотите отказаться от подписки, используйте опцию "Отказаться от рассылки" в Вашем личном кабинете <http://commersant.msk.ru/cabinet> на сайте Издательского Дома КоммерсантЪ.

Кейс 4 «Массовая рассылка»

Тип работ:

- Проверка осведомлённости сотрудников

Методы (OSINT + Pentest + SE):

- Поиск информации в социальных сетях
- Создание вспомогательных материалов
- Фишинг

Результаты:

- LinkedIn-профили 190 сотрудников
- 51 e-mail адрес (указанный в профилях LinkedIn)
- 3500 e-mail адресов (некорректные настройки одного из серверов)
- 350 переходов по ссылке на опрос (из 1000)
- 50 попыток ввода валидных аутентификационных данных сотрудников

1.4 Описание проведенных работ

Работы по социальной инженерии проводились экспертами-исследователями в три этапа:

1. Поиск информации о Заказчике в открытых источниках. Был выполнен поиск информации о сотрудниках, их именах, должностях, адресах электронной почты, структуре компании; анализ отчетности, бухгалтерских документов, протоколов совещаний акционеров, публикаций в прессе и другой публичной информации. Список найденных файлов находится в Приложении А.
2. Поиск информации о выбранных сотрудниках Заказчика в социальных сетях, что позволило определить круг их увлечений, контакты, адреса и найти прочую информацию, которая может оказаться полезной злоумышленнику.

   В качестве углубленного исследования профилей сотрудников в социальных сетях, Заказчик предложил для анализа следующих сотрудников:

   - [ДАННЫЕ УДАЛЕНЫ], гл. специалист ОИТС
     Найдена в социальных сетях vkontakte.ru и odnoklassniki.ru.
   - [ДАННЫЕ УДАЛЕНЫ], секретарь директора по ИТ
     Найдена в социальной сети vkontakte.ru.
   - [ДАННЫЕ УДАЛЕНЫ], гл. специалист ОИТС
     В социальных сетях vkontakte.ru и odnoklassniki.ru не найдена.

   Также был осуществлен автоматический поиск профилей возможных сотрудников ОАО «[redacted]» на LinkedIn.
3. Рассылка письма со специально подготовленной ссылкой выбранной группе из 1000 сотрудников ОАО «[redacted]». Переход по ссылке фиксировался экспертом-исследователем с помощью специального ПО.

Кейс 4 «Массовая рассылка»

сотрудников ОАО «[redacted]», полный список профилей находится в Приложении Б.

Для углубленного анализа был выбран профиль сотрудника ОАО «[redacted]» [ДАННЫЕ УДАЛЕНЫ], главного специалиста ОИТС.

Сценарий использования – Злоумышленник находит профиль [ДАННЫЕ УДАЛЕНЫ] в социальной сети vkontakte.ru и получает информацию о ее увлечениях (ручная роспись по ткани, народные танцы, оригами), любимой музыке (Воскресенье, Pink Floyd, Nautilus Pompilius, Smokie), круге друзей и месте работы. Затем он готовит индивидуальное письмо для объекта исследования и предлагает принять участие в выставке оригами или конкурсе народных танцев. Заинтересовавшись письмом, [ДАННЫЕ УДАЛЕНЫ] переходит по ссылке либо открывает вложение к письму и заражает свой ПК вредоносной программой.

В случае неудачи, злоумышленник открывает раздел «Коллеги» в профиле [ДАННЫЕ УДАЛЕНЫ] и повторяет эту последовательность действий с другим сотрудником ОАО «[redacted]».

Атака по данному сценарию не была санкционирована Заказчиком и не проводилась.

С целью получения доступа или инсайдерской информации была осуществлена массовая

Кейс 5 «Insurance, от слова Sure»

Тип работ:

- Аудит защищённости ИС, проверка осведомлённости сотрудников

Методы (OSINT + SE + Pentest):

- Поиск информации в социальных сетях
- Создание вспомогательных материалов
- Фишинг
- Претекстинг и легендирование
- Вишинг

Результаты:

- Анализ 55 групп в социальной сети VK, в которых зарегистрированы сотрудники заказчика, позволил выявить 4 центра распространения информации

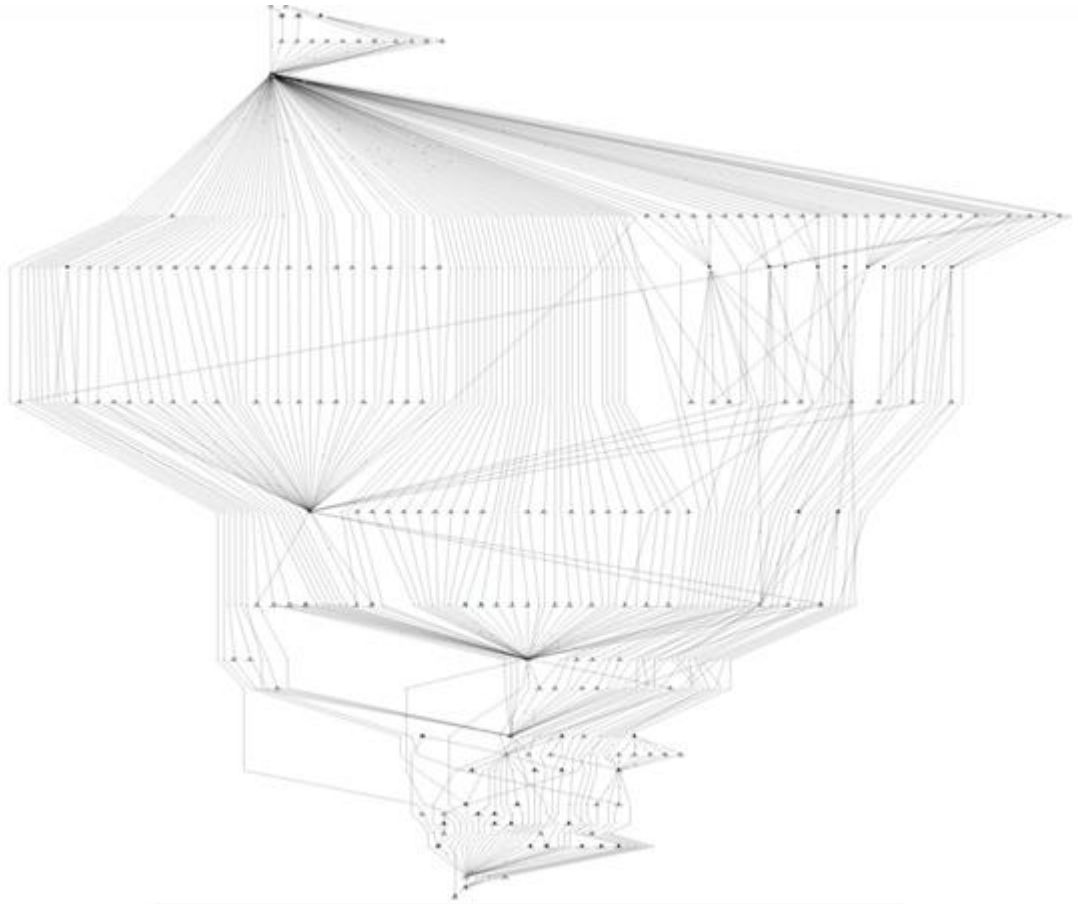


Рисунок 39 – Схематическое представление групп и связей

Кейс 5 «Insurance, от слова Sure»

Результаты фишинга:

- Из 100 адресов, участвовавших в первой рассылке, действительными оказались 64, из них 14 адресатов прочитали письмо и 10 из них попытались открыть приложенный документ.

- Из 177 адресов, участвовавших во второй рассылке, 70 оказались недействительными и на 2 адреса доставка не была произведена. Почту прочитали 18 пользователей, из которых 6 перешли по ссылке, а 4 ввели какие-либо данные в форму.

Кейс 5 «Insurance, от слова Sure»

Результаты вишинга:

- Было предложено 4 сценария проведения атаки, соответствующих 2-м моделям:

Модель	Сценарий
1. Звонок от лица внешнего субъекта	1.1 Злоумышленник от лица менеджера по персоналу некой компании звонит сотруднику компании Заказчика с целью получения информации о бывших сотрудниках.
	1.2 Злоумышленник звонит в компанию Заказчика с целью получения информации о состоянии здоровья застрахованного лица, представившись его родственником.
2. Звонок на мобильный сотрудника компании Заказчика от лица его коллеги	2.1 Злоумышленник звонит сотруднику с целью получения информации о других сотрудниках.
	2.2 Злоумышленник звонит сотруднику с целью получения учетных данных.

- Из 21 номера телефонов, выбранных для проведения атаки, на 7 номерах телефона не был получен ответ. На звонок ответили 14 сотрудников, среди которых 8 доверились злоумышленнику и 4 из них предоставили всю требуемую информацию.

Кейс 5 «Insurance, от слова Sure»

Город	Номер сценария	Результат
[ДАННЫЕ УДАЛЕНЫ]	1.1	Получена полная информация об уволившемся сотруднике: должность, оклад, состояние здоровья и семейное положение.
[ДАННЫЕ УДАЛЕНЫ]	1.1	Получен отказ
[ДАННЫЕ УДАЛЕНЫ]	1.1	Получена информации о должности уволившегося сотрудника. На просьбу огласить другие данные получен отказ.
Санкт-Петербург	1.1	Получен отказ
	1.1	Получен отказ
	1.2	Получен отказ
	2.2	Получен отказ
	2.2	Получена информация о дефолтном логине «[redacted]» и парольной политике (Первая буква заглавная, 6 символов в пароле, обязательно буквы и цифры, смена пароля необязательна).
Москва	1.1	Получен отказ
	1.1	Получена информация о должности уволившегося сотрудника
	2.1	Установлено доверительное общение с сотрудником компании Заказчика. Сотрудник не смог предоставить информацию, поскольку был не на рабочем месте.
	2.1	Получена контактная информация другого сотрудника
	2.2	Установлено доверительное общение с сотрудником компании Заказчика. Сотрудник готов был предоставить данные, но он не обладал нужной информацией.
	2.2	Получена информация о сотрудничестве с [redacted].

Кейс 6 «Тысячи продавцов»

Тип работ:

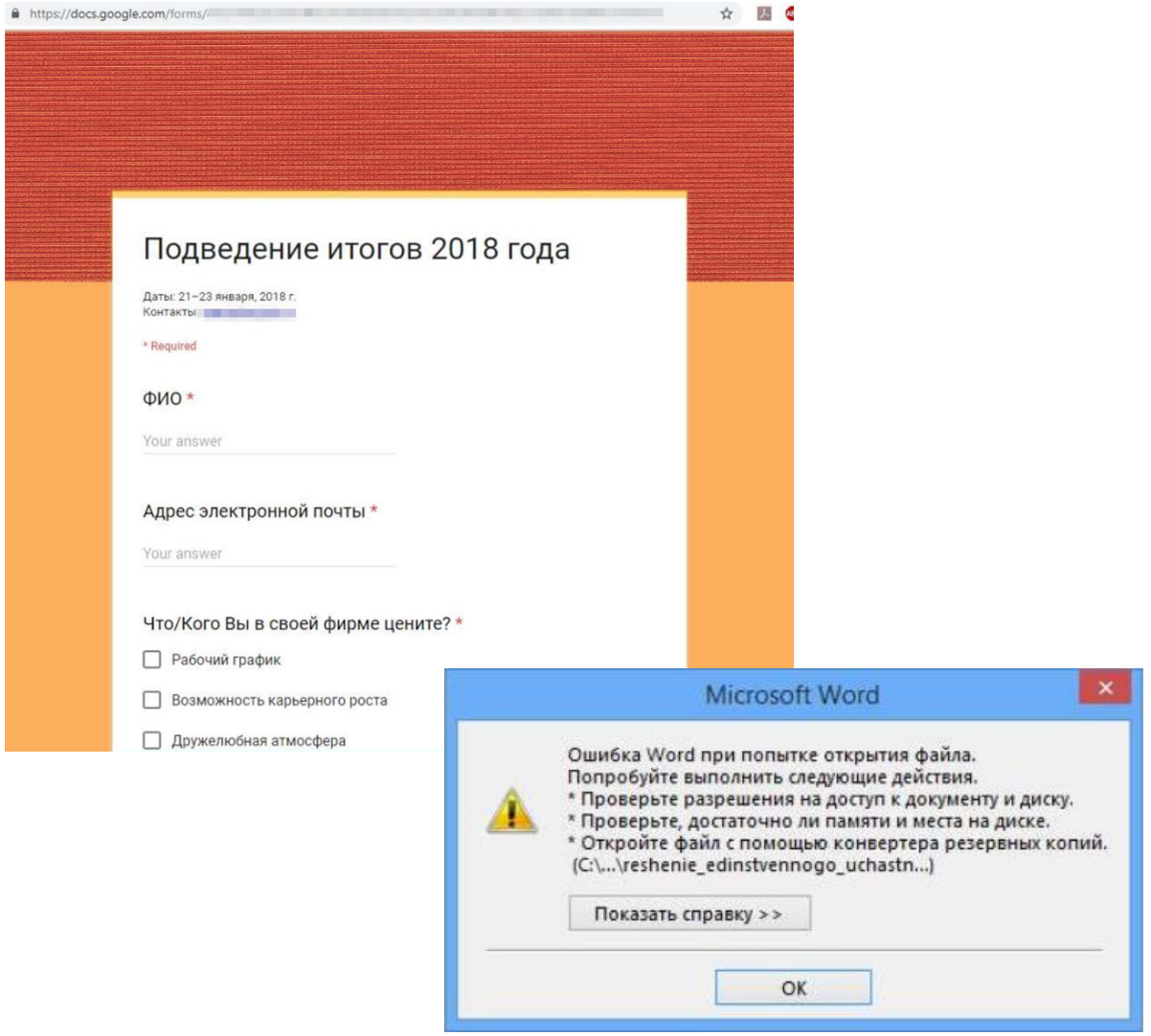
- Аудит защищённости ИС, проверка осведомлённости сотрудников

Методы (OSINT + SE + Pentest):

- Сетевое сканирование
- Создание вспомогательных материалов
- Фишинг

Результаты:

- В ходе анализа сетевой инфраструктуры Заказчика был обнаружен файл с 34 218 доменными логинами и должностями сотрудников (некорректные настройки одного из серверов)



Кейс 6 «Тысячи продавцов»

Результаты фишинга:

- Из 117 адресатов, участвовавших в первой рассылке, 33 открыли письмо. 26 перешли по ссылке и 15 ввели свои учетные данные в форму авторизации. Полученная в ходе фишинга информация позволила произвести подключение к почтовому серверу компании.

- Из 324 адресатов, участвовавших во второй рассылке, 50 прочли письмо и 29 открыли документ. При этом, количество попыток открыть документ составило 108. Т.е. после первой попытки у сотрудников не возникло подозрений в нелегитимности полученного письма, и попытки отрыть документ повторялись более 3-х раз.

Меры противодействия социальной инженерии

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо за внимание!

Новиченко Александр

специалист направления Open Source Intelligence

Alexandr.Novichenko@amonitoring.ru