



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Социальная инженерия на практике

Проектный опыт ЗАО «ПМ»

Новиченко Александр

Деятельность ЗАО «ПМ»



Мониторинг инцидентов ИБ



Разработка ПО

```
private $password;  
private $database;  
private $charset;  
static private $link = null;  
static public function connect()  
{  
    self::$link = mysql_connect(self::$host, self::$  
    if (!self::$link)  
        throw new MySQLException("Cannot connect to  
}
```

Тестирование на проникновение



Расследование инцидентов ИБ



Анализ защищённости ПО



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: [redacted]



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

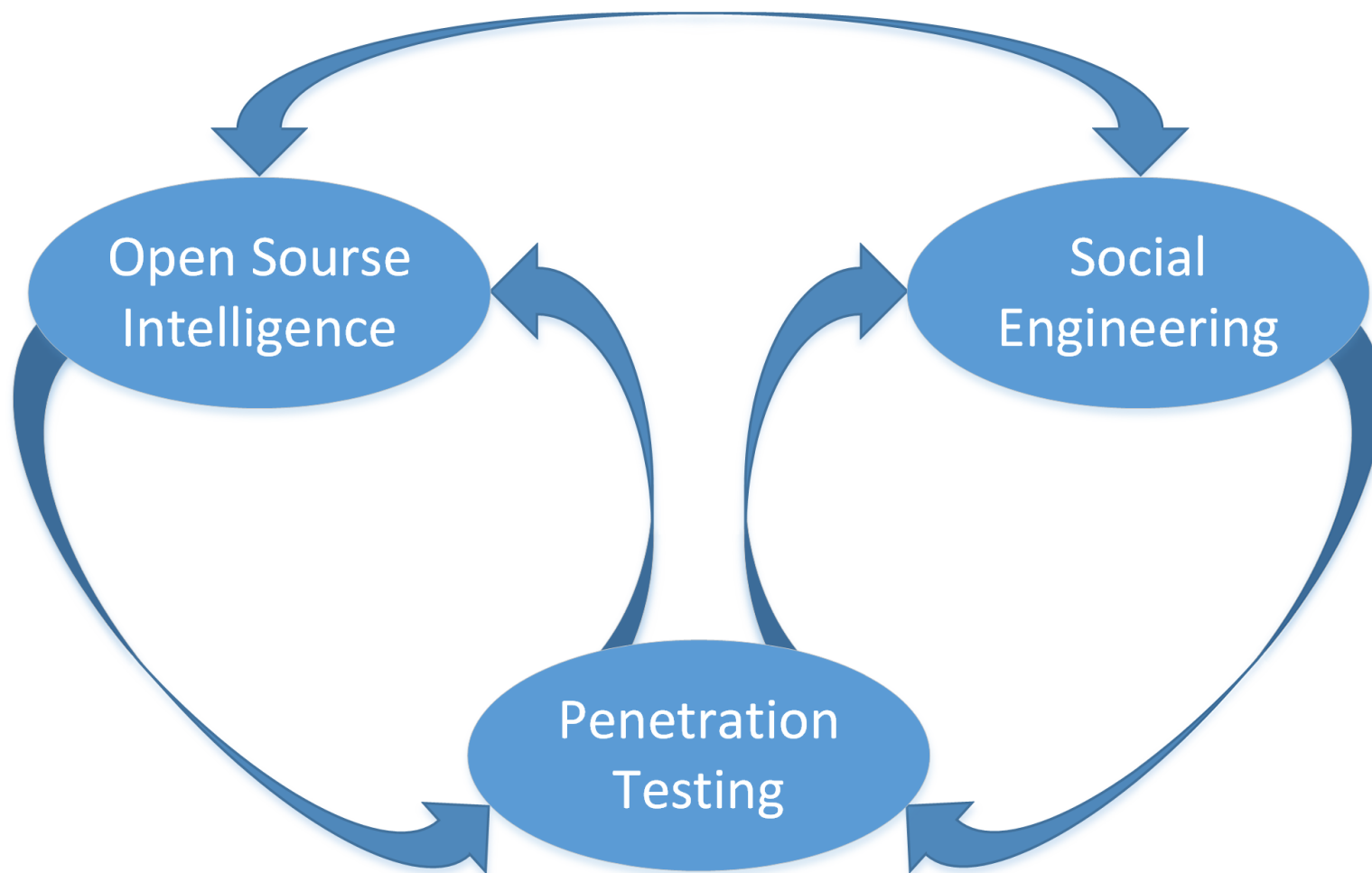
- Цели СИ-исследования
- Используемые типы атак
- Категории сотрудников
- Время проведения работ

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

| | | |
|--|---|--|
| <p>Разговор с [REDACTED] 1 (01.07.20) — Протокол</p> <p>[Олег [REDACTED]] Слушаю.</p> <p>[Максим Адашкин] Алло, здравствуйте. Олег [REDACTED] это?</p> <p>[Олег [REDACTED]] Да.</p> <p>[Максим Адашкин] Максим Адашкин, компания Инефотекс. Зовут Вас по имени-фамиле. В рамках программы информативности ОАО [REDACTED] в этом году мы проводим работу по оценке осведомлённости [REDACTED] и [REDACTED], в которые входит исследование безопасности эксплуатации [REDACTED] ОАО [REDACTED] и FTP-сервера АСУ [REDACTED]. Как Вам было сказано, к Вам можно обратиться с вопросом по администрированию этих систем?</p> <p>[Олег [REDACTED]] Вам давно да, FTP нет.</p> <p>[Максим Адашкин] Только по [REDACTED] А по администрированию FTP-сервера нет?</p> <p>[Олег [REDACTED]] Да.</p> <p>[Максим Адашкин] Хорошо. Что касается [REDACTED] По сути это соглашение с известными мне людьми [REDACTED] главным образом [REDACTED] и в основном начальство [REDACTED] вы хотели бы обратиться к вам с просьбой о помощи в проведении этого исследования.</p> <p>[Олег [REDACTED]] В какие сроки вы хотели проводить исследование?</p> <p>[Максим Адашкин] Это как раз один из тех вопросов, которые мы бы хотели согласовать. То есть исследование, насколько я знаю, будет проводиться три-то месяц, и вы хотели бы уточнить, когда Вам было бы удобно?</p> <p>[Олег [REDACTED]] Ну, наверное, лучше в августе. Я там иногда в отпуске. Наверное, лучше во второй половине августа.</p> <p>[Максим Адашкин] Во второй половине августа?</p> <p>[Олег [REDACTED]] Да.</p> <p>[Максим Адашкин] А Вам будут уточнять этот вопрос у руководства, но, наверное, это вас не устроит.</p> <p>[Максим Адашкин] Ещё один вопрос. Нет ли у Вас возможности предоставить нам документацию, регламентирующую работу с [REDACTED]?</p> <p>[Олег [REDACTED]] У меня её нет. Вы можете вкратце какую документацию? Инструкцию для своего персонала, если только. Это список правил, а что не подходит?</p> <p>[Максим Адашкин] Ну, например.</p> <p>[Олег [REDACTED]] Каким процедурам... Ну, если только. Я её запрошу, вам предоставят.</p> | <p>[Максим Адашкин] А можно узнать вашу электронную почту, для связи...</p> <p>[Олег [REDACTED]] Вконтакте или вконтрактное?</p> <p>[Максим Адашкин] Вконтакте.</p> <p>[Олег [REDACTED]] Лучше скажите адрес с [REDACTED]@mail.ru</p> <p>[Максим Адашкин] На неё писать, да?</p> <p>[Олег [REDACTED]] Да [REDACTED]@mail.ru</p> <p>[Максим Адашкин] Значит, кроме этой инструкции для своего персонала никаких регламентов нет.</p> <p>[Олег [REDACTED]] Нет.</p> <p>[Максим Адашкин] По приватке доступа к [REDACTED] ещё что-нибудь?</p> <p>[Олег [REDACTED]] Когда-то что-то разрабатывали когда-то, но у меня этого нет. Лет 10 назад.</p> <p>[Максим Адашкин] Может быть какие-то ссылки на подключение пользователей, перечень пользователей.</p> <p>[Олег [REDACTED]] Они же в интраворке все же.</p> <p>[Максим Адашкин] Может быть, есть какой-то регламент взаимодействия пользователей с системой...</p> <p>[Олег [REDACTED]] Нет, через "интраворку" подключаются, как и все, в общие ресурсы. Ну, есть общий портал, типа [REDACTED]. Вот в рамках него. Когда-то была такая организация, которая проводила какую-то сертификацию. Это [REDACTED] должен лучше знать. Задача там что-то "и", во, в общем, это [REDACTED] только лучше знать. Какого-то была организация, которая сертифицировала какое-то приложение. Там вот.</p> <p>[Максим Адашкин] Давай.</p> <p>[Олег [REDACTED]] Ну да, скажет так вам, я не знаю, шаровало вложить по-то и то-то, больше колосс не может быть, ну, и притому; а по тому правили, скажем, скажем, Ну, условия говоря. Или что-то ещё. Должны быть записи на IP-адреса, значит должны быть записи. Ну вот как бы. Я один раз это выполнял, дальше просто исполнял.</p> <p>[Максим Адашкин] Тогда...</p> <p>[Олег [REDACTED]] Такая работа... "шаровало"</p> <p>[Максим Адашкин] Тогда пока у меня вопросы больше нет. Они, наверное, появятся по тем практикам, которые в отпуске документацию привнесёте для объяснения безопасности. Но это пока. То что вы, наверное, могли бы мне ещё дополнительно помочь, это к кому обратиться по поводу безопасности FTP-сервера АСУ [REDACTED]</p> | <p>[Максим Адашкин] Хорошо, тогда и следующая с господином [REDACTED] уточню, что у вас может быть...</p> <p>[Олег [REDACTED]] Он эти все вопросы курирует.</p> <p>[Максим Адашкин] ... и я на ту почту, что вы предоставили, отправлю сообщение со своего адреса и тогда, если вы сможете выдать те документы, о которых мы говорили.</p> <p>[Олег [REDACTED]] Вряд ли. Нет. Я же пишу вам! Ну, он не может. Совершенно. Эти требования I и я слышал и с ней вы выполняете. Поэтому мне эти документы не очень нужны. Я скорее выполняю требования безопасности, нежели на разрабатываю.</p> <p>[Максим Адашкин] То есть даже для своего персонала вы не знаете, как получить информацию?</p> <p>[Олег [REDACTED]] Знаю, почему. Я же сказал...</p> <p>[Максим Адашкин] Тогда у [REDACTED]</p> <p>[Олег [REDACTED]] Я же сказал, что я её возму.</p> <p>[Максим Адашкин] То есть вы её сможете послать? Для своего.</p> <p>[Олег [REDACTED]] Да, я же сказал, что пошло. Я возму в производственном отделе и пошло. Я это уже сказал.</p> <p>[Максим Адашкин] Да, я просто начал говорить, что вы шаг адрес...</p> <p>[Олег [REDACTED]] А то, что по безопасности, это у [REDACTED] По вашим требованиям и в отпуске.</p> <p>[Максим Адашкин] У...</p> <p>[Олег [REDACTED]] Я же разрабатываю этого дела, там и править бы необходимо. Я могу проверить и сказать, тут исправлять, тут нормальное. Исправлю и всё.</p> <p>[Максим Адашкин] Хорошо, тогда и следующая с [REDACTED] и уточню у него этот вопрос...</p> <p>[Олег [REDACTED]] Ну да, скажет так вам, я не знаю, шаровало вложить по-то и то-то, больше колосс не может быть, ну, и притому; а по тому правили, скажем, скажем, Ну, условия говоря. Или что-то ещё. Должны быть записи на IP-адреса, значит должны быть записи. Ну вот как бы. Я один раз это выполнял, дальше просто исполнял.</p> <p>[Максим Адашкин] Тогда...</p> <p>[Олег [REDACTED]] Такая работа... "шаровало"</p> <p>[Максим Адашкин] Тогда пока у меня вопросы больше нет. Они, наверное, появятся по тем практикам, которые в отпуске документацию привнесёте для объяснения безопасности. Но это пока. То что вы, наверное, могли бы мне ещё дополнительно помочь, это к кому обратиться по поводу безопасности FTP-сервера АСУ [REDACTED]</p> |
| <p>[Олег [REDACTED]] Ну, вообще, насколько я знаю, с точки зрения вот самого сервера это отпад делов. Ну, установка оборудования, сопровождение самого оборудования. Я думаю, что это скорее всего сейчас.</p> <p>[Максим Адашкин] А что касается IP-адреса?</p> <p>[Олег [REDACTED]] Вас [REDACTED] опять же, неграмот. То есть я вижу же. Почему что... Вы из какой организации?</p> <p>[Максим Адашкин] Инефотекс.</p> <p>[Олег [REDACTED]] Ну, Инефотекс, по-моему, и разрабатывал все документы для сервера.</p> <p>[Максим Адашкин] Ох... Нас-то сейчас интересует, как осуществляется доступ пользователей, выделение заявок и так далее. Это тоже в отпуске?</p> <p>[Олег [REDACTED]] Это и нет, но, по-моему, Инефотекс, как раз и разрабатывал документацию, как это всё делать.</p> <p>[Максим Адашкин] К сожалению, знаю это кем-то, и не отдела душка.</p> <p>[Олег [REDACTED]] Я ещё раз говорю, соседний отдел, у вас же все в документах, как на серверах это всё организовано. Я серьёзно говорю, не смеюсь над вами. Это инфотексовская разработка.</p> <p>[Максим Адашкин] Я верю.</p> <p>[Олег [REDACTED]] У [REDACTED] отпуски, это также инфотексовская разработка. В соответствии с тем документом, который привал инфотекс, так они и выполняю.</p> <p>[Максим Адашкин] Хорошо, давай, тогда, наверное, на данный момент...</p> <p>[Олег [REDACTED]] Я вам не делую, что, как и кого узнавать, просто я помогу, что это Инефотекс разрабатывал и выдал.</p> <p>[Максим Адашкин] Я уточню этот вопрос, спасибо.</p> <p>[Олег [REDACTED]] Тут проще и быстрее может быть. Потому что документы по безопасности они же на инфотексовские.</p> <p>[Максим Адашкин] Давай, хорошо, спасибо, тогда до свидания.</p> <p>[Олег [REDACTED]] Где ты будешь вы уже сами решить.</p> <p>[Максим Адашкин] Да, конечно...</p> <p>[Олег [REDACTED]] Я просто для информации вам говорю, что инфотексовская разработка. Привести тогда инфотексовским. Но если окажется, что они исправлять, значит, соответственно, инфотексовским, будет с ними контактировать.</p> <p>[Максим Адашкин] Я уже, кто у вас имя замывался, если замывался, и...</p> <p>[Олег [REDACTED]] Ну, конечно, да. Да.</p> | <p>[Максим Адашкин] Ещё раз, большое спасибо...</p> <p>[Олег [REDACTED]] Пожалуйста. По поводу реальной работы, это не сейчас.</p> <p>[Максим Адашкин] А когда у вас будет время обсудить это более подробно?</p> <p>[Олег [REDACTED]] Давайте на следующей неделе. Вы можете позвонить, когда convenient сам, свои работы?</p> <p>[Максим Адашкин] Нет, свои работы у вас выполняю то, что наши исследователи будут предоставлять доступ к вашему серверу [REDACTED] насколько я знаю, там есть [REDACTED] и вот система [REDACTED]...</p> <p>[Олег [REDACTED]] Есть, да.</p> <p>[Максим Адашкин] Для этого вам на вашей стороне необходимо определить, кто будет заниматься исследованием. Или сделать чтобы предоставляли информацию коллеге о системе, организации, с тем, как происходит взаимодействие на практике. Договоритесь с вами, как как будет удобнее...</p> <p>[Олег [REDACTED]] Ну, понятно, что на рабочий сервер доступ будет свободный, поэтому я могу как prima dare, например, стараться только не включать там ничего другого.</p> <p>[Максим Адашкин] То есть я могу сделать подключение через VPN?</p> <p>[Олег [REDACTED]] Да, в принципе, да. Ну, можно не через VPN — это не ко вам, так как на инфоброке никакого доступа-ссылки нет, это всё на инфоброке, и на инфоброке отключено. Но, наверное, да. Это лучше всего же в соседнем отделе. У вас там вообще есть. По адрес и вам сразу, пожалуйста.</p> <p>[Максим Адашкин] Замкнуло.</p> <p>[Олег [REDACTED]] [REDACTED]</p> <p>[Максим Адашкин] Это реально? Да?</p> <p>[Олег [REDACTED]] Да.</p> <p>[Максим Адашкин] А идентификация как происходит?</p> <p>[Олег [REDACTED]] Ну, это мне всё-таки нужно, чтобы [REDACTED] подтвердил.</p> <p>[Максим Адашкин] Мне всёского словения.</p> <p>[Олег [REDACTED]] Чтобы что-то такое конкретное. С моей точки зрения, мы позволим любой IP, например, что все это будет доступ.</p> <p>[Максим Адашкин] Я же спрашиваю деловое.</p> <p>[Олег [REDACTED]] Но, в частности, даже если вы что-то хотите...</p> <p>[Максим Адашкин] Нет, вы не собираетесь читать...</p> | <p>[Олег [REDACTED]] Но мне шаровало — это тогда [REDACTED] Пусть распределяет доступ, на вопрос, даны ли какие-то сертификаты или сертификаты, с тем уровнем доступа, что вы сами определите, какой вам нужен.</p> <p>[Максим Адашкин] Мне всёского словения! У Андрея [REDACTED] вы надо будет и другие вопросы уточнить, так что я могу написать. Его контакты информации у вас есть?</p> <p>[Олег [REDACTED]] Угу. Единственно, что и могу сказать, вот, ограничение по дате на инфоброке, в принципе. И по дате парол, соответственно, тоже. Это чисто инфоброковская вещь. Такая система, дате не позволяет выдать дату.</p> <p>[Максим Адашкин] Я это отпишу.</p> <p>[Олег [REDACTED]] И первый список должен быть актуальным. В июне пользователи. Сменили ОС инфоброке. То есть такой организации, насколько я знаю... Чтобы вы не попали в замешательство, что как-то у вас [REDACTED] но, по-моему, не будет, потому что это технически невозможно. Просто сразу вам говорю, чтобы вы время не тратили.</p> <p>[Максим Адашкин] Понятно, хорошо. Давай, тогда, наверное, пока всё. До свидания.</p> <p>[Олег [REDACTED]] До свидания.</p> |



Кейс 2 «Ненадёжный форум»

Тип работ:

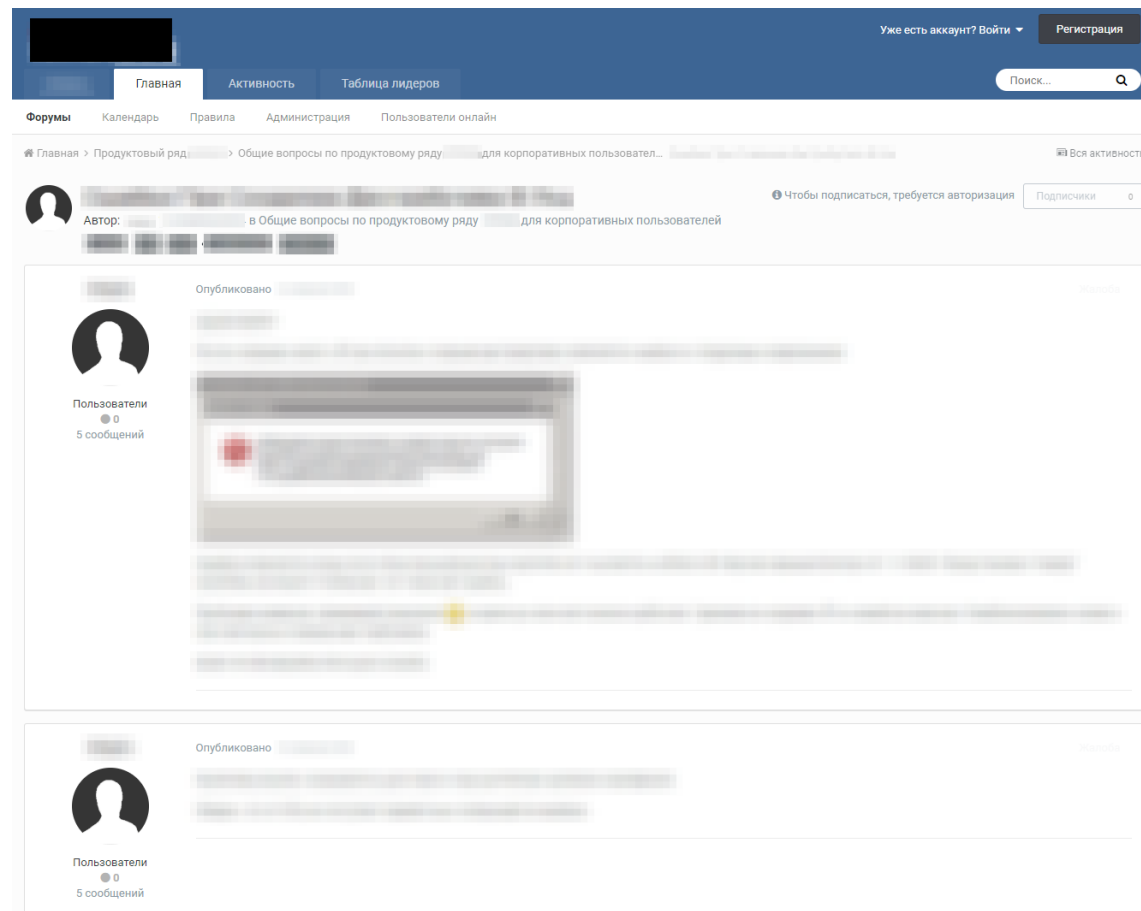
- Проверка осведомлённости сотрудников

Методы (SE + Pentest):

- Претекстинг и легендирование
- Создание вспомогательных материалов
- Клиқджекинг

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@commercant.msk.ru>

Отправлено:
Кому:

Внесение изменений в порядок расчета 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 4468-1 "О пенсионном обеспечении лиц, проходивших военную службу, службу в органах... (весь текст) <http://commercant.msk.ru/nadbavka_k_pensil_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://commercant.msk.ru/cabinet>> на сайте Издательского Дома Коммерсантъ.

Парковка личного автотранспорта

Коммерсант.ru Новости Столица <news@commercant.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://commercant.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://commercant.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:

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

Также был осуществлен автоматический поиск профилей возможных сотрудников ОАО «██████████» на LinkedIn.

3. Рассылка письма со специально подготовленной ссылкой выбранной группе из 1000 сотрудников ОАО «██████████». Переход по ссылке фиксировался экспертом-исследователем с помощью специального ПО.



Кейс 4 «Массовая рассылка»

сотрудников ОАО «██████████», чьи профили находятся в приложении 2.

Для углубленного анализа был выбран профиль сотрудника ОАО «██████████» [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 «██████████».

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

С целью получения доступа или иной важной 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

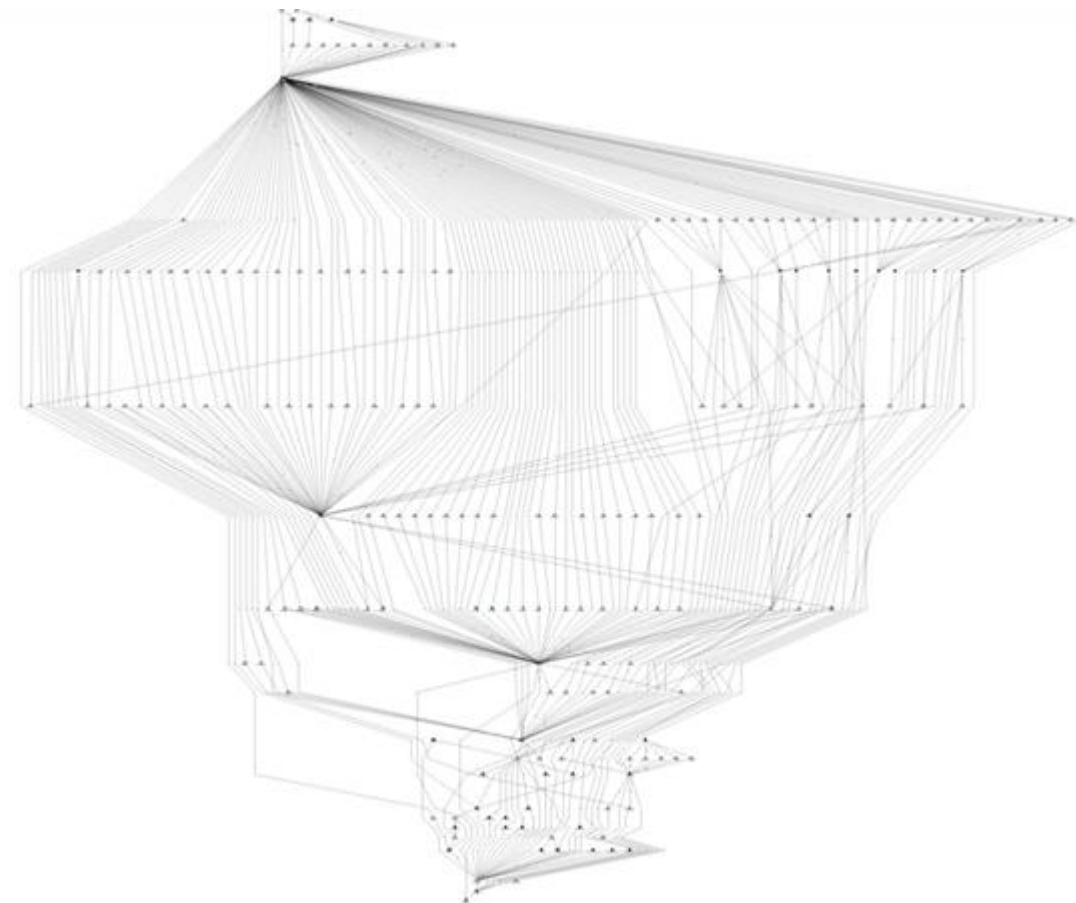


Рисунок 39 – Схематическое представление групп и связей



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 |
|-------------------|----------------|--|
| [ДААННЫЕ УДАЛЕНЫ] | 1.1 | Получена полная информация об уволившемся сотруднике: должность, оклад, состояние здоровья и семейное положение. |
| [ДААННЫЕ УДАЛЕНЫ] | 1.1 | Получен отказ |
| [ДААННЫЕ 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 «████████» 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 ██████████. |



Кейс 6 «Тысячи продавцов»

Тип работ:

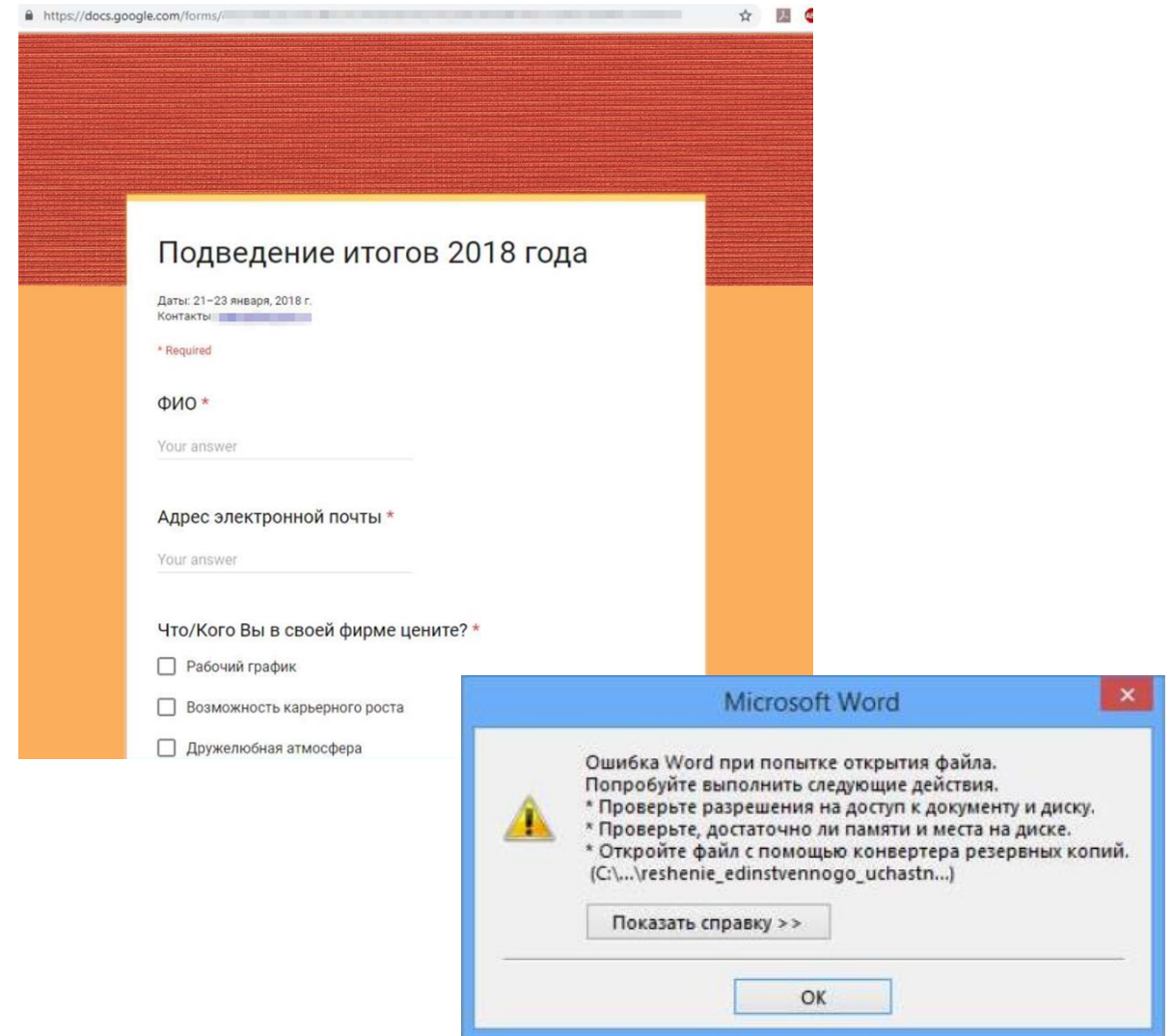
- Аудит защищённости ИС, проверка осведомлённости сотрудников

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 открыть 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
