GIS DAYS

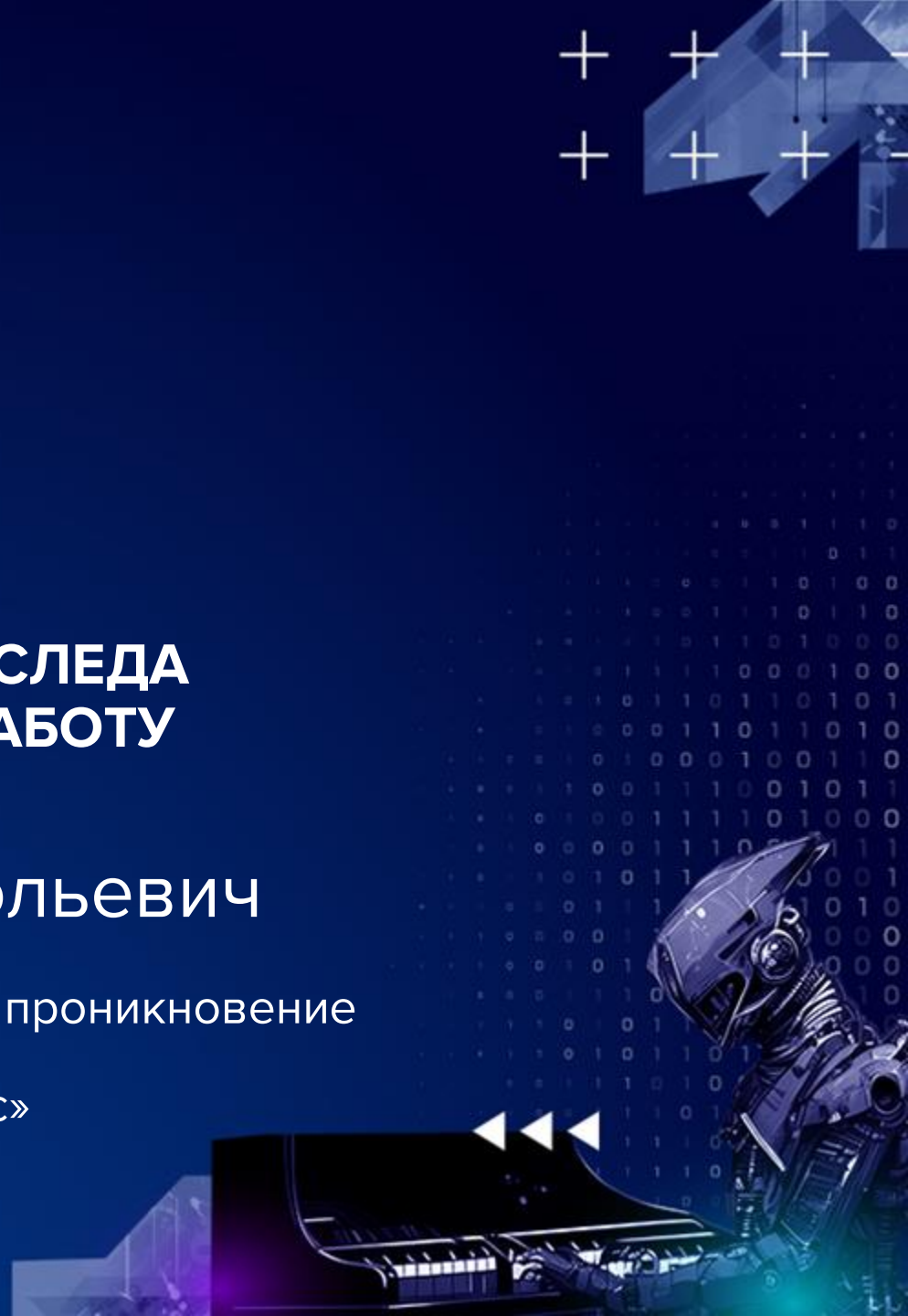
OSINT

ВЛИЯНИЕ ЦИФРОВОГО СЛЕДА ПРИ УСТРОЙСТВЕ НА РАБОТУ

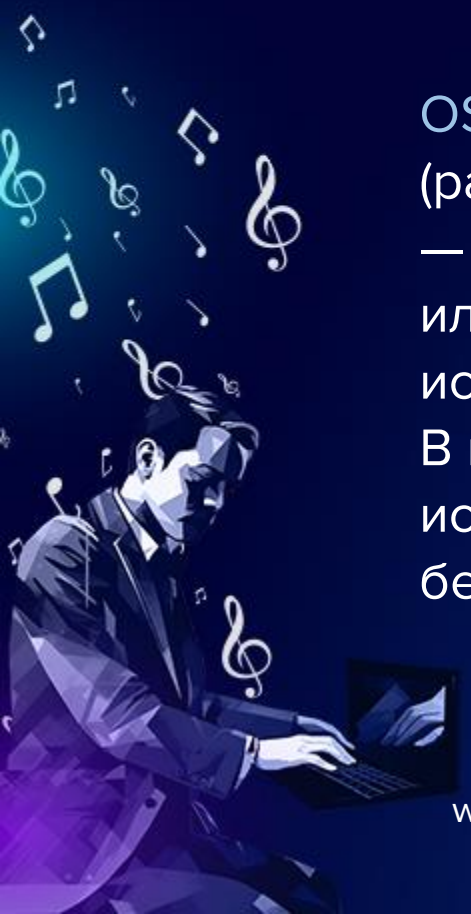
Носков Сергей Анатольевич

Руководитель группы тестирования на проникновение

ООО «Газинформсервис»



Что такое OSINT?



OSINT или open-source intelligence, (разведка на основе открытых данных) — это сбор информации о человеке или организации из открытых источников и ее последующий анализ. В настоящий момент OSINT активно используется в информационной безопасности

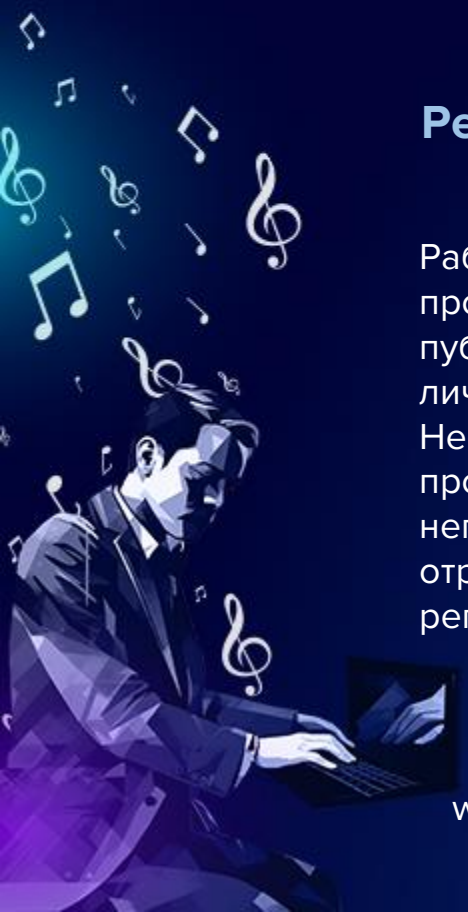
Цифровой след

Цифровой след (или цифровые следы) — это информационные следы, оставленные человеком в цифровой среде или при использовании цифровых технологий

Размер цифрового следа каждую минуту в наше время

YOUTUBE	INSTAGRAM	GOOGLE	MAIL
4 146 600	46 740	3 472 000	204 000 000
Человек смотрят видео	Новых фото	Запросов	Сообщений

Влияние цифрового следа при устройстве на работу



Репутация

Работодатели могут проверять профили соц.сетей и общественные публикации, чтобы узнать больше о личности и поведении кандидата. Несоответствие работника профессиональным стандартам или негативные комментарии/посты могут отрицательно отразиться на его репутации

Коммуникационные навыки

Онлайн-профили и активность в социальных сетях могут дать представление о коммуникативных навыках кандидата. Правильное использование языка, грамотное написание и умение поддерживать продуктивные диалоги могут быть важными факторами при выборе кандидата

Противоречивая информация

Работодатели могут проверять цифровой след, чтобы убедиться, что предоставленная кандидатом информация соответствует действительности. Если в онлайн-профиле или публичных записях присутствуют противоречия или неправдивая информация, это может вызвать сомнения в честности кандидата

Собираем компромат на себя за 10 минут

Какую информацию можно получить, зная номер телефона?

МОБИЛЬНЫЕ БАНКИ

Например: через банк, сделав перевод можно узнать имя, отчество и первую букву фамилии человека, также пол соответственно

СОЦИАЛЬНЫЕ СЕТИ

Если владелец номера связал его с аккаунтом в социальных сетях и разрешил публичный доступ к своим контактным данным, то можно найти профили владельца номера и получить дополнительную информацию

УТЕЧКИ

Большая часть информации содержится именно в утечках, По номеру через данные сервисы можно узнать: паспортные данные, ФИО, данные для входа в социальные сети, место проживания и т.д.

Пример проведения OSINT и обнаружение цифрового следа при приеме на работу

ЦЕЛЬ

Определить подходит ли кандидат к требованиям компании

ХОД РАБОТ

1. Изучить личность кандидата
2. Произвести поиск по известным данным и найти социальные сети кандидата
3. Произвести анализ социальных сетей
4. Составить отчет

РЕЗУЛЬТАТ

В ходе проделанной работы, определяется, подходит ли кандидат на данную должность

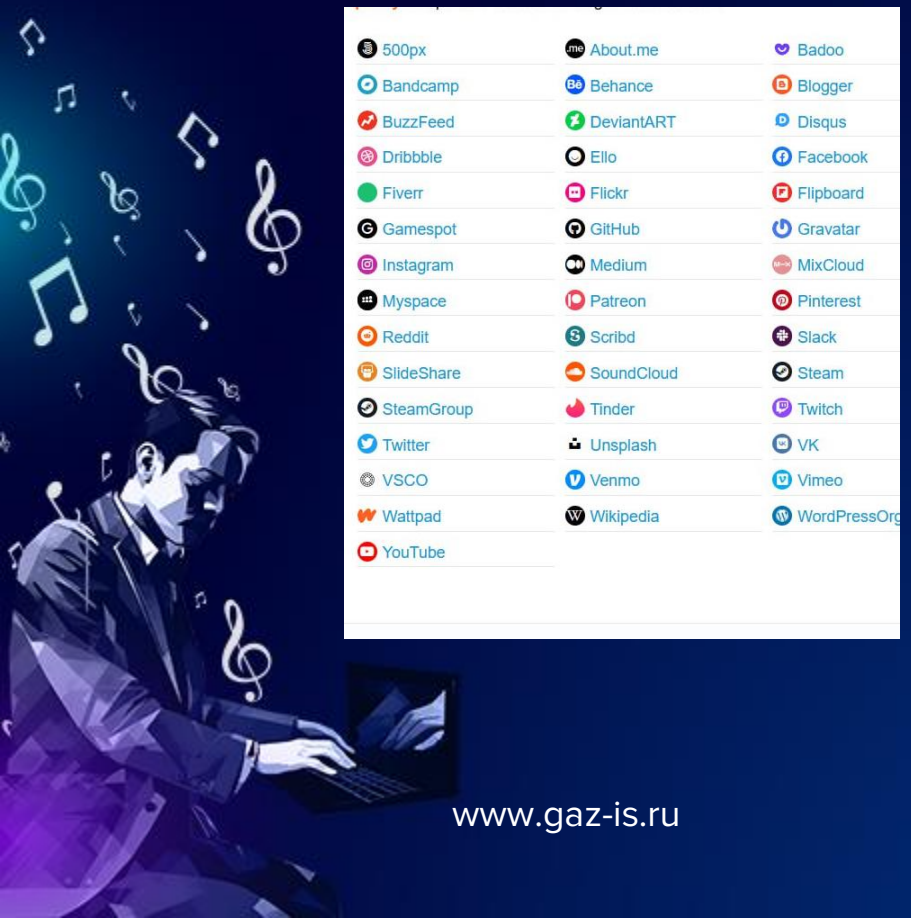
Сценарий №1

Поступил запрос от руководства, где нужно произвести сбор информации по кандидату, который хочет устроиться в компанию

ЦЕЛЬ

Составить отчет подходит ли он на данную должность

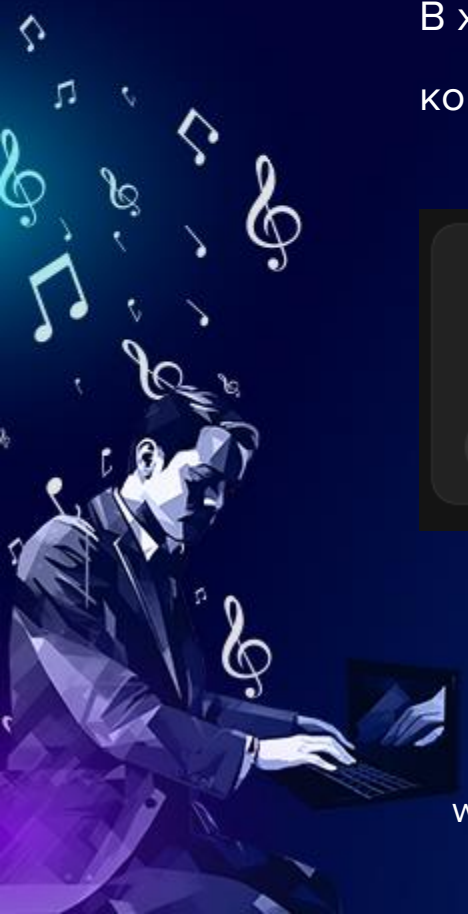
Сценарий №1

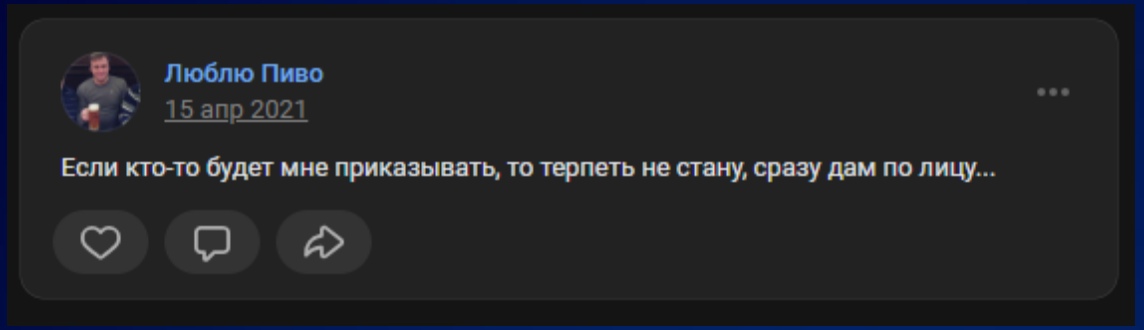


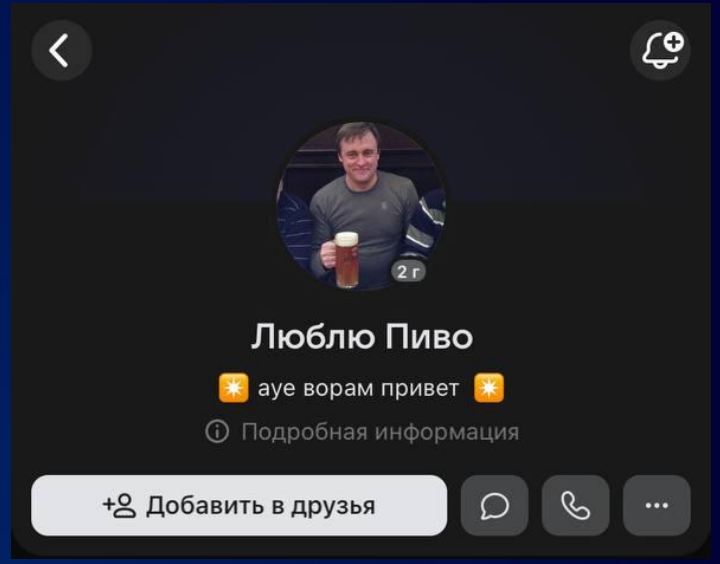
1. Изучаем личность кандидата Иванова Михаила Ивановича
2. Используем веб-инструмент https://www.peekyou.com для обнаружения социальных сетей по известному ФИО
3. Проводим анализ по предоставленным социальным сетям и рассматриваем более детально те платформы, на которых пользователь ведет активную деятельность
4. Замечаем, что наиболее активен пользователь в социальной сети ВКонтакте. Проводим полный анализ страницы (фото, коментарии, подписки, друзья). На основе найденной информации составляем психологический портрет

Сценарий №1

В ходе составления психологического портрета выясняем, что, человек ведет неподобающий для компании и должности образ жизни, что может привести к репутационным рискам







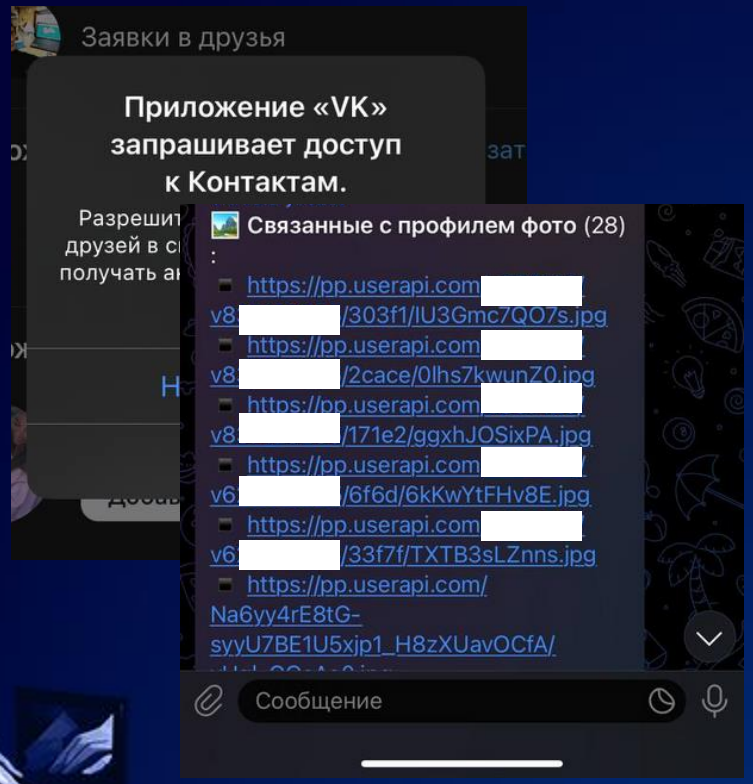
Сценарий №2

Поступило предложение от кандидата, который хочет устроиться в предприятие, работающее с государственной тайной

ЦЕЛЬ

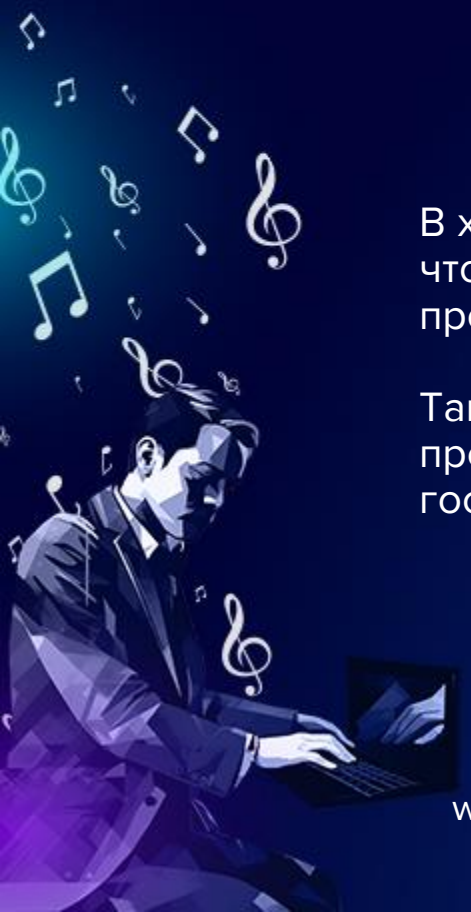
Составить отчет подходит ли он на данную должность

Сценарий №2



1. Известен личный номер и ФИО кандидата
2. Пробуем найти по ФИО социальные сети человека, но безрезультатно
3. Используем один из способов для нахождения человека в ВКонтакте по номеру телефона. Для этого на мобильном устройстве добавляем номер в телефонную книгу, а затем осуществляем ее импорт в социальной сети
4. Удаётся найти аккаунт ВКонтакте пользователя, но он оказывается пустой
5. В таком случае, используем бота в телеграмме https://t.me/VKHistoryRobot, который показывает удаленную информацию из ВК. Анализируем полученные данные

Сценарий №2



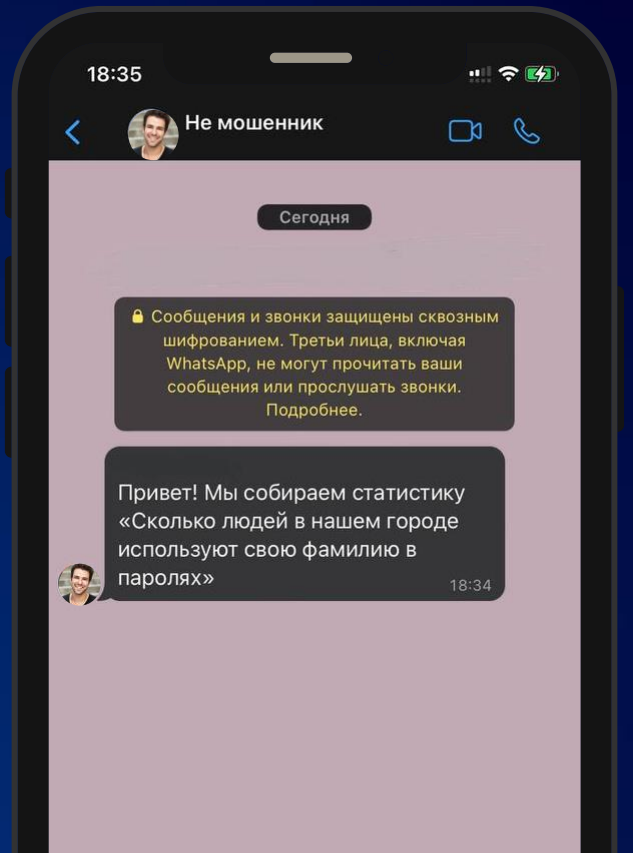
В ходе проделанной работы можно обнаружить, что кандидат любит путешествовать в США и проявляет симпатию к данной стране

Таким образом, данный кандидат не может претендовать на место в предприятии с государственной тайной

GIS DAYS

Социальная инженерия: применение результатов

Социальная инженерия – метод получения нужной информации, который опирается на понимание психологических особенностей людей



GIS DAYS

К чему может привести социальная инженерия с применением добытых данных о цели?

УТЕЧКА КОРПОРАТИВНОЙ ИНФОРМАЦИИ

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ ОБЪЕКТОВ

Практический пример проведения OSINT в разрезе с социальной инженерией

ЦЕЛЬ

Провести социальную инженерию для получения необходимых действий от цели

ХОД РАБОТ

1. Перед проведением социальной инженерии осуществляем сбор информации о цели
2. Ознакамливаемся с полученной информацией и постараться узнать, какая информация для пользователя является наиболее значимой
3. Составить историю, которая будет производить психологическое воздействие на пользователя
4. Составить отчет об итоге проведенной социальной инженерии

РЕЗУЛЬТАТ

Осуществляется получение необходимой информации, либо совершение каких-либо действий от цели

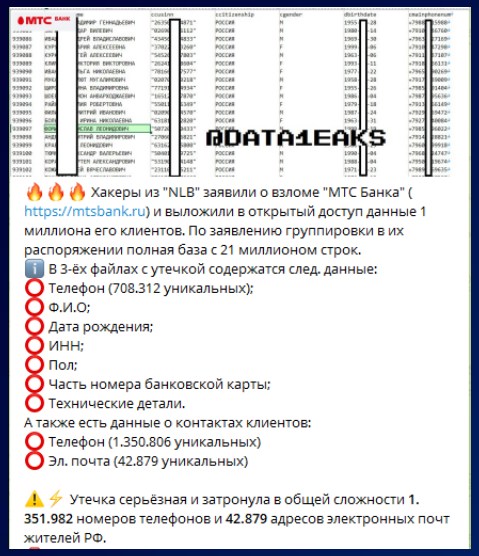
Сценарий №1

Злоумышленник притворяется сотрудником банка, база данных которых была недавно слита в общий доступ

ЦЕЛЬ

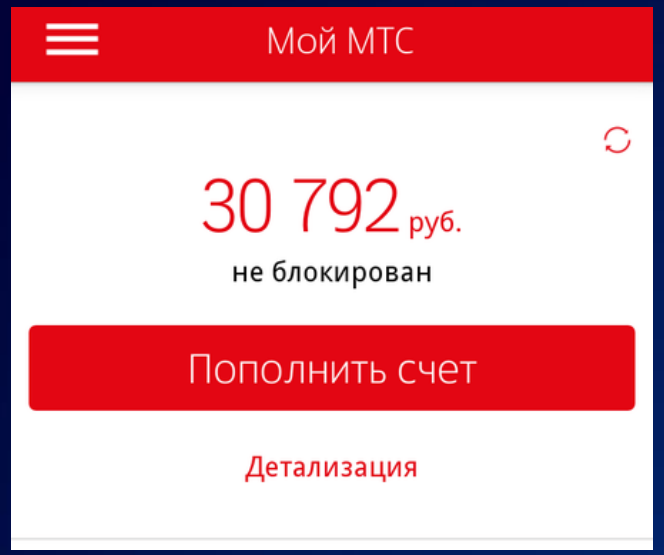
Заставить жертву осуществить перевод денежных средств

Сценарий №1



1. Злоумышленник анализирует слитую базу данных и собирает для себя необходимую информацию
2. Составляет список жертв и придумывает для них сценарий при проведении социальной инженерии
3. Производит звонок на номер жертвы и представляется сотрудником данного банка
4. Проводит сценарий, что произошла утечка его конфиденциальных данных. Необходимо в срочном порядке произвести перевод всей суммы на безопасный счет банка

Сценарий №1



Злоумышленнику удаётся обмануть жертву, в результате чего, он получает перевод огромной суммы

Жертва в свою очередь не подозревает о злоумышленнике и переводит всю сумму мошеннику, в следствии чего, теряет её

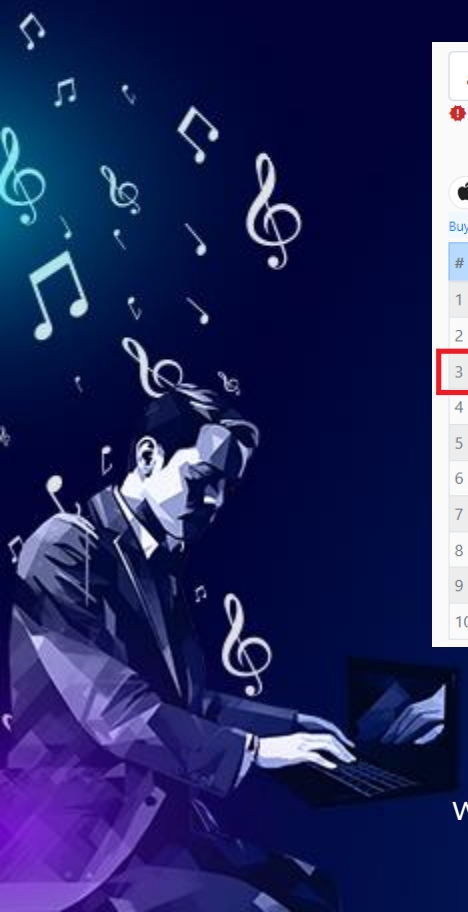
Сценарий №2

Проведение конкурентной разведки в целях получения финансовой информации оклада сотрудника

ЦЕЛЬ

Переманивание сотрудников в свою компанию

Сценарий №2



apple.com

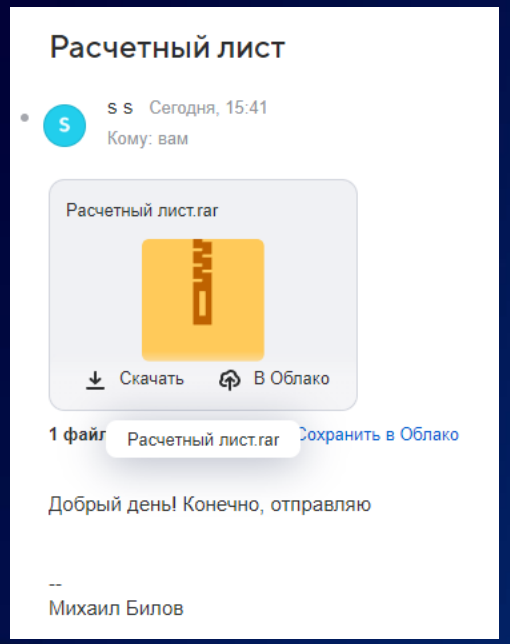
apple.com (6298 emails)

Buy now all 6298 emails of this domain.

#	Email (6298)
1	kimsilv@apple.com
2	rvalenzuela@apple.com
3	Alex-techsupport@apple.com
4	commute@apple.com
5	jack_tran@apple.com
6	tkerr@apple.com
7	dburger@apple.com
8	michele_wyman@apple.com
9	djohnston@apple.com
10	emolina1@apple.com

- сбор корпоративных почтовых адресов компании для проведения социальной инженерии
- Поиск корпоративных почтовых адресов по домену компании, используем веб-инструмент https://www.skymem.info
- Подбираем наиболее подходящую под тех. поддержку компании
- Создаем аналогичную почту с незначительным изменением. Например, убирается дефис
- Производится рассылка по всем найденным корпоративным адресам, содержащая информацию о сбое системы и необходимости прислать расчетный лист за прошлый месяц

Сценарий №2



В ходе проведенной социальной инженерии, конкурентной компании удаётся получить финансовую информацию о некоторых сотрудниках, которые доверились почте злоумышленника

Как снизить риски воздействия?

- Использовать 2FA-аутентификацию (при ее наличии)
- Периодически (не реже раз в пол года) обновлять пароли от сервисов. При информации об утечках данных на одном из сервисов – обновить пароль на нем в кротчайшее время
- Как можно меньше выкладывать о себе информации на различных ресурсах (статьи, комментарии, видео, фотографии и т.п.). Если вы это делаете, то оценивайте риски публикации данной информации
- Закрывать профили (при наличии таких функций)
- Запретить синхронизацию любых данных вашего сервиса с данными телефона (например, контакты)
- Предоставлять как можно меньше прав приложениям публичных ресурсов (VK, OZON, Instagram и т.п.). Должны быть предоставлены только те разрешения (в минимальном объеме), которые требуются для его нормального функционирования
- Если вы видите, что приложение использует разрешения превышающие минимально допустимые для его функционирования, используйте веб-версию данного сервиса (при наличии такой возможности)

GIS DAYS

СПАСИБО ЗА ВНИМАНИЕ

@GIS_PENTEST

Контакты
www.gaz-is.ru

SOC GIS