



GIS
D A Y S

OSINT

**ВЛИЯНИЕ ЦИФРОВОГО СЛЕДА
ПРИ УСТРОЙСТВЕ НА РАБОТУ**

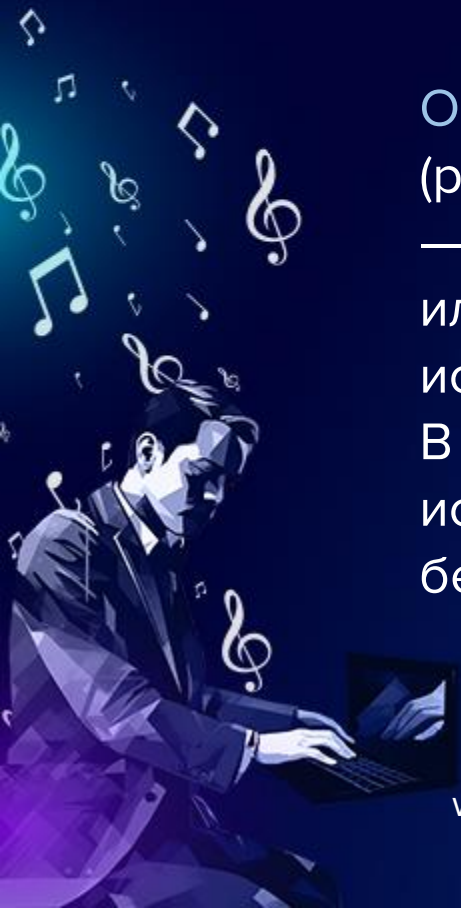
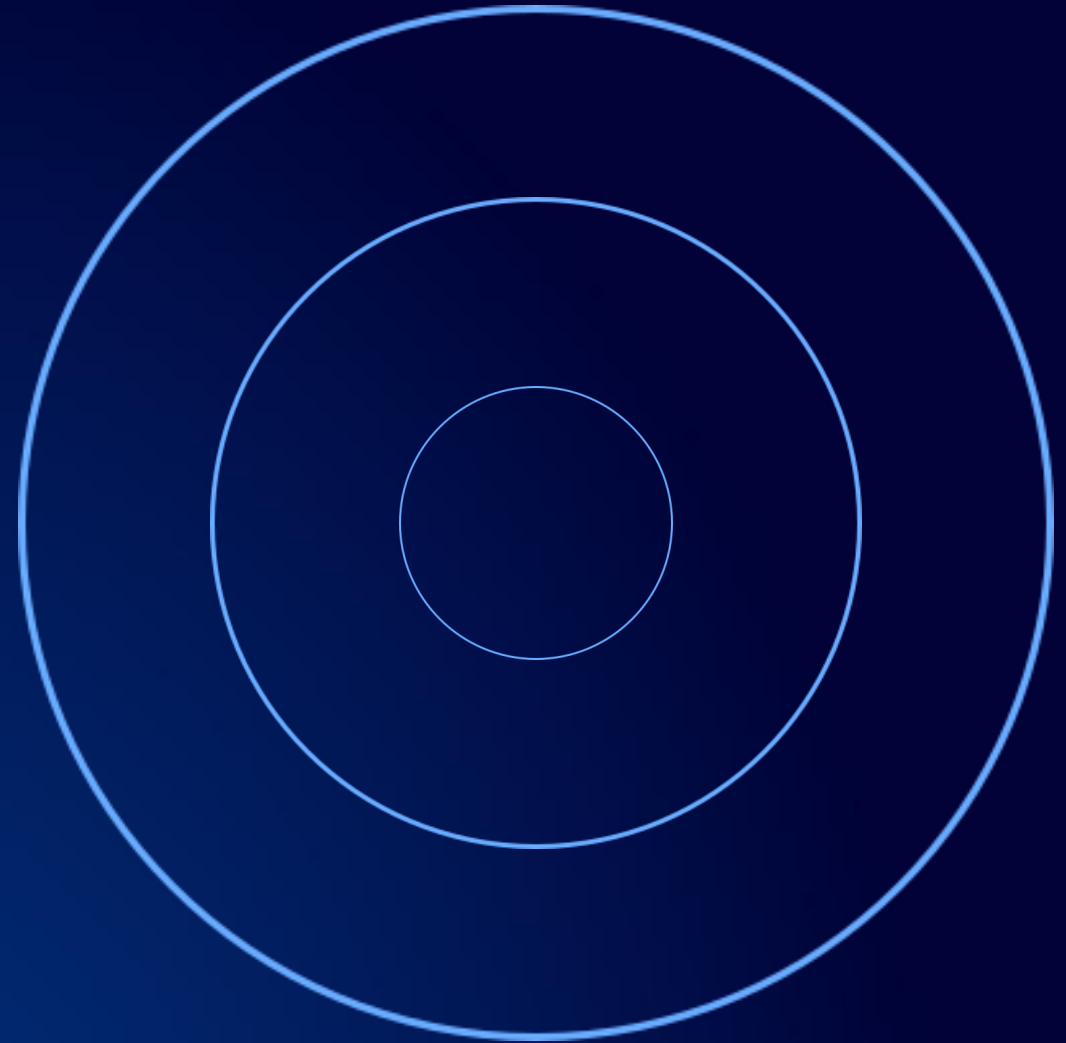
Носков Сергей Анатольевич

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

4 146 600

Человек смотрят видео

 INSTAGRAM

46 740

Новых фото

 GOOGLE

3 472 000

Запросов

 MAIL

204 000 000

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?

www.gaz-is.ru

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 контактными 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

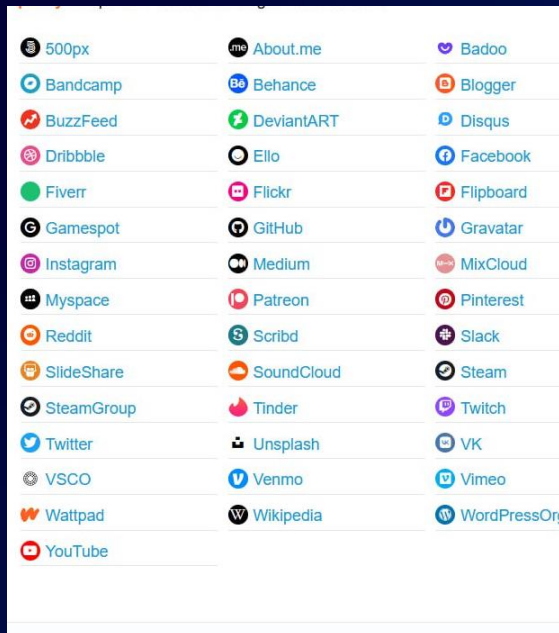
Поступил запрос от руководства, где нужно произвести сбор информации по кандидату, который хочет устроиться в компанию

ЦЕЛЬ

Составить отчет подходит ли он на данную должность



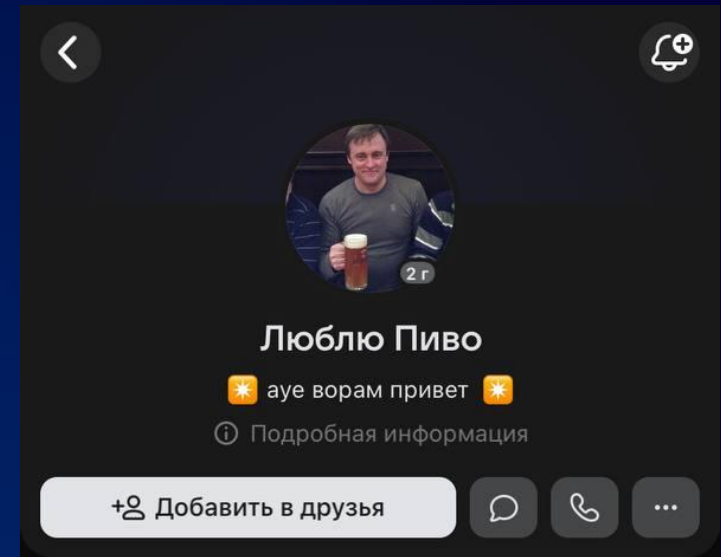
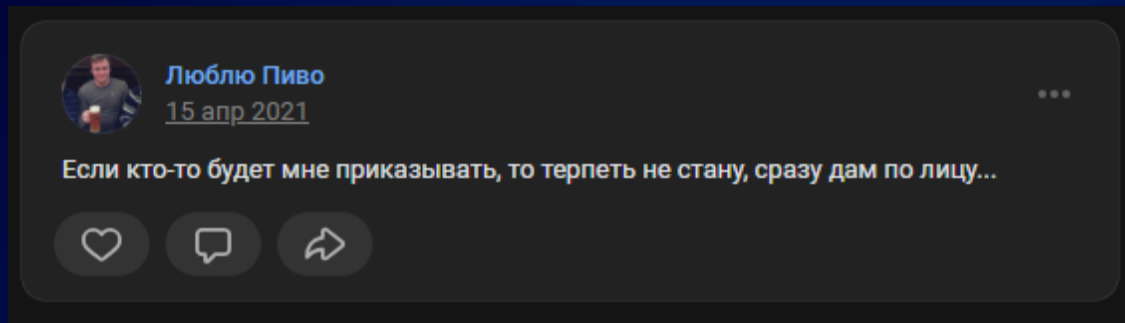
Сценарий №1



1. Изучаем личность кандидата Иванова Михаила Ивановича
2. Используем веб-инструмент <https://www.seekeyou.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, комментарии, 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



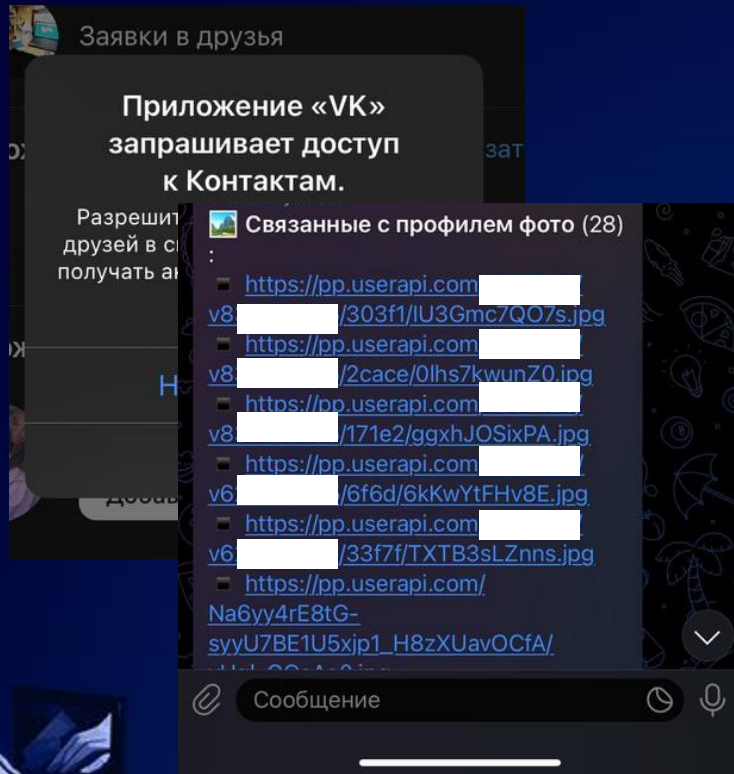
Сценарий №2

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

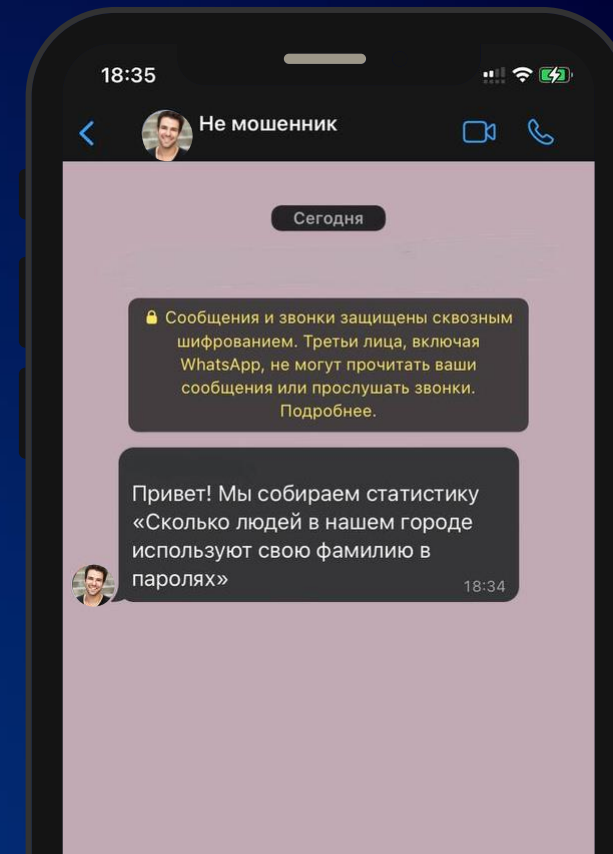
Таким образом, данный кандидат не может претендовать на место в предприятии с государственной тайной



Социальная инженерия: применение результатов

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

www.gaz-is.ru



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

УТЕЧКА
КОРПОРАТИВНОЙ
ИНФОРМАЦИИ

ФИНАНСОВОЕ
МОШЕННИЧЕСТВО

РАСПРОСТРАНЕНИЕ
ВРЕДНОСНЫХ 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 N°1

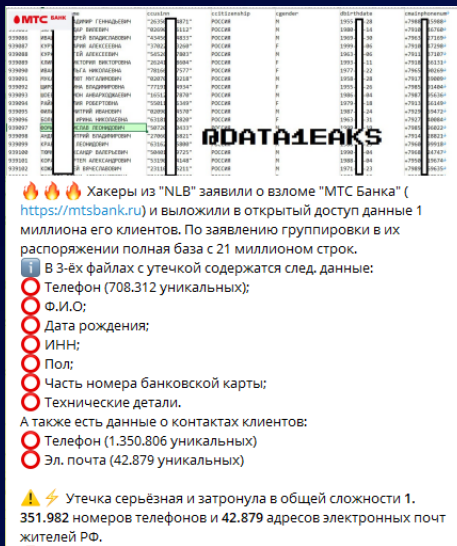
Злоумышленник притворяется сотрудником банка, база данных которых была недавно слита в общий доступ

ЦЕЛЬ

Заставить жертву осуществить перевод денежных средств



Сценарий №1



MTS BANK

id	ФИО	ИНН	Дата рождения	Пол	Номер телефона	Адрес электронной почты
100001	Иванов Иван Иванович	7707083893	1985-01-15	М	7900000000	ivanov@mtsbank.ru
100002	Петров Петр Петрович	7707083893	1985-01-15	М	7900000000	petrov@mtsbank.ru
100003	Сидоров Сергей Сергеевич	7707083893	1985-01-15	М	7900000000	sidorov@mtsbank.ru
100004	Смирнов Алексей Алексеевич	7707083893	1985-01-15	М	7900000000	smirnov@mtsbank.ru
100005	Соколов Дмитрий Дмитриевич	7707083893	1985-01-15	М	7900000000	sokolov@mtsbank.ru
100006	Соловьев Александр Александрович	7707083893	1985-01-15	М	7900000000	solovьев@mtsbank.ru
100007	Степанов Евгений Евгеньевич	7707083893	1985-01-15	М	7900000000	stepanov@mtsbank.ru
100008	Тихонов Владимир Владимирович	7707083893	1985-01-15	М	7900000000	tykhonov@mtsbank.ru
100009	Толкачев Николай Николаевич	7707083893	1985-01-15	М	7900000000	tolkachev@mtsbank.ru
100010	Трофимов Алексей Алексеевич	7707083893	1985-01-15	М	7900000000	trofimov@mtsbank.ru
100011	Федотов Дмитрий Дмитриевич	7707083893	1985-01-15	М	7900000000	fedotov@mtsbank.ru
100012	Фролов Сергей Сергеевич	7707083893	1985-01-15	М	7900000000	frolov@mtsbank.ru
100013	Харьков Евгений Евгеньевич	7707083893	1985-01-15	М	7900000000	kharkov@mtsbank.ru
100014	Хохлов Алексей Алексеевич	7707083893	1985-01-15	М	7900000000	khokhlov@mtsbank.ru
100015	Цыганов Дмитрий Дмитриевич	7707083893	1985-01-15	М	7900000000	tsyganov@mtsbank.ru
100016	Чайков Александр Александрович	7707083893	1985-01-15	М	7900000000	chaykov@mtsbank.ru
100017	Чернов Евгений Евгеньевич	7707083893	1985-01-15	М	7900000000	chernov@mtsbank.ru
100018	Шаров Владимир Владимирович	7707083893	1985-01-15	М	7900000000	sharov@mtsbank.ru
100019	Шестаков Николай Николаевич	7707083893	1985-01-15	М	7900000000	shestakov@mtsbank.ru
100020	Шутов Алексей Алексеевич	7707083893	1985-01-15	М	7900000000	shutov@mtsbank.ru
100021	Щеголов Дмитрий Дмитриевич	7707083893	1985-01-15	М	7900000000	shchegolov@mtsbank.ru
100022	Щербинин Евгений Евгеньевич	7707083893	1985-01-15	М	7900000000	shcherbinin@mtsbank.ru
100023	Щукин Александр Александрович	7707083893	1985-01-15	М	7900000000	shchukin@mtsbank.ru
100024	Экимова Мария Михайловна	7707083893	1985-01-15	Ж	7900000000	ekimova@mtsbank.ru
100025	Юсупов Дмитрий Дмитриевич	7707083893	1985-01-15	М	7900000000	yusupov@mtsbank.ru
100026	Яковлев Алексей Алексеевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100027	Яковлев Дмитрий Дмитриевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100028	Яковлев Евгений Евгеньевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100029	Яковлев Иван Иванович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100030	Яковлев Петр Петрович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100031	Яковлев Сергей Сергеевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100032	Яковлев Владимир Владимирович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100033	Яковлев Дмитрий Дмитриевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100034	Яковлев Евгений Евгеньевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100035	Яковлев Иван Иванович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100036	Яковлев Петр Петрович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100037	Яковлев Сергей Сергеевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100038	Яковлев Владимир Владимирович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100039	Яковлев Дмитрий Дмитриевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100040	Яковлев Евгений Евгеньевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100041	Яковлев Иван Иванович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100042	Яковлев Петр Петрович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100043	Яковлев Сергей Сергеевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100044	Яковлев Владимир Владимирович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100045	Яковлев Дмитрий Дмитриевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100046	Яковлев Евгений Евгеньевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100047	Яковлев Иван Иванович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100048	Яковлев Петр Петрович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100049	Яковлев Сергей Сергеевич	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru
100050	Яковлев Владимир Владимирович	7707083893	1985-01-15	М	7900000000	yakovlev@mtsbank.ru

DATALEAKS

🔥🔥🔥 Хакеры из "NLB" заявили о взломе "МТС Банка" (<https://mtsbank.ru>) и выложили в открытый доступ данные 1 миллиона его клиентов. По заявлению группировки в их распоряжении полная база с 21 миллионом строк.

📁 В 3-х файлах с утечкой содержатся след. данные:

- 📞 Телефон (708.312 уникальных);
- 👤 Ф.И.О;
- 📅 Дата рождения;
- 🏠 ИНН;
- ♂️ Пол;
- 📇 Часть номера банковской карты;
- 🔧 Технические детали.

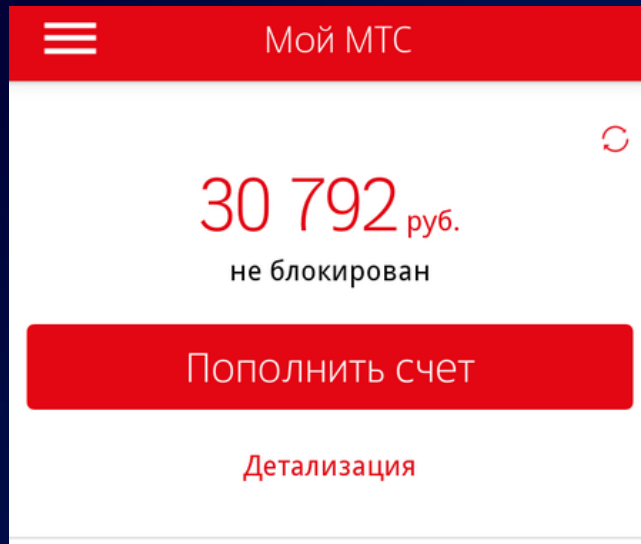
А также есть данные о контактах клиентов:

- 📞 Телефон (1.350.806 уникальных)
- ✉️ Эл. почта (42.879 уникальных)

⚠️ Утечка серьезная и затронула в общей сложности 1.351.982 номеров телефонов и 42.879 адресов электронных почт жителей РФ.

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 удастся 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 N°2

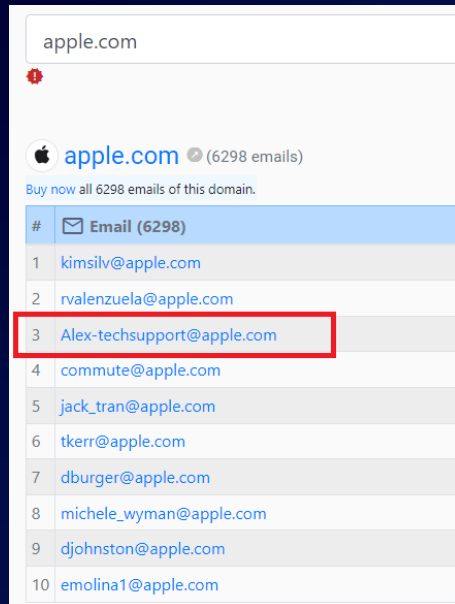
Проведение конкурентной разведки в целях получения финансовой информации
оклада сотрудника

ЦЕЛЬ

Переманивание сотрудников в свою компанию



Сценарий N°2



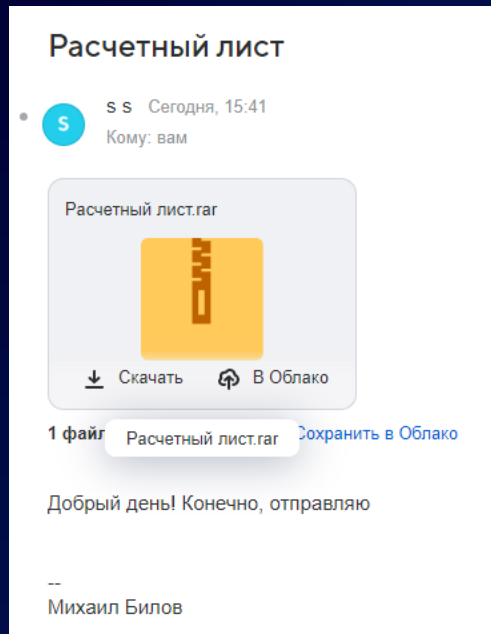
apple.com

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 N°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 кратчайшее 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
D A Y S

СПАСИБО ЗА ВНИМАНИЕ



Контакты
www.gaz-is.ru

SOC GIS