Выходим за периметр: угрозы извне, о которых лучше узнать заранее

МОСКВА 2023

SOC
FORUM
2023

АЛЕКСАНДР ВУРАСКО

ГК «Солар»

SOC FORUM 2023

ИЗМЕНЕНИЕ МОТИВАЦИИ АТАКУЮЩИХ ПОВЛЕКЛО СМЕЩЕНИЕ ЛАНДШАФТА УГРОЗ

Объемы утечек российских организаций в 2023 году

SOC FORUM 2023

333

ОРГАНИЗАЦИИ, ДАННЫЕ КОТОРЫХ ПОПАЛИ В СЕТЬ С ЯНВАРЯ ПО ОКТЯБЬ

103,4 ТБ

ОБЩИЙ ОБЪЕМ ОПУБЛИКОВАННЫХ ДАННЫХ

Базы данных, размещенные в общем доступе с начала года

SOC FORUM 2023

СОСТАВ

91%

от общего числа утечек составляют массивы структурированной информации

99%

от общего объема утечек составляют публикации архивов файлов, полученных из внутренних сетей организаций

СОДЕРЖАНИЕ

4,8 МЛРД

строк данных

141,5 МЛН

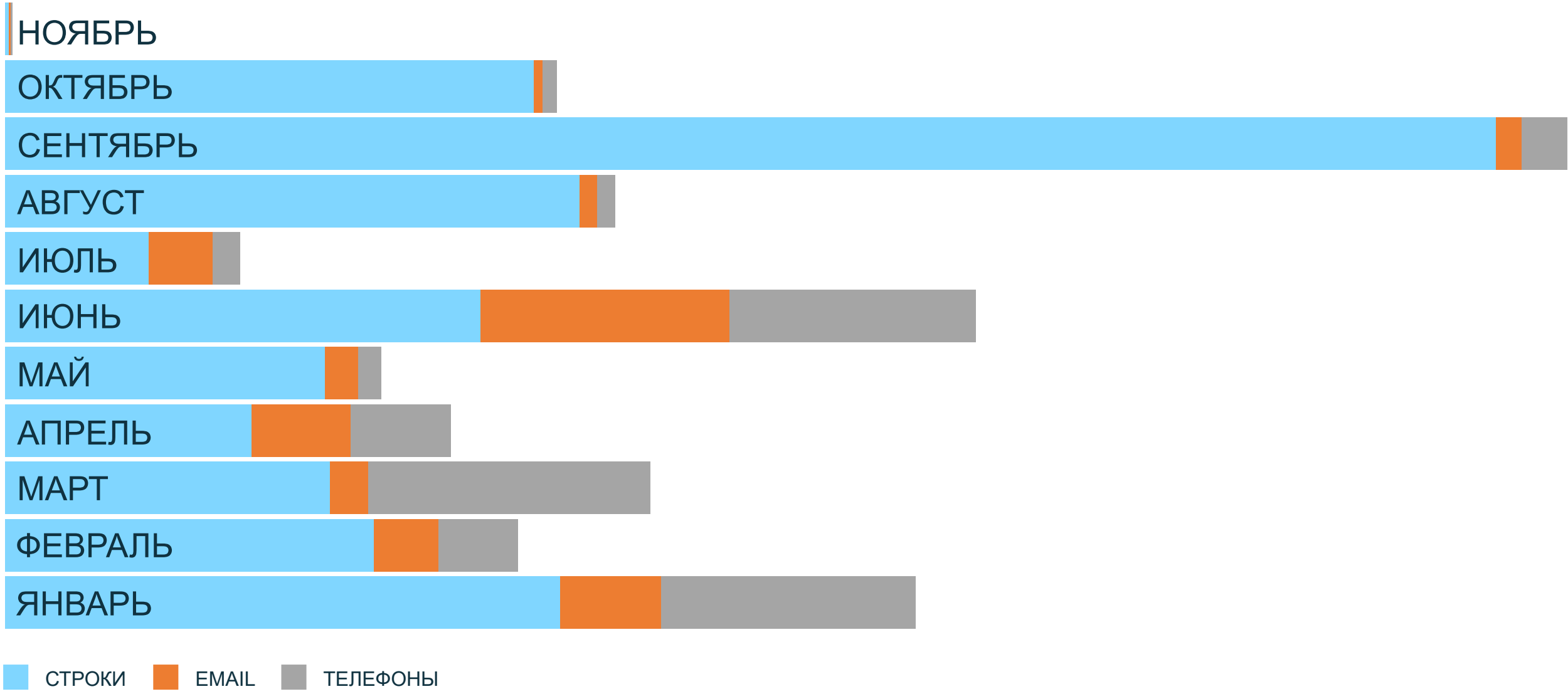
адресов электронной почты

219,8 МЛН

телефонных номеров

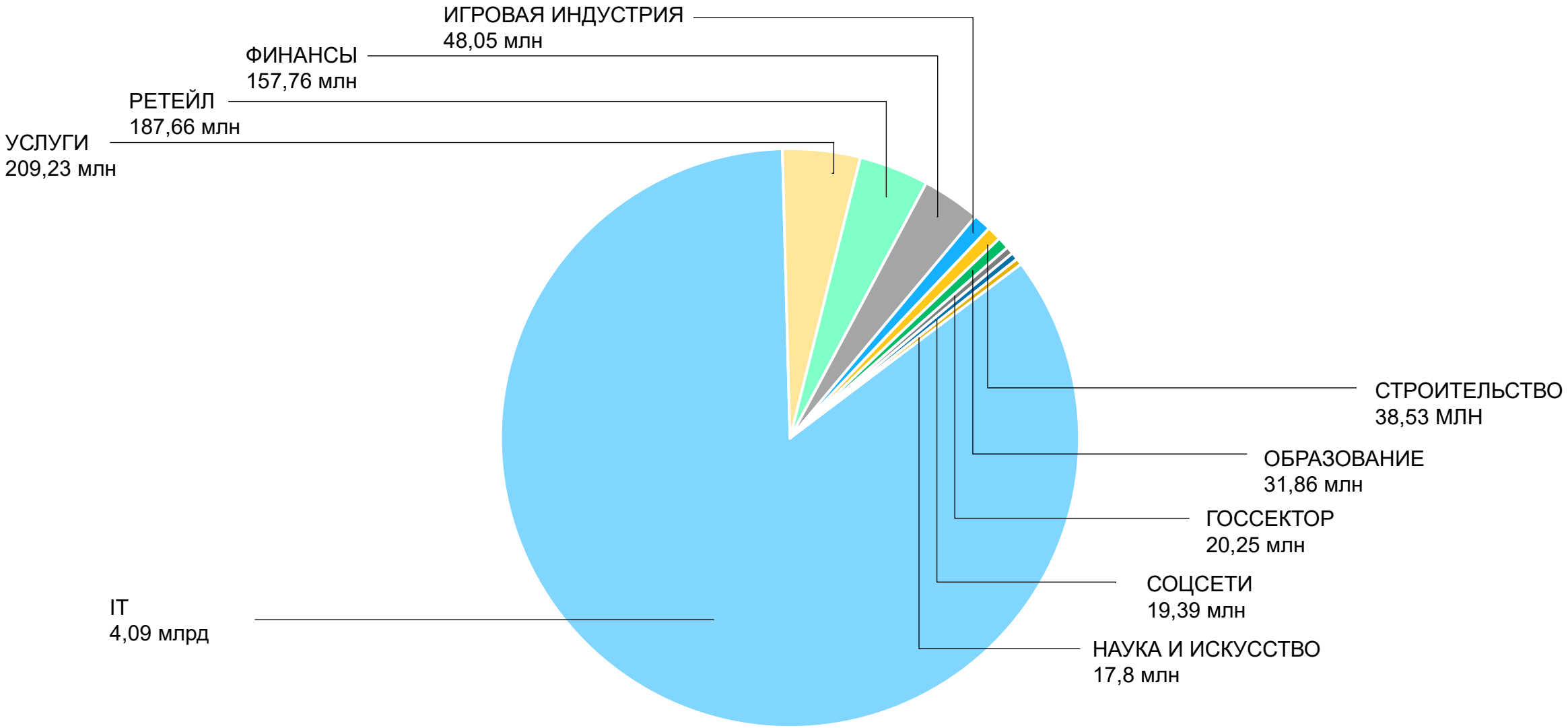
Российские утечки по месяцам

SOC FORUM 2023



Распределение утечек по отраслям

SOC FORUM 2023



SOC FORUM 2023

ИСКАТЬ ЛИШЬ ТЕ ИНЦИДЕНТЫ, КОТОРЫЕ НЕПОСРЕДСТВЕННО ЗАТРАГИВАЮТ ВАШУ КОМПАНИЮ, СТАЛО НЕЭФФЕКТИВНО

Косвенные утечки – неочевидная, но реальная угроза

SOC FORUM 2023

ТРЕНД ОСЕНИ 2023: АТАКИ НА СОТРУДНИКОВ ОТ ИМЕНИ ГЕНЕРАЛЬНОГО ДИРЕКТОРА КОМПАНИИ

1 ЭТАП

Поиск корпоративных адресов электронной почты в различных утекших базах

2 ЭТАП

Анализ связанных с корпоративными адресами персональных данных

3 ЭТАП

Поиск в открытых источниках данных о руководстве компании, в случае удачи – копирование сведений из настоящего профиля гендиректора в Telegram

4 ЭТАП

Создание фейкового профиля и рассылка сообщений в адрес сотрудников

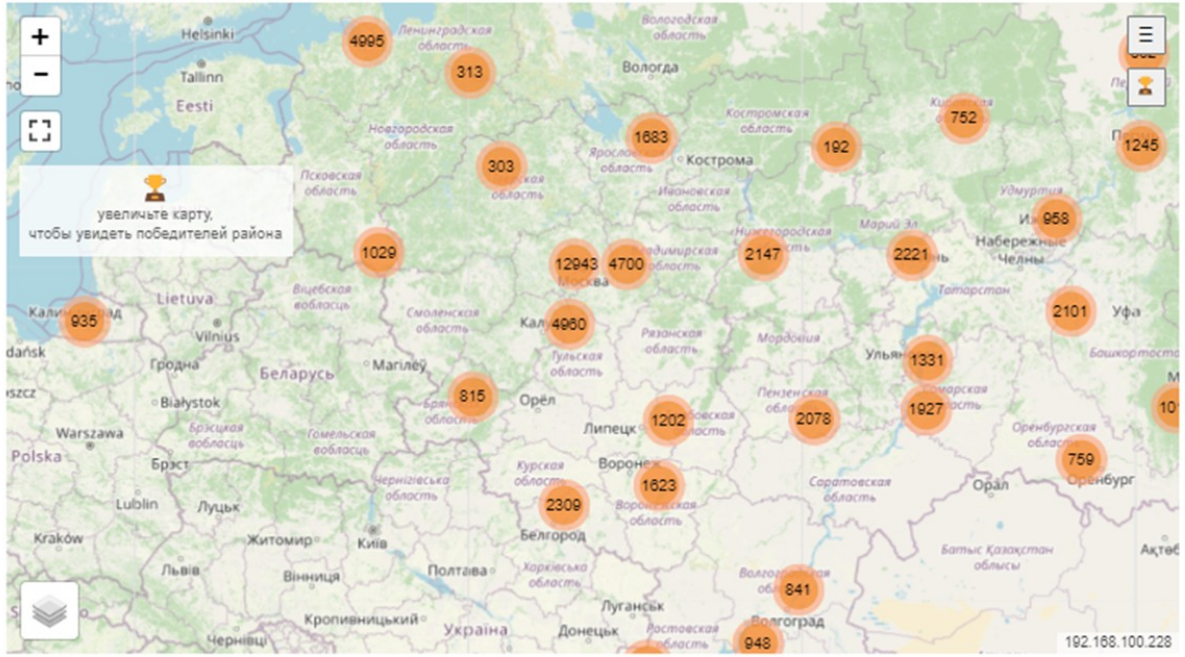
Не ФИО единым…

SOC FORUM 2023

Проверка информации из слитых баз данных на карте

- 🔍 Проверка по номеру телефона или фамилии
- 🌍 Проверка по адресу на карте
- Список публичных людей. Часть 1
- Список публичных людей. Часть 2
- Список публичных людей. Часть 3
- 📁 Torrent архивы а также инструкции по установке сайта. (🆕 обновлено)
- Новости

После начала военной спецоперации России на Украине, в результате массовых кибер атак на веб ресурсы РФ множество личных данных было незаконно выложено в сеть.
Мы увидели, насколько цена нашей конфиденциальности не ценится и решили запустить новую версию сайта. Суд оштрафовал "Яндекс.Еду" на 60 тыс руб за утечку данных клиентов, т.е. наши адреса доставки и личностные данные стоят 0.009 руб за пользователя(6397035 пользователей)
Все больше информации попадает в руки преступников, которой могут воспользоваться с целью запугивания или обмана.
Чтобы понимать риски, вы можете проверить, какая персональная информация есть у мошенников и уголовников.
Предупрежден значит вооружен!
ℹ Кажется, компаниям и стране плевать на персональные данные, поэтому мы публикуем полные данные на сайте и архивы на отдельной странице.
27 мая добавлено миллион адресов Delivery Club
saverudata.online | saverudata.info | saverudata.net



Источники, и важные ссылки

Second hand, или Полезный мусор

SOC FORUM 2023

МЫ ПРОАНАЛИЗИРОВАЛИ:

338+ млн учетных данных, опубликованных в период с января по апрель 2023 года

от 10+ тыс. различных сервисов

В РЕЗУЛЬТАТЕ ОБНАРУЖИЛИ АККАУНТЫ:

134 406 клиентов российских банков

977 615 пользователей российских социальных сетей

887 707 пользователей популярных российских почтовых сервисов

Фишинговые атаки. Тенденции и прогнозы

SOC FORUM 2023

МАКСИМАЛЬНАЯ АВТОМАТИЗАЦИЯ

от регистрации доменного имени
до формирования фишинговых ссылок,
взаимодействия с жертвой
и вывода похищенных денег

СКРЫТНОСТЬ

Все чаще используются
различные методы защиты
от обнаружения

СНИЖЕНИЕ ДОЛИ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТ-ЭКВАЙРИНГА

на фишинговых сайтах – акцент смещается с
разового списания платежа в сторону попытки
получить доступ к личному кабинету в системе
онлайн-банкинга

МАССОВЫЙ ПРИТОК В ОТРАСЛЬ НИЗКОКВАЛИФИЦИРОВАННЫХ КАДРОВ,

способных при этом осуществлять
технически сложные атаки
благодаря наличию продвинутых
инструментов

ИСПОЛЬЗОВАНИЕ ДОМЕНОВ, НЕ СВЯЗАННЫХ С КОНКРЕТНЫМ БРЕНДОМ

Все чаще в фишинговых схемах
задействованы произвольно
сгенерированные доменные имена

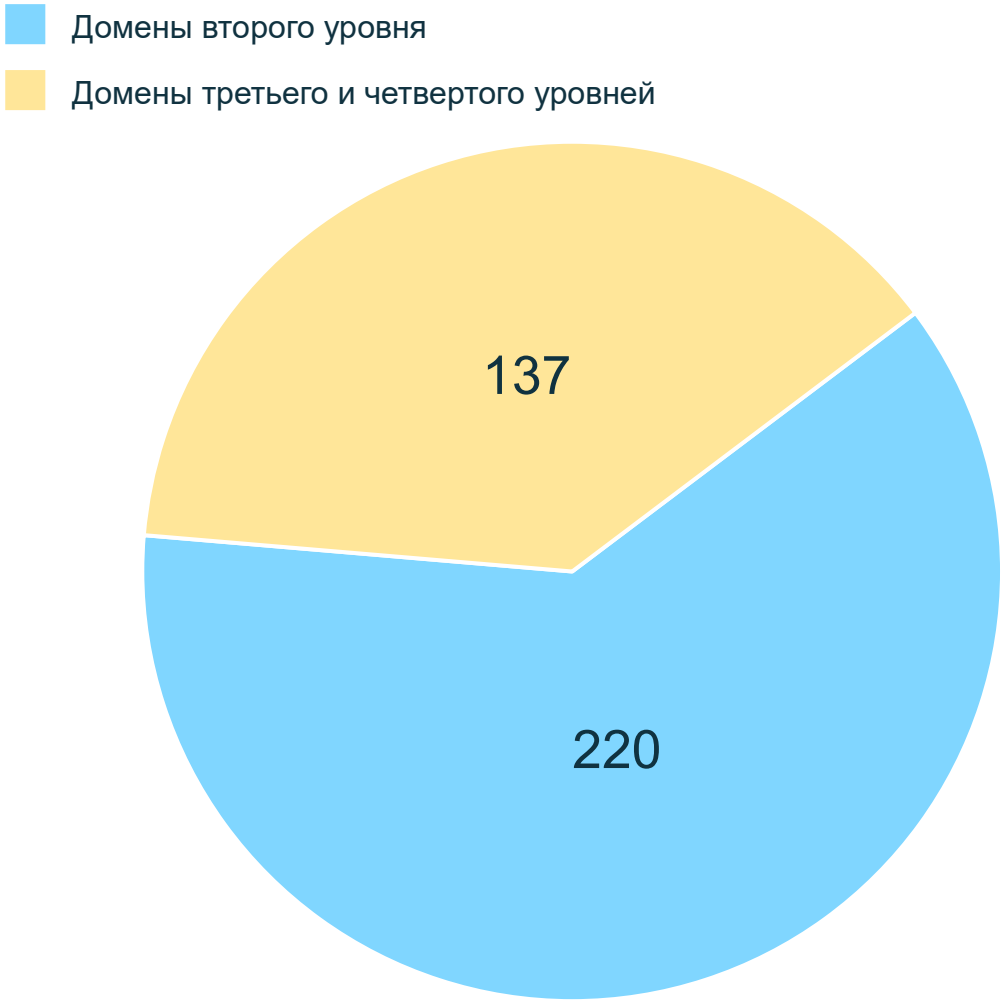
ФИШИНГ КАК ПРИКЛАДНОЙ ИНСТРУМЕНТ

Фишинговые ресурсы все чаще
используются как дополнительный
инструмент телефонных и иных
мошенников

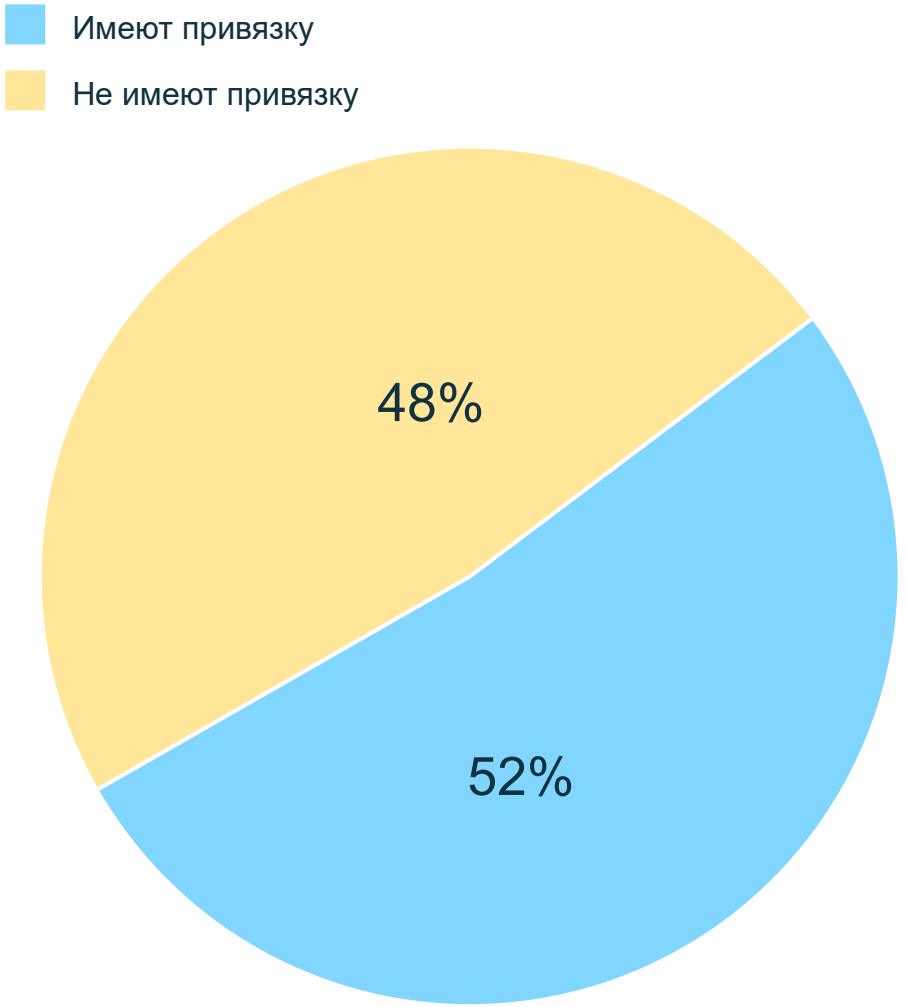
Тенденции фишинга на реальном примере

SOC FORUM 2023

СООТНОШЕНИЕ ВЫЯВЛЕННЫХ ФИШИНГОВЫХ ДОМЕНОВ

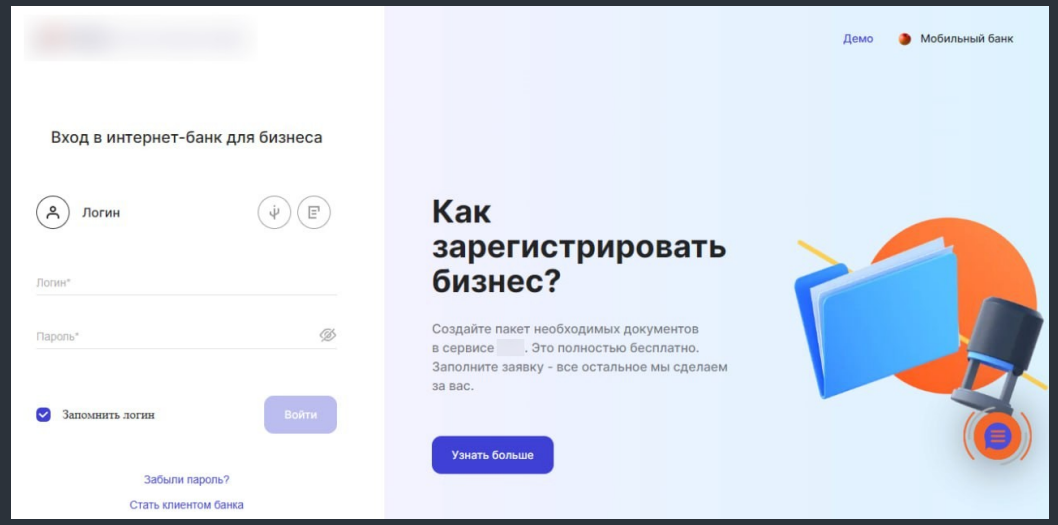


ПРИВЯЗКА ДОМЕНА К БРЕНДУ

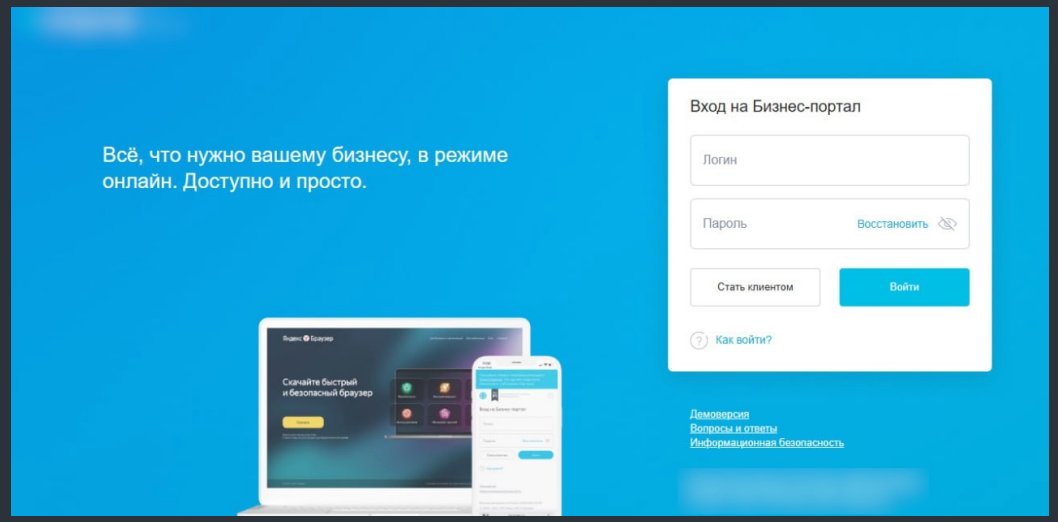


Поиск по шаблону

SOC FORUM 2023



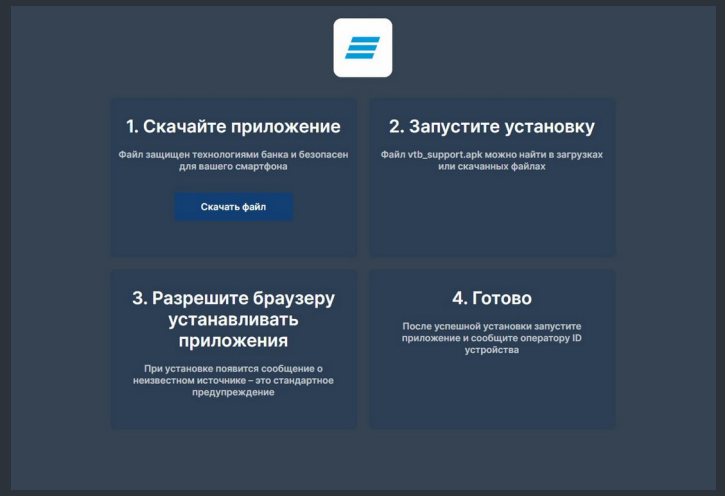
https://ibcaswb.space/

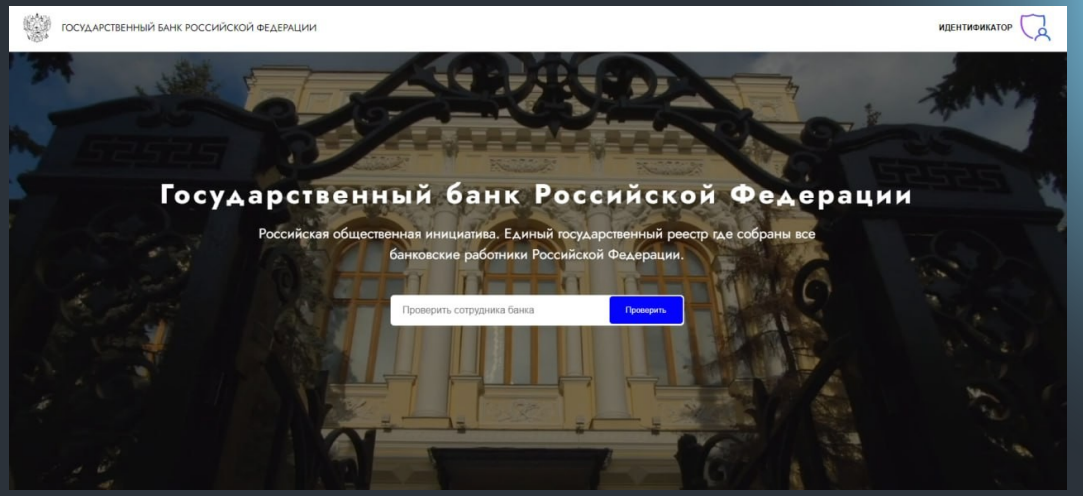


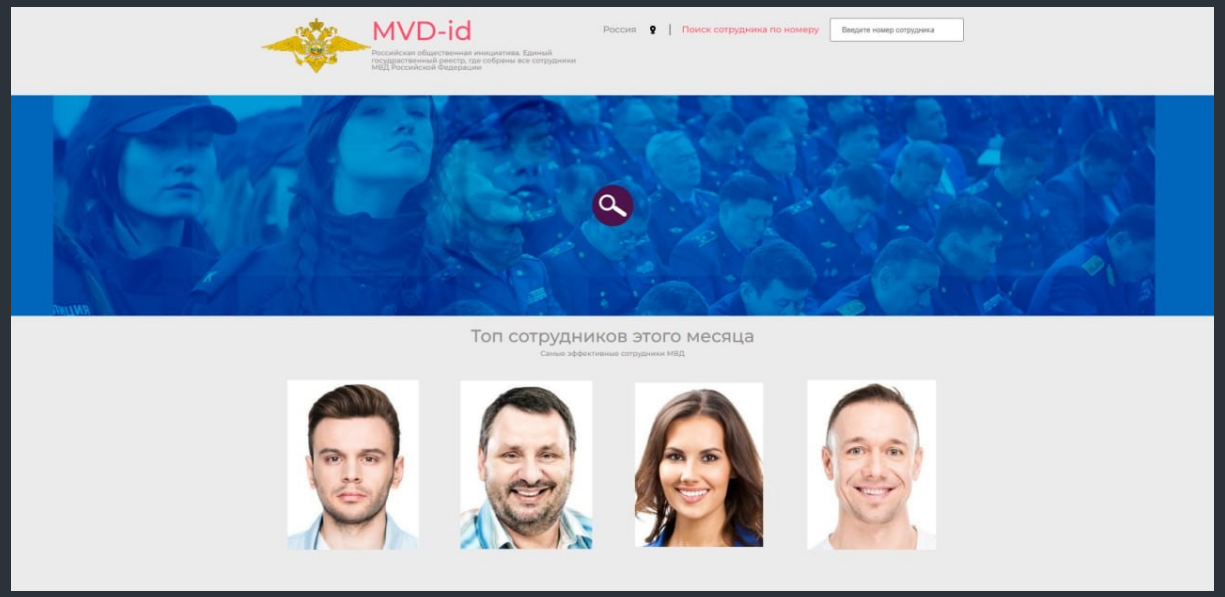
https://bp-****.ibcaswb.space/login

Фишинг + телефонные мошенничества

SOC FORUM 2023







Выводы

SOC FORUM 2023

КИБЕРПРЕСТУПНОСТЬ СЕГОДНЯ – ЭТО ХОРОШО ОТЛАЖЕННАЯ ИНДУСТРИЯ. ЭТО ТЫСЯЧИ ЛЮДЕЙ, ИМЕЮЩИХ ОПЫТ И ПРОДВИНУТЫЕ ИНСТРУМЕНТЫ ДЛЯ ОСУЩЕСТВЛЕНИЯ КИБЕРАТАК

[01] Безопасность вашей компании зависит не только от вас: косвенные инциденты могут представлять серьезную угрозу

[02] Злоумышленники постоянно совершенствуют методы работы, соответственно инструменты противодействия угрозам должны постоянно развиваться

[03] Ручной поиск в сети без использования аналитических инструментов и доступа к широкому перечню источников данных неэффективен

SOC
FORUM
2023

ВОПРОСЫ?

SOC FORUM 2023

8 (800) 302-85-23
solar@rt-solar.ru

ГК «Солар»
Никитский переулок, 7, стр. 1, г. Москва