ANGARA
SOC

OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

ANGARA
SOC

Виктория Варламова

Руководитель отдела защиты бренда

OPEN SOURCE INTELLIGENCE

OSINT – сбор и анализ информации из открытых источников

ЗАЩИТА БРЕНДА

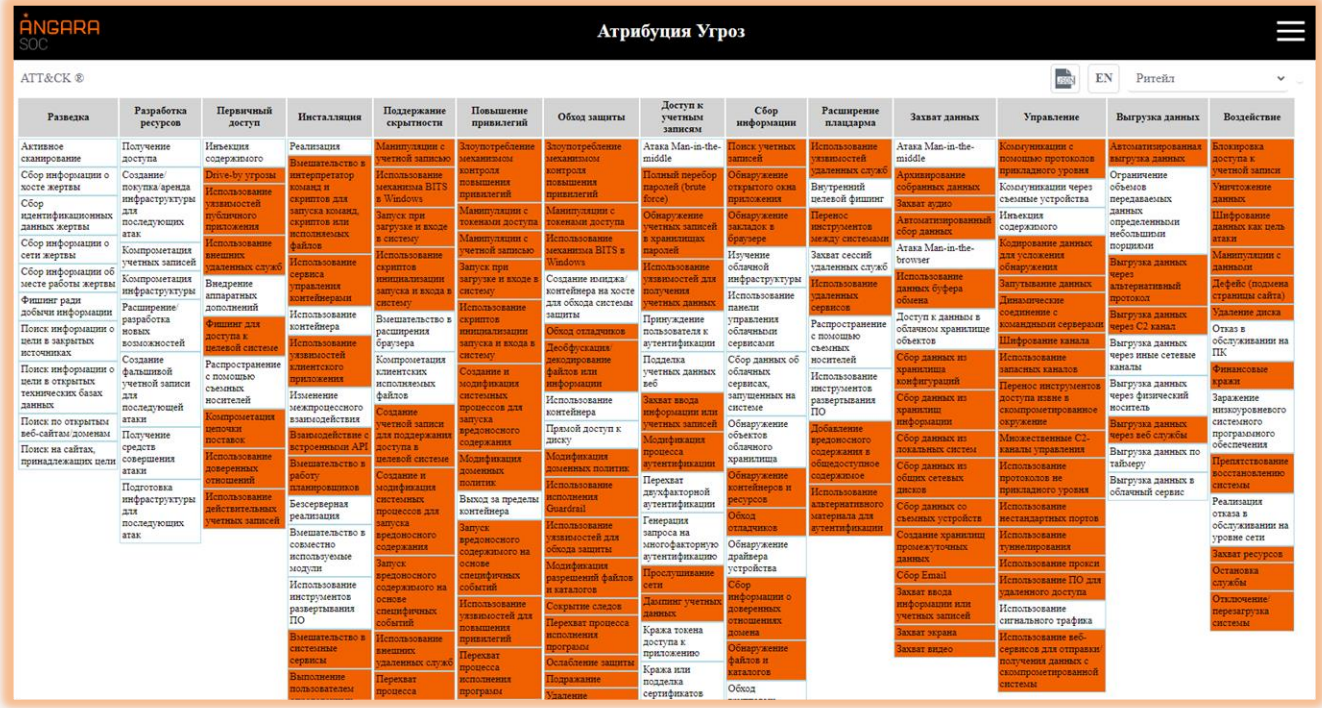
Цель защиты бренда – предупредить и минимизировать репутационные и финансовые потери компании

DFIR* + OSINT

*Digital Forensics and Incident Response
Цифровая криминалистика и реагирование на инциденты

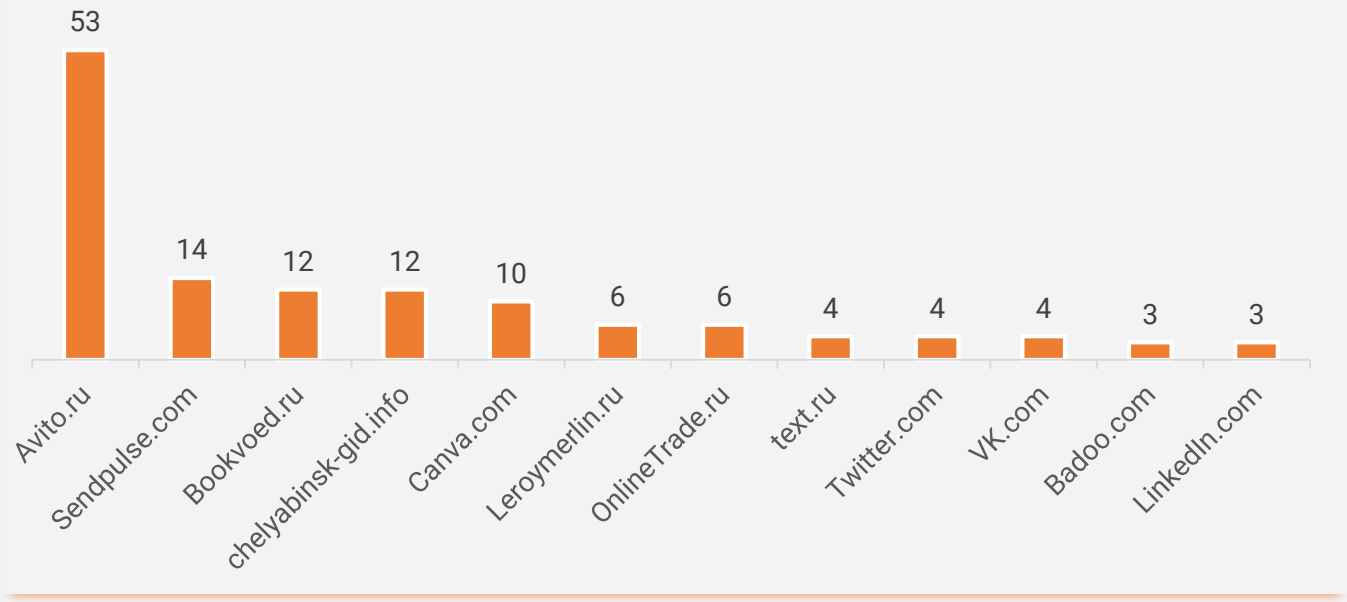
OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

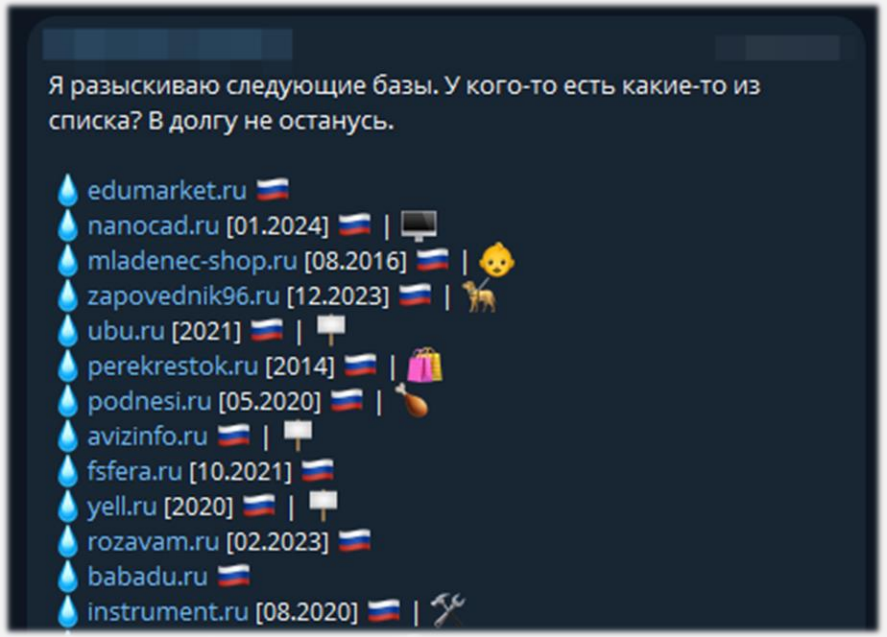
- Разведка
- Вооружение
- Доставка
- Заражение
- Установка
- Управление и контроль
- Выполнение действий



OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Разведка	Вооружение	Доставка и Заражение
T1589 Сбор идентификационных данных жертвы (учетные данные)		T1078 Использование действительных учетных записей (доменный аккаунт)





OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

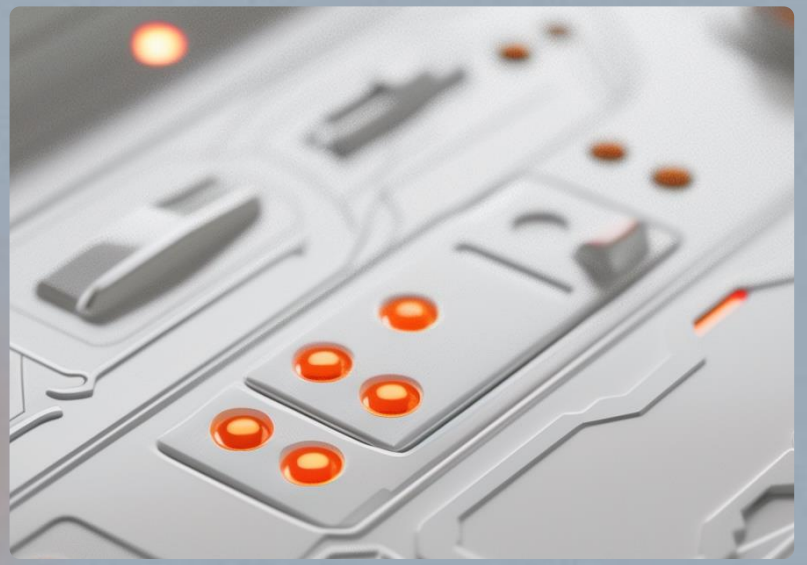
Разведка

T1593 Поиск по открытым веб-сайтам/доменам

OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Разведка или Вооружение

T1583 Покупка/аренда инфраструктуры (домен)



wildberries-wb.com
wildberries-zakup.com
wildberries-ru.com
wildberries-server.com
bankwildberries.com
wildberriesbank.com

wildberries.ru

aliexpress.ru

www-aliexpress.ru
wwwaliexpress.ru
aliexpresser.ru
aliexpressgroup.ru
aliexpresshop.ru
aliexpress-markets.com
russians-aliexpress.ru

OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Разведка

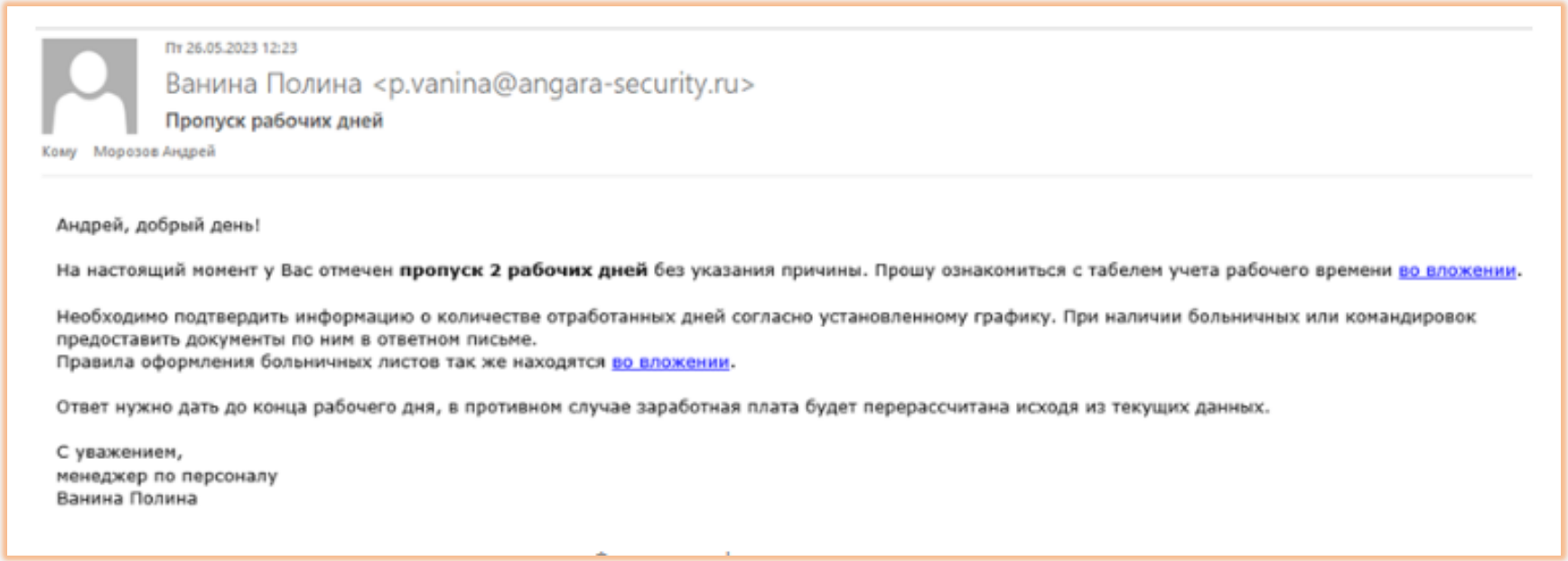
T1589 Сбор идентификационных данных жертвы (эл адреса, ФИО)

Вооружение

T1583 Покупка/аренда инфраструктуры (домен)

Доставка

T1583 Фишинг



Пт 26.05.2023 12:23

Ванина Полина <p.vanina@angara-security.ru>

Пропуск рабочих дней

Кому Морозов Андрей

Андрей, добрый день!

На настоящий момент у Вас отмечен **пропуск 2 рабочих дней** без указания причины. Прошу ознакомиться с табелем учета рабочего времени во вложении.

Необходимо подтвердить информацию о количестве отработанных дней согласно установленному графику. При наличии больничных или командировок предоставить документы по ним в ответном письме.
Правила оформления больничных листов так же находятся во вложении.

Ответ нужно дать до конца рабочего дня, в противном случае заработная плата будет перерассчитана исходя из текущих данных.

С уважением,
менеджер по персоналу
Ванина Полина

Разведка

Сбор эл. адресов из утечки

Вооружение

Покупка домена angara-security.ru

Доставка

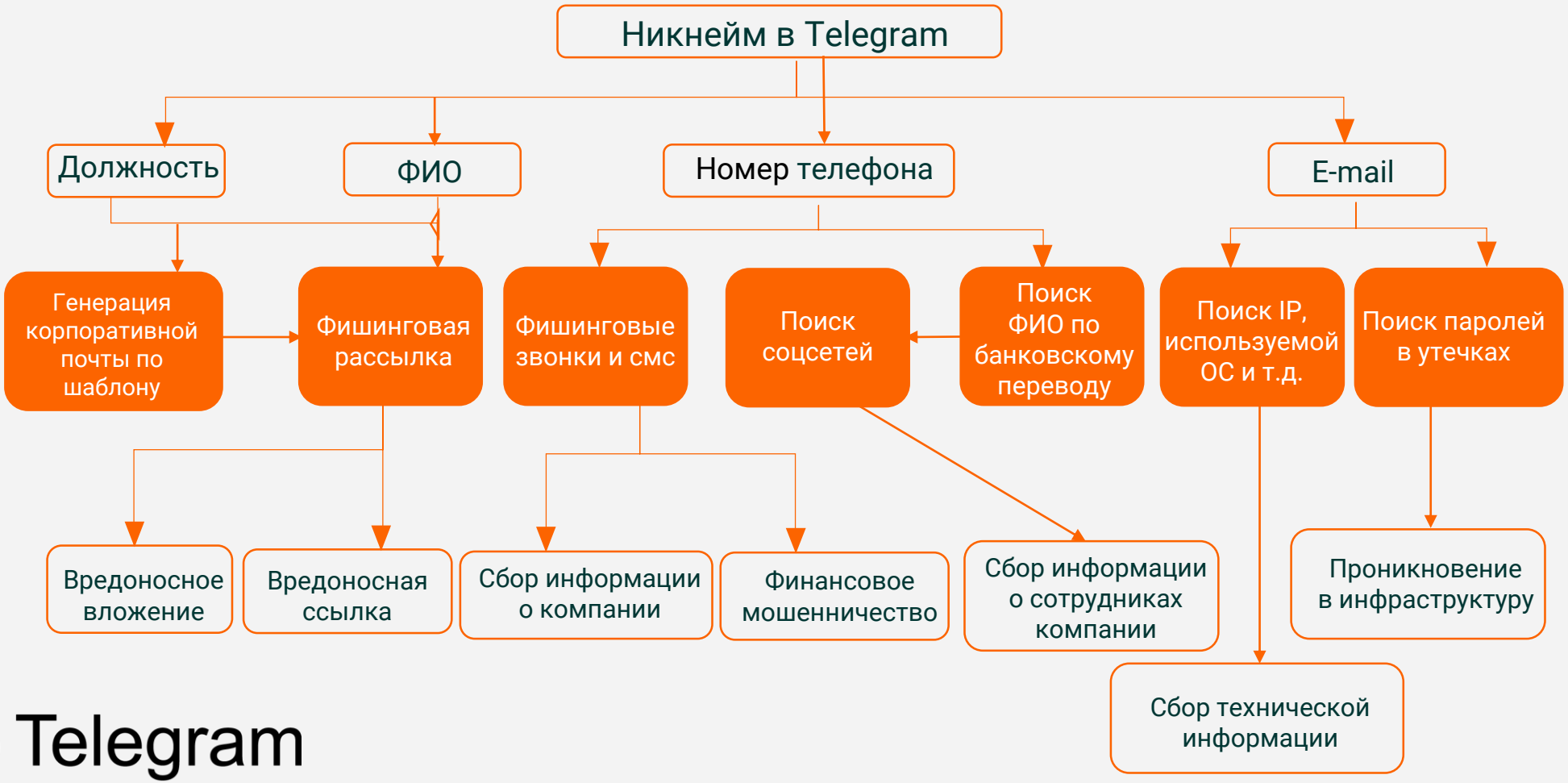
Почтовый фишинг

OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Разведка	Вооружение	Доставка
T1589 Сбор идентификационных данных жертвы (номер телефона)		T1583 Фишинг(вложение или ссылка)
T1598 Фишинг для добычи информации		

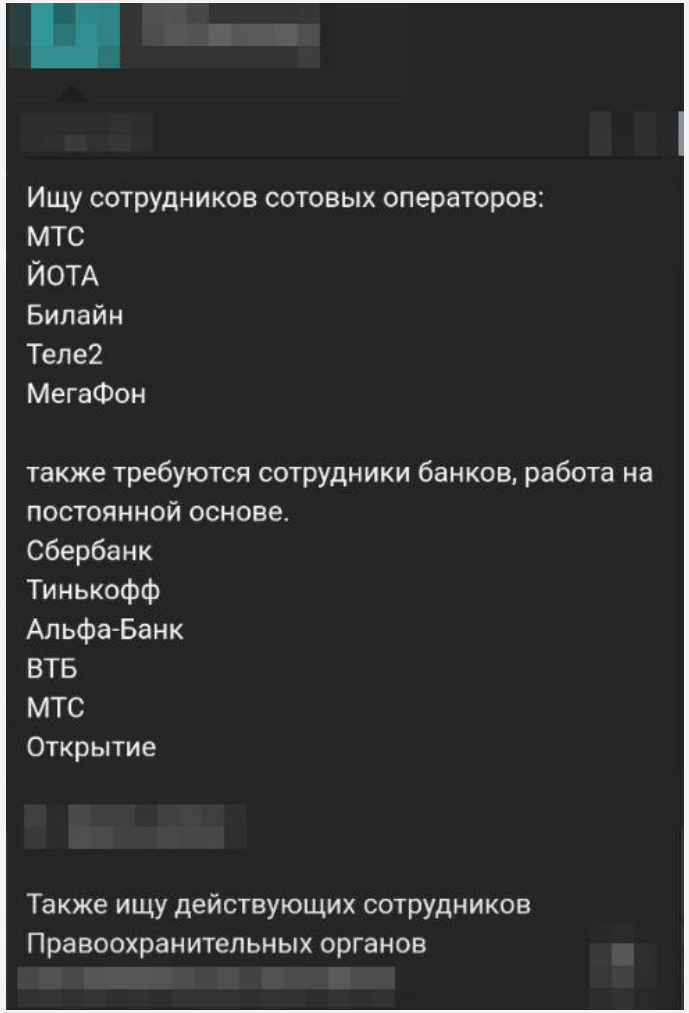
Telegram

OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ



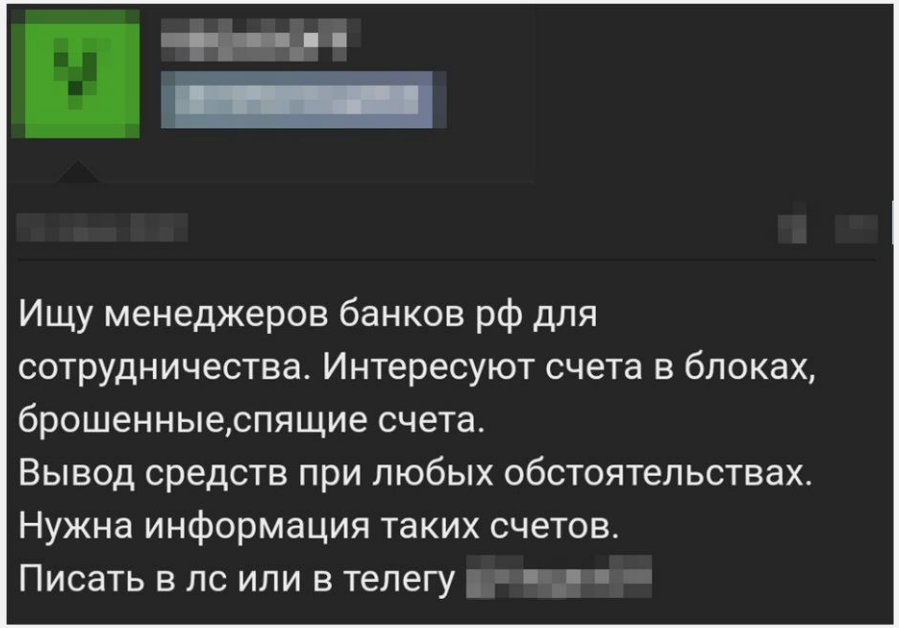
Telegram

OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ



Разведка

T1589 Поиск информации о цели в закрытых источниках

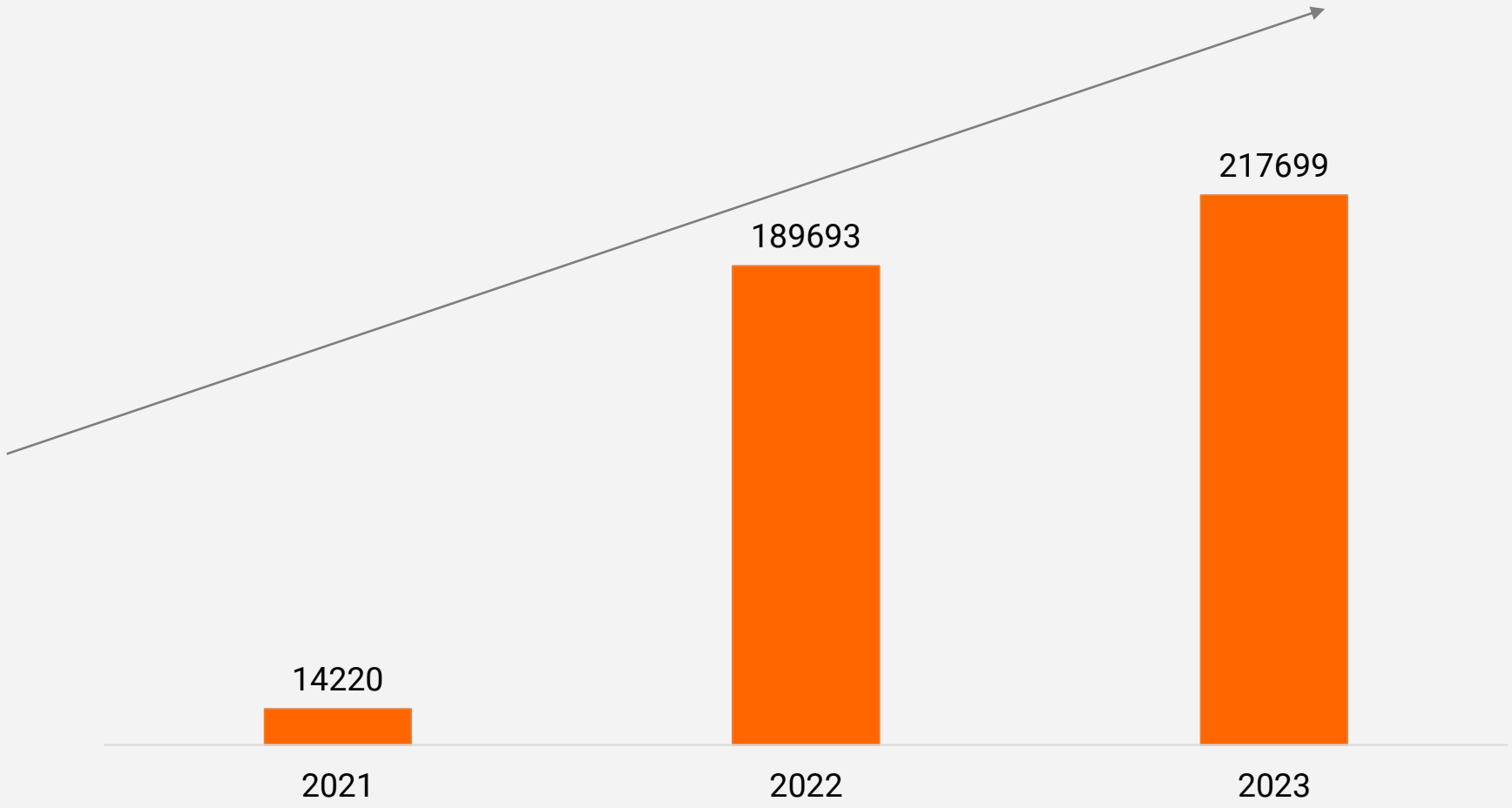


OSINT В РАМКАХ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Результат работы экспертов формируется в отчет, который содержит

- ✓ Перечень скомпрометированных учетных данных
- ✓ Список сайтов и веб-страниц, представляющих собой подделку официальных ресурсов Заказчика
- ✓ Список доступных веб-ресурсов Заказчика
- ✓ Чувствительные данные Заказчика, содержащиеся в открытом доступе
- ✓ Предложения о покупке/продаже данных Заказчика

КОЛИЧЕСТВО ЗАПРОСОВ ПО ТЕМЕ OSINT



ANGARA
SOC

СПАСИБО ЗА ВНИМАНИЕ!

+7 495 269-26-06

www.angarasecurity.ru