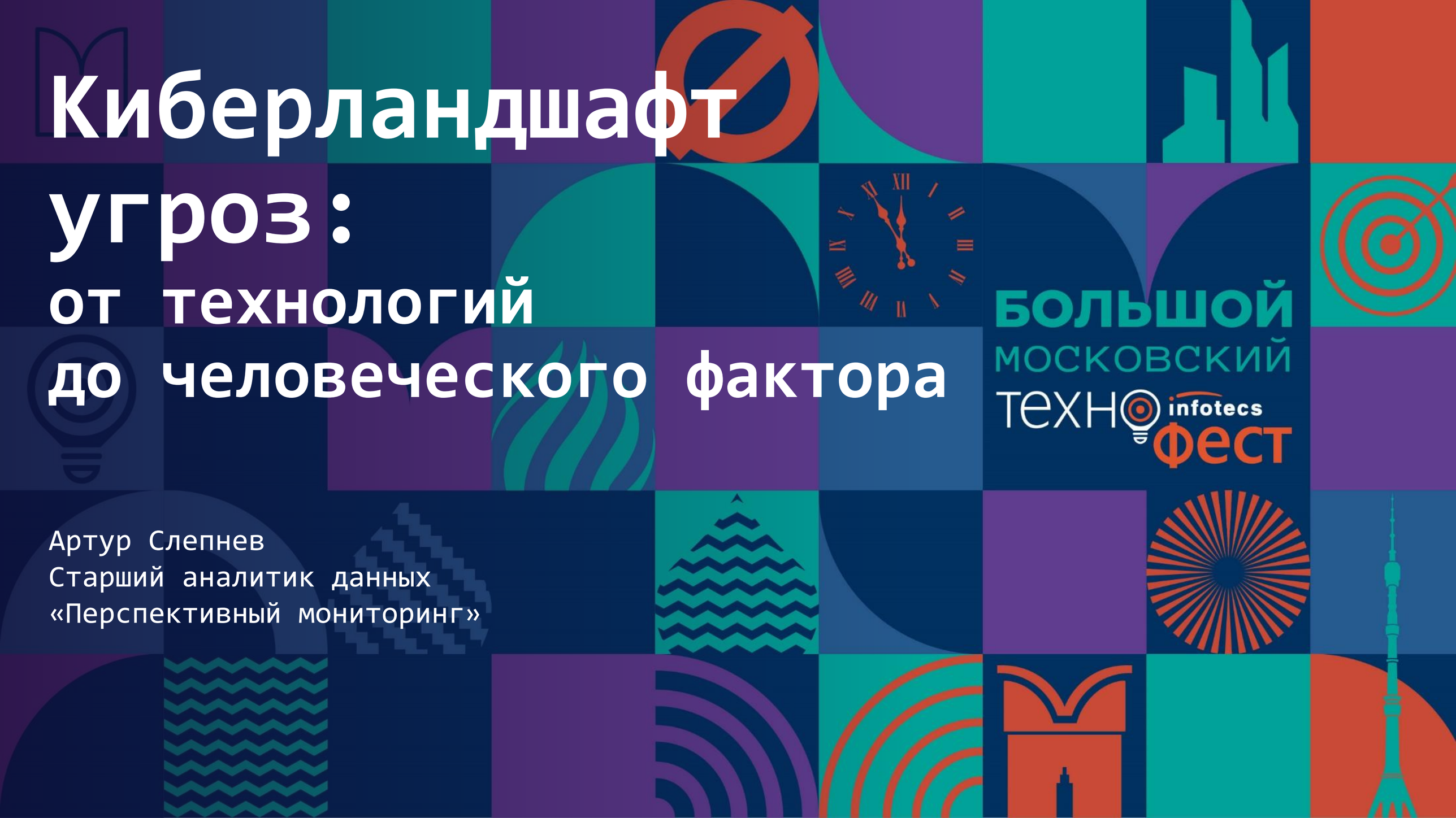
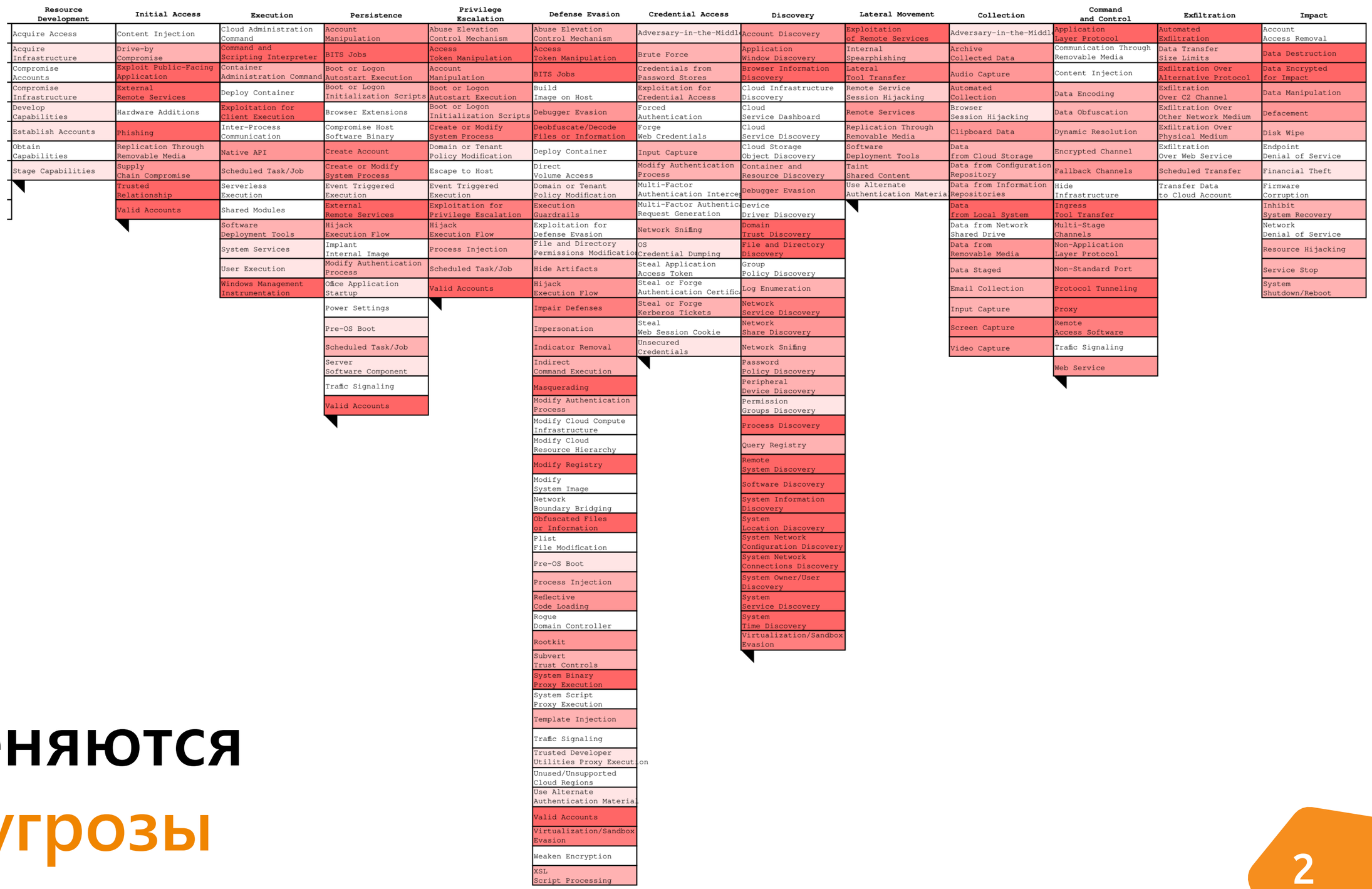
Киберландшафт угроз:
от технологий до человеческого фактора



Артур Слепнев
Старший аналитик данных
«Перспективный мониторинг»



Как меняются киберугрозы

Цифровая среда 2025: новые возможности - новые риски

Рост цифровой зависимости

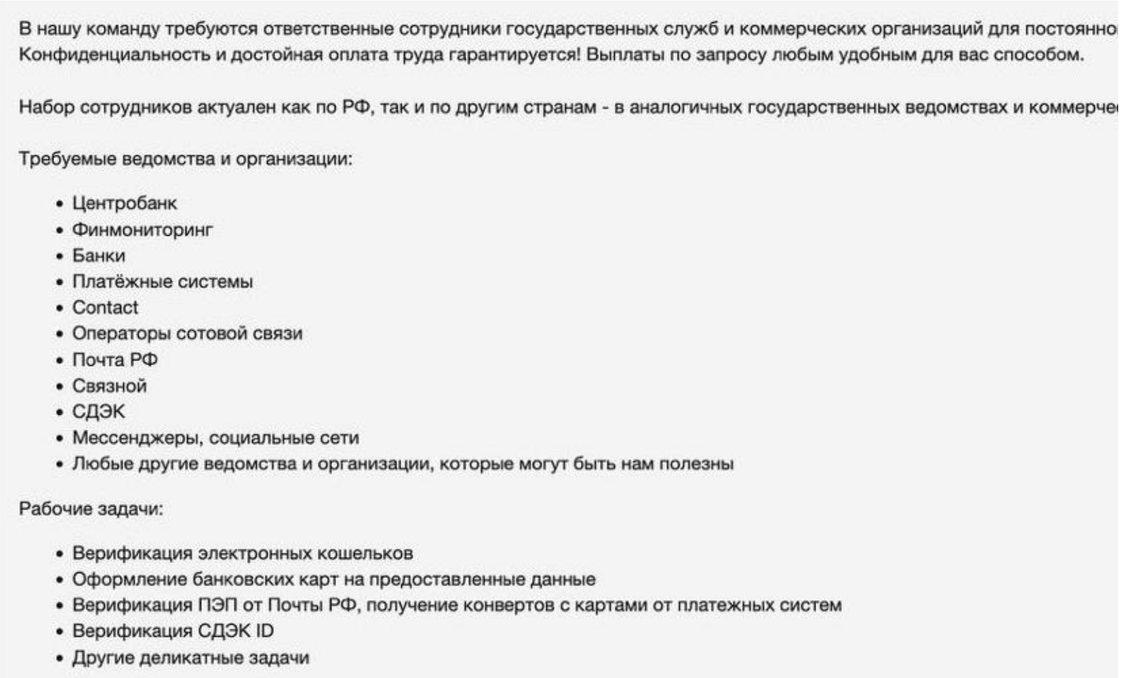
Увеличение атакуемой поверхности

Массовое внедрение ИИ

Экономика киберпреступности

Главные тренды 2025

Экономика утечек



В нашу команду требуются ответственные сотрудники государственных служб и коммерческих организаций для постоянно
Конфиденциальность и достойная оплата труда гарантируется! Выплаты по запросу любым удобным для вас способом.

Набор сотрудников актуален как по РФ, так и по другим странам - в аналогичных государственных ведомствах и коммерче

Требуемые ведомства и организации:

- Центробанк
- Финмониторинг
- Банки
- Платёжные системы
- Contact
- Операторы сотовой связи
- Почта РФ
- Связной
- СДЭК
- Мессенджеры, социальные сети
- Любые другие ведомства и организации, которые могут быть нам полезны

Рабочие задачи:

- Верификация электронных кошельков
- Оформление банковских карт на предоставленные данные
- Верификация ПЭП от Почты РФ, получение конвертов с картами от платежных систем
- Верификация СДЭК ID
- Другие деликатные задачи

H1
2025

40%

рост предложений по продаже корп.учеток, доступов

Главные тренды 2025

Атаки на API, интеграции,
цепочки поставок

H1
2025

80%

ИИ в киберугрозах

Рост атак с использованием голосовой связи (вишинг):

H1
2025

80%

вишинг (с прим. ИИ)
Составляет 60% от
всех фиш. атак

ИИ в киберугрозах

ИИ и фишинг

H1
2025
>80% писем
сгенерировано ИИ

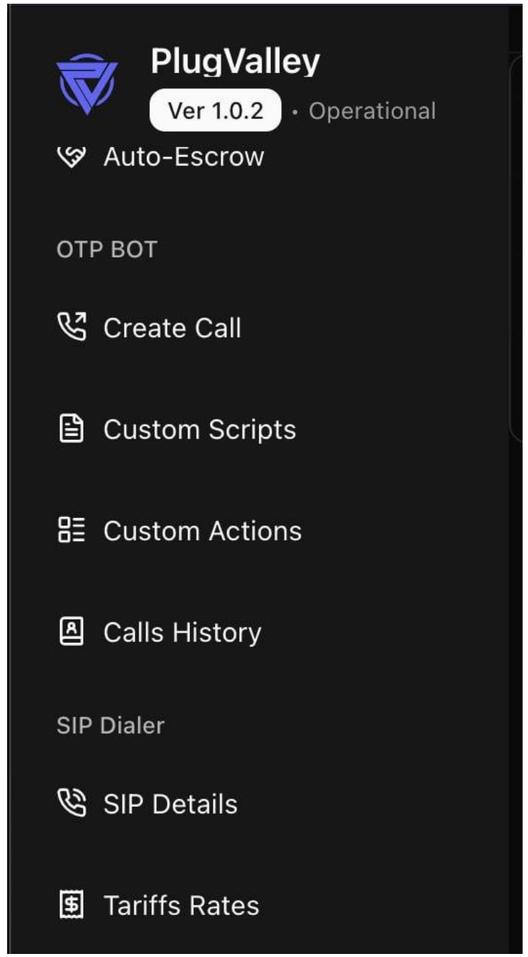
Главные тренды 2025

Crime-as-a-Service или
Фишинг/вишинг/Ransomware по подписке

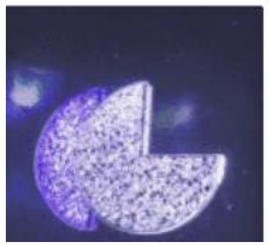
Фишинг-платежка CC+3DS Stripe 🔒: Перехват данных карт и SMS от банков.
27 языков 🌍, включая арабский.
Абузоустойчивый сервер + домен и SSL 🛡️.
Гайд по созданию шопов 📝.
Пассивный доход 💰: Постоянный материал CC+3DS из любых стран.

Что входит? 📦

Скрипт для фишинга CC+3DS ⚙️.
Инструкция по настройке шопа и платежки 💳.
Гайд по SEO и продвижению (Google, FB, Reddit) 📈.
SEO и бесплатный трафик: Оптимизация + вбив баланса Google Ads 🚦.
Поддержка 24/7 🤝.



Местный



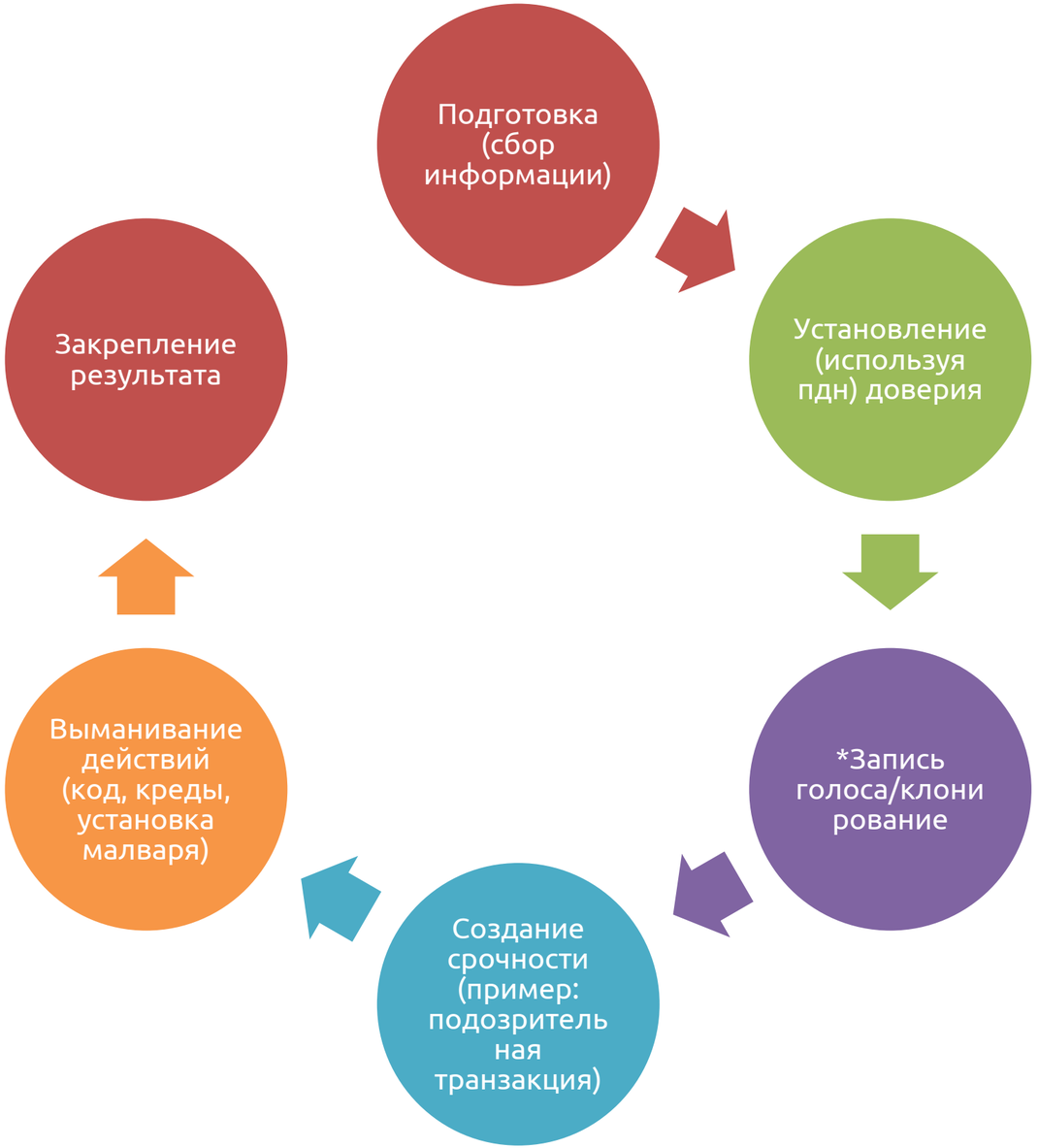
Фишинг & Дрейнер
Автоматическая система фишинга!
Клоакинг, уникализация дизайнов полный контроль!
Фишинг - 100+ дизайнов - полная отчетность! Наша система автоматически проверяет данные и присылает скрины с TrustWallet и SafePal.
Дрейнер Solana - человек апрувает все монетки - у каждого работника свой и бот и полная отчетность!
Дрейнер ETH - автоматически снимает основную монету
Drainer через смарт контракт
Автоматически выводит либо монету ETH, либо токены , либо NFT. Выводит в зависимости от того, что стоит дороже.

Главные тренды 2025

Первоначальный доступ

H1
2025
35% human first

Сценарий вишинга



Главные тренды 2025

Эволюция защиты

Zero Trust, AI-SOC, Darknet Monitoring

Наше решение

Для выявления подделки голоса в аудиозаписях, была разработана AI модель, которая способна распознавать даже последние решения ИИ и из совокупности различных факторов предоставляет аналитический вывод

```
(voice_venv) C:\work\SystemBRP\TMP_BRP\VoiceFake\voice>python "voice_test – копия.py" real\real_voice1.flac
Сырые признаки:
 {'MFCC_mean': array([-446.64307  ,  106.38964  ,   19.33801  ,   23.989317 ,
         11.020493 ,    9.585844 ,    2.1750026,    8.92336  ,
          3.6278095,    1.699804 ,    3.3694386,   -3.546823 ,
         -5.2146134], dtype=float32), 'Spectral_flatness': 0.0007109302678145468, 'Pitch_mean': 1318.2384033203125,
         'Pitch_variance': 1205898.375, 'Jitter': 0.030560575917880493, 'Shimmer': 0.1285684739291407}

Статичный вердикт: Живой голос (вероятность: 50.0%)
LLM вердикт: Синтетический голос (вероятность синтетичности: 22.7%)
```

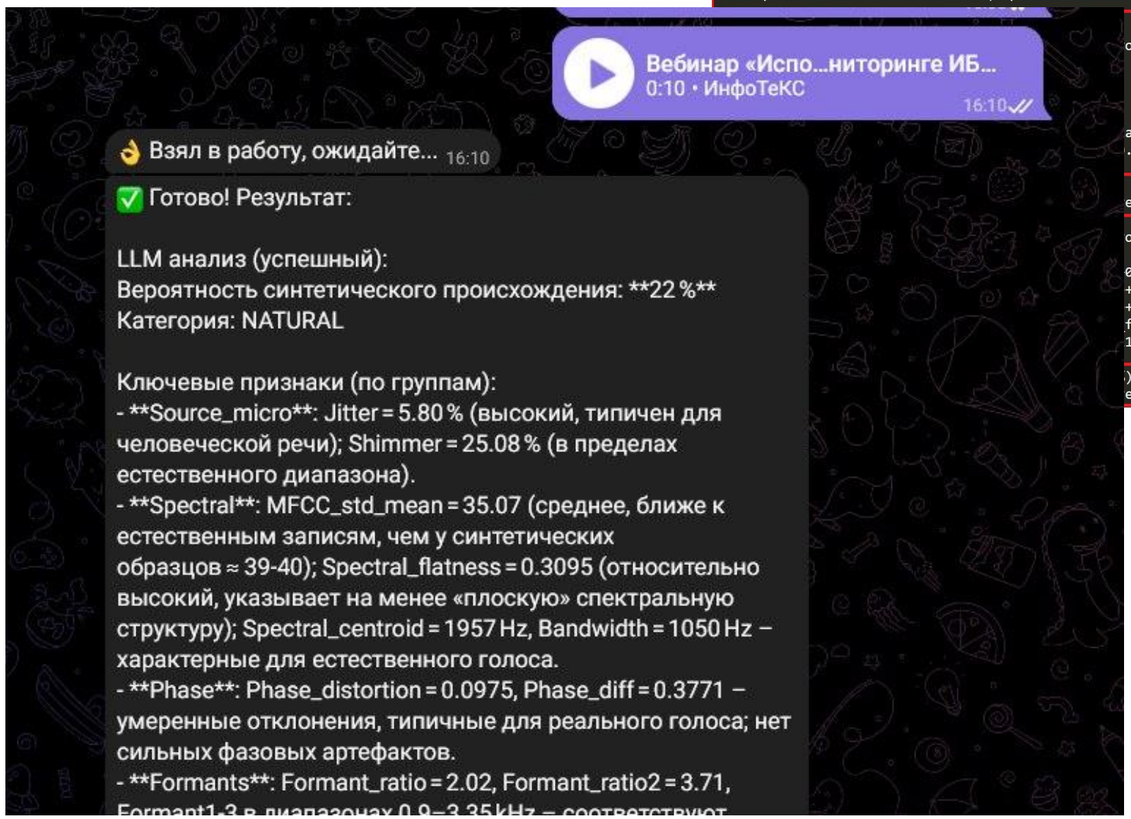
Реальные голоса

```
(voice_venv) C:\work\SystemBRP\TMP_BRP\VoiceFake\voice>python "voice_test – копия.py" real\real_voice2.flac
Сырые признаки:
 {'MFCC_mean': array([-578.93365  ,  132.35172  ,   17.10791  ,   19.597387 ,
          8.60741  ,    6.493033 ,   -3.447291 ,   10.594808 ,
          5.2864237,    4.694693 ,    5.0526986,   -4.212876 ,
         -4.5344515], dtype=float32), 'Spectral_flatness': 0.0013062956277281046, 'Pitch_mean': 1376.008056640625,
         'Pitch_variance': 1212143.0, 'Jitter': 0.03429694496673103, 'Shimmer': 0.12410853760800312}

Статичный вердикт: Живой голос (вероятность: 50.0%)
LLM вердикт: Синтетический голос (вероятность синтетичности: 1.0%).
```

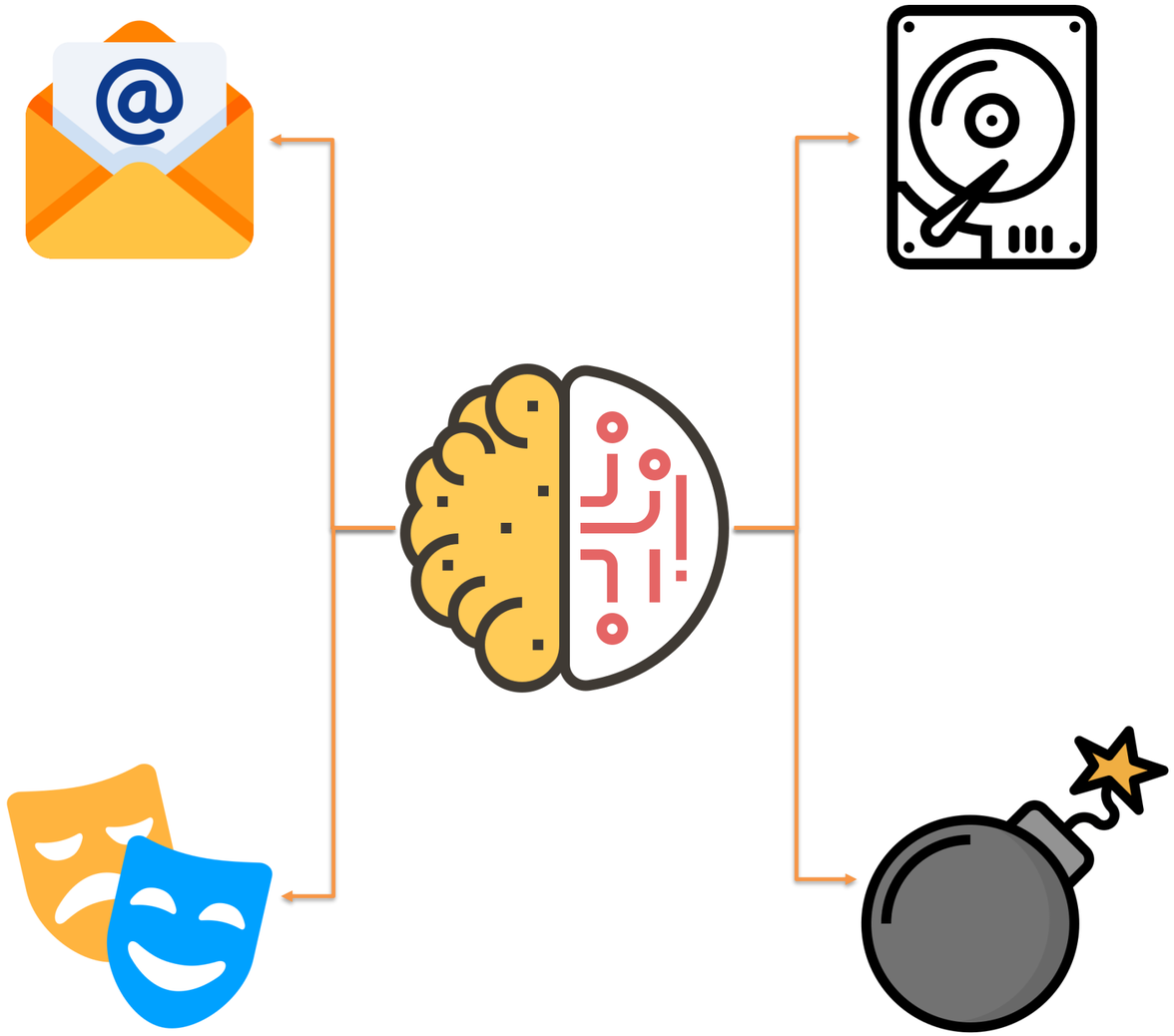
```
(voice_venv) C:\work\SystemBRP\TMP_BRP\VoiceFake\voice>python "voice_test – копия.py" fake\fake_voice1.wav
Сырые признаки:
 {'MFCC_mean': array([-371.31668  ,  121.61343  ,   22.504404 ,   22.940685 ,
          6.1270304,    1.9572675,    0.6880992,   11.041117 ,
         -2.3596015,    2.4301376,   -4.66303  ,   -6.390747 ,
         -4.055937 ], dtype=float32), 'Spectral_flatness': 0.01208010595291853, 'Pitch_mean': 1360.706787109375,
         'Pitch_variance': 1276062.625, 'Jitter': 0.014520480027312105, 'Shimmer': 0.09340188093282513}

Статичный вердикт: Живой голос (вероятность: 33.3%)
LLM вердикт: Синтетический голос (вероятность синтетичности: 0.2%).
```

```
oice>python "voice_test – копия.py" fake\fake_voice2.1.wav

   8.554639 ,   34.510174 ,
 -0.9689663,
 -2.9611812,
atness': 0.01772473193705082, 'Pitch_mean': 1425.8692626953125,
.022001601329303264, 'Shimmer': 0.10405541299986218}

етичности: **85%**)
```

```
oice>python "voice_test – копия.py" fake\fake_voice2.2.wav

02,  9.6229630e+00,  2.2763191e+01,
+00,  1.4775324e+00,
+00, -3.0713734e-01,
flatness': 0.13301701843738556, 'Pitch_mean': 1397.1204833984375,
1289465183917992, 'Shimmer': 0.09715879633300731}

)
етичности: 94.0%).
```



ИИ в киберугрозах



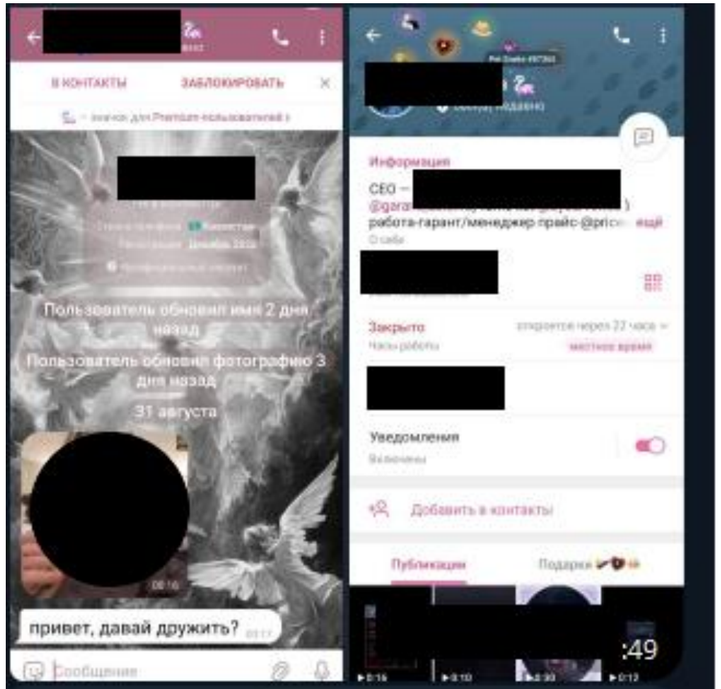
Дети. Статистика

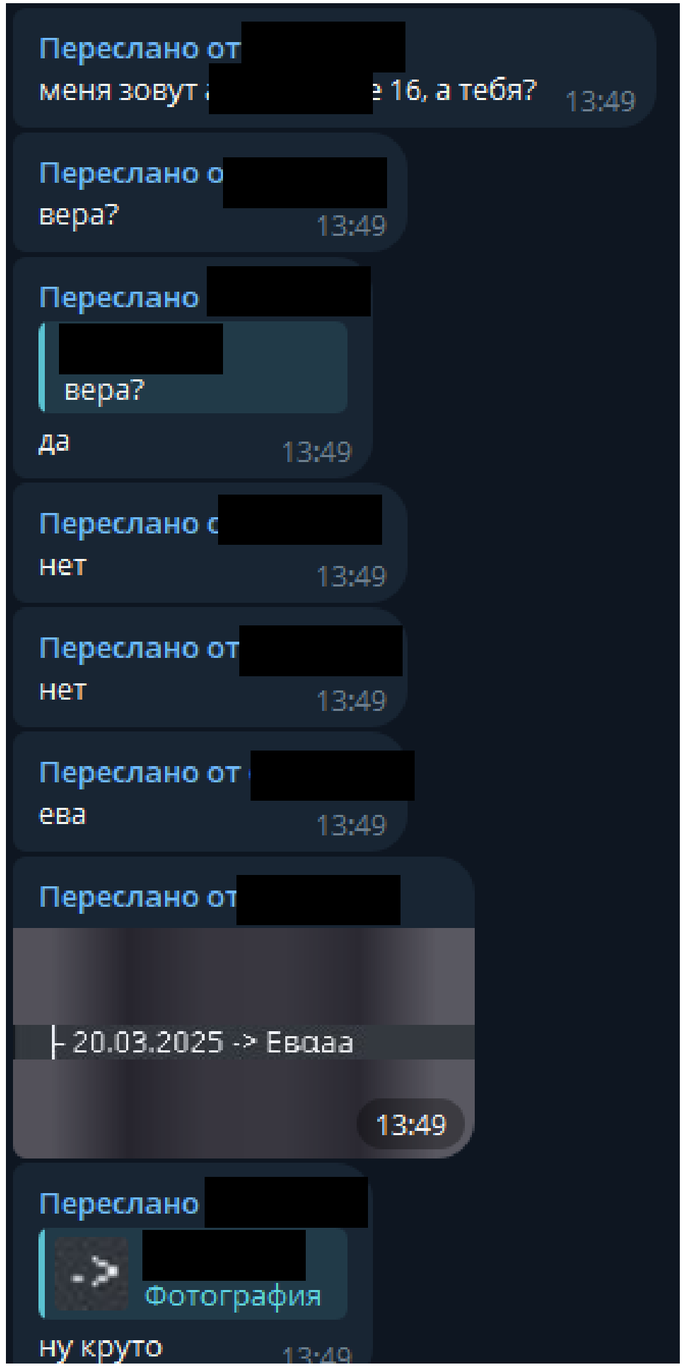
Пострадавших несовершеннолетних
от кибермошенников

H1
2025

+25%*

***по данным МВД**


В КОНТАКТЫ
ЗАБЛОКИРОВАТЬ
Пользователь обновил имя 2 дня назад
Пользователь обновил фотографию 3 дня назад
31 августа
привет, давай дружить?
Информация
Закрыто
Уведомления
Добавить в контакты
Публикации
Подарки
:49
Переслано от @
osint-это цифровая разведка по отрытым источникам, так что
13:49
Переслано от @u
если я найду твои данные
13:49
Переслано от
то знай
13:49
Переслано от @
что все законно
13:49
Переслано от
ну ты мой проект
13:49

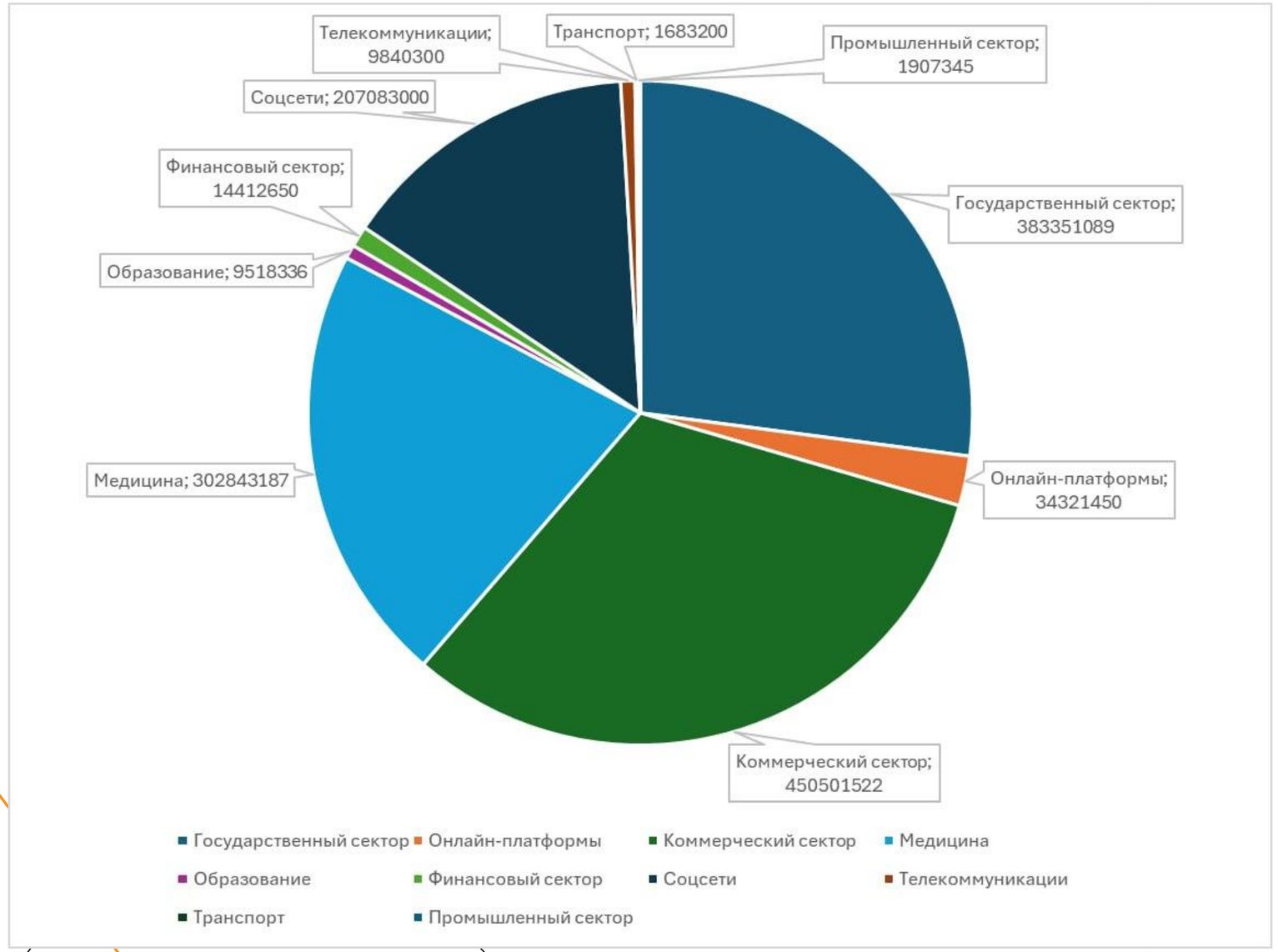

Переслано от
меня зовут
е 16, а тебя?
13:49
Переслано о
вера?
13:49
Переслано
вера?
да
13:49
Переслано с
нет
13:49
Переслано от
нет
13:49
Переслано от
ева
13:49
Переслано от
20.03.2025 -> Евраа
13:49
Переслано
Фотография
ну круто


Переслано
В КОНТАКТЫ
ЗАБЛОКИРОВАТЬ
дней назад
26 августа
пр
телефон
оператор мтс новгород
гоу подарок
на 123
1
2
2...
3
ВЫДАМ КЦ...
гоу подарок
неа
Переслано
Вы
ты кто?
Твой любимый мальчик
[+] Поиск данных...
[+] Страна: Россия, Российская Федерация
[+] Город:
[+] Почтов
[+] Код ва
[+] Телефо
[+] Гос. но
[+] Оператор:

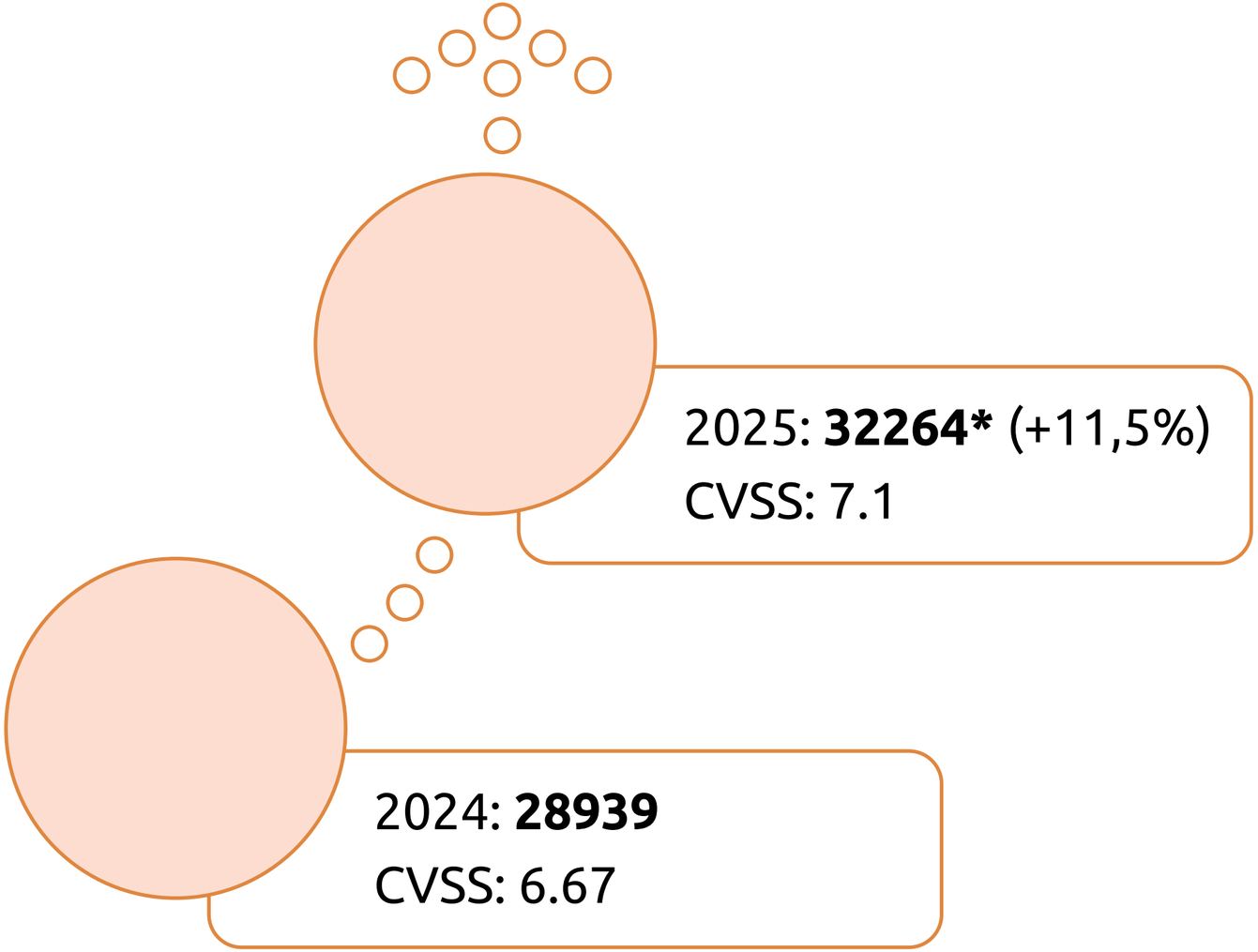

Переслано с
В КОНТАКТЫ
ОТВЕРГНУТЬ
Регистрация Декабрь 2022
Не официальный аккаунт
Пользователь обновил имя 2 дня назад
Пользователь обновил фотографию 3 дня назад
31 августа
здарова
циркуль
0
привет
ты кто
Ммммм .. ещё чая
Переслано от
В КОНТАКТЫ
ЗАБЛОКИРОВАТЬ
Дочь
Дочь
Дочь
Дочь
Дочь
Дочь

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Утечки информации



Как меняются киберугрозы



Инструменты в 2025

Актуализированные вредоносные загрузчики

•**Stealerium**

Анализирует, посещает ли жертва сайт 18+

Распространяется через фишинг и GitHub

•**Lockbit**

Шифровальщик

Автоматическое распространение внутри организации

Партнерская программа

•**Lumma**

Злоупотребление легитимным ПО

•**AutoIt** — используется как интерпретатор для запуска вредоносных скриптов

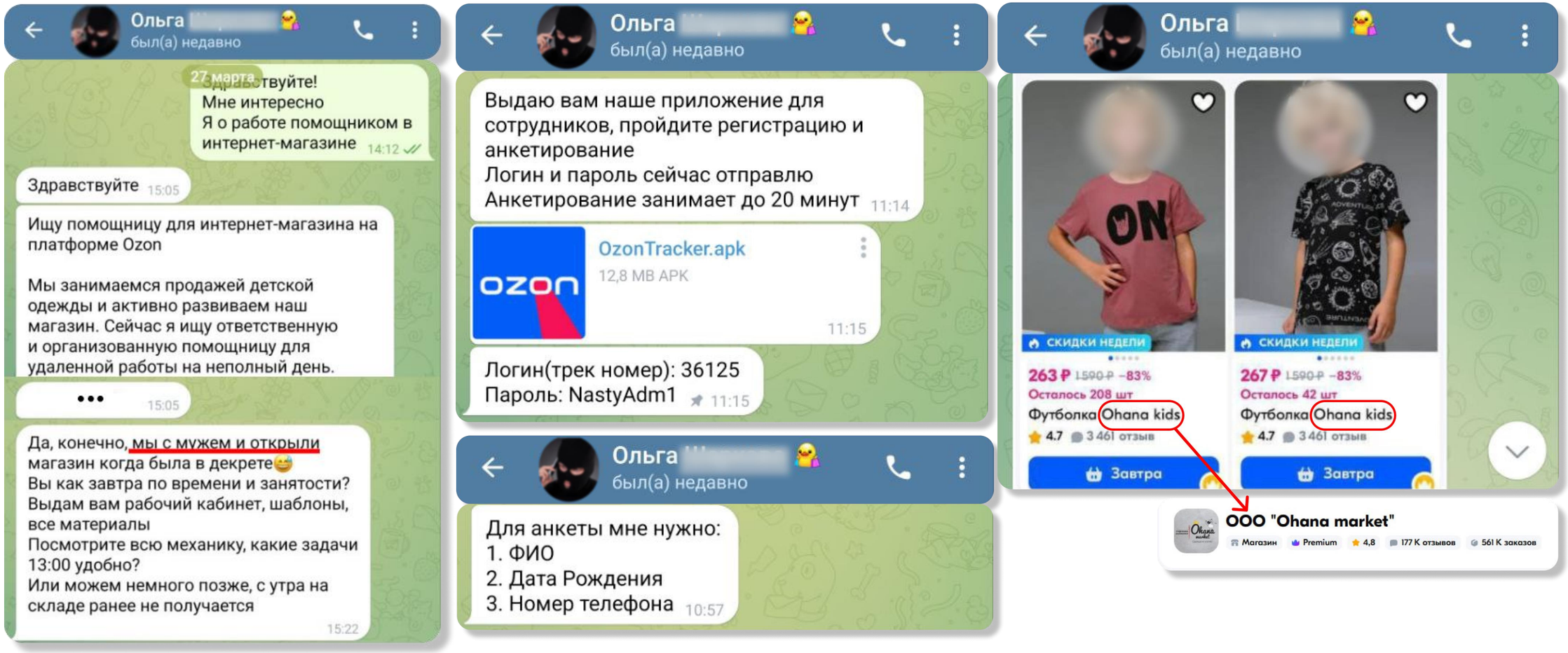
•**UltraVNC / AnyDesk / TeamViewer** — эксплуатируются для скрытого удаленного доступа

•**Forfiles** — применяется в цепочках исполнения вредоносного кода

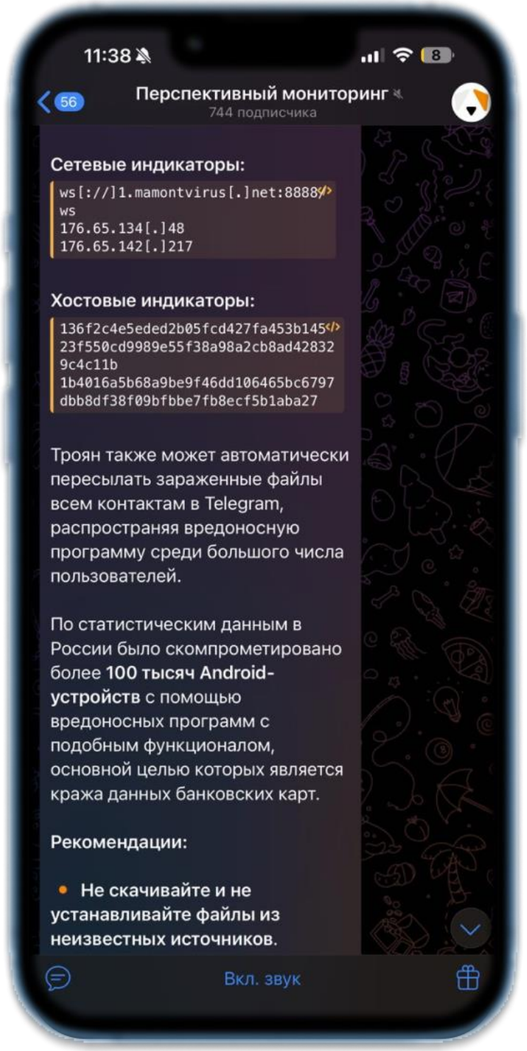
Обход EDR / антивирусов за счёт легитимности файлов

Google Drive использовался для распространения стилеров

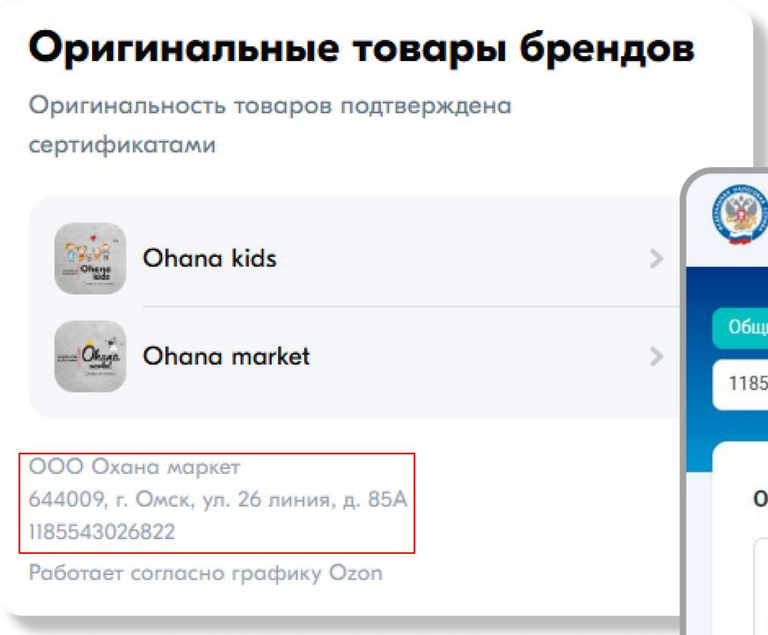
DeliveryRAT

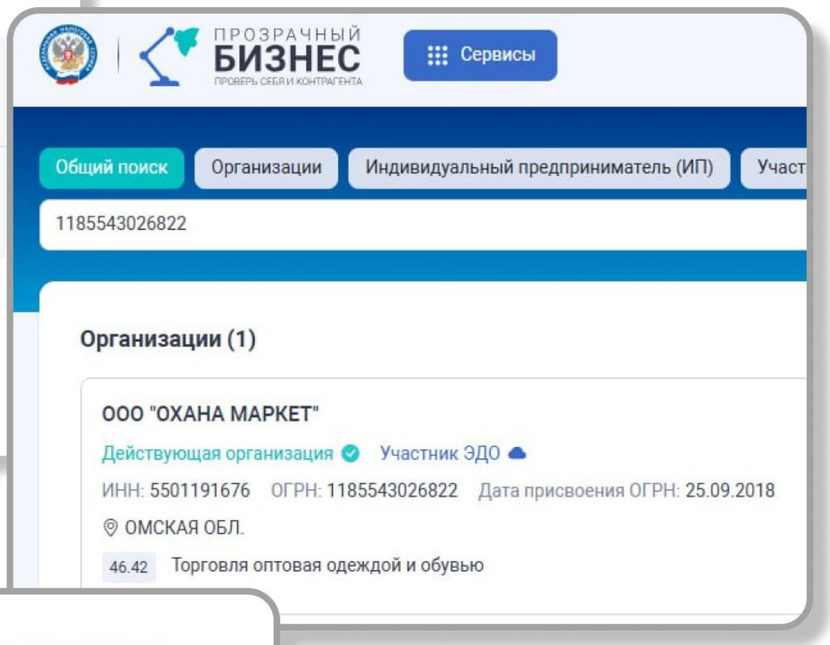


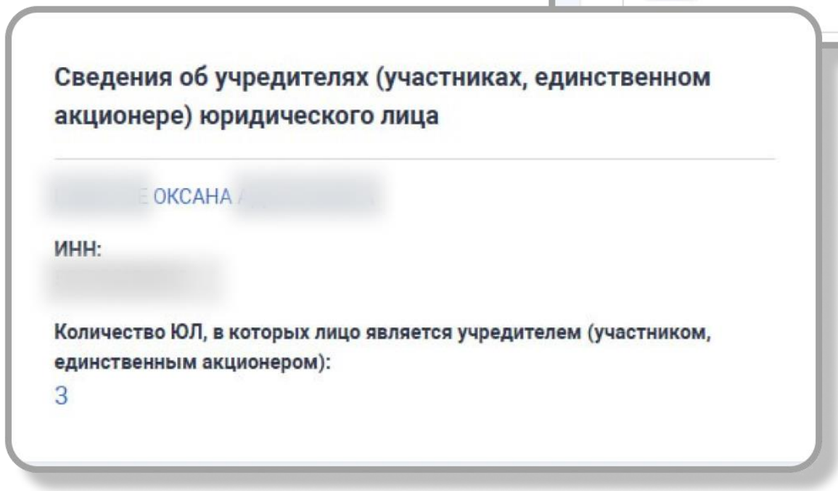
DeliveryRAT



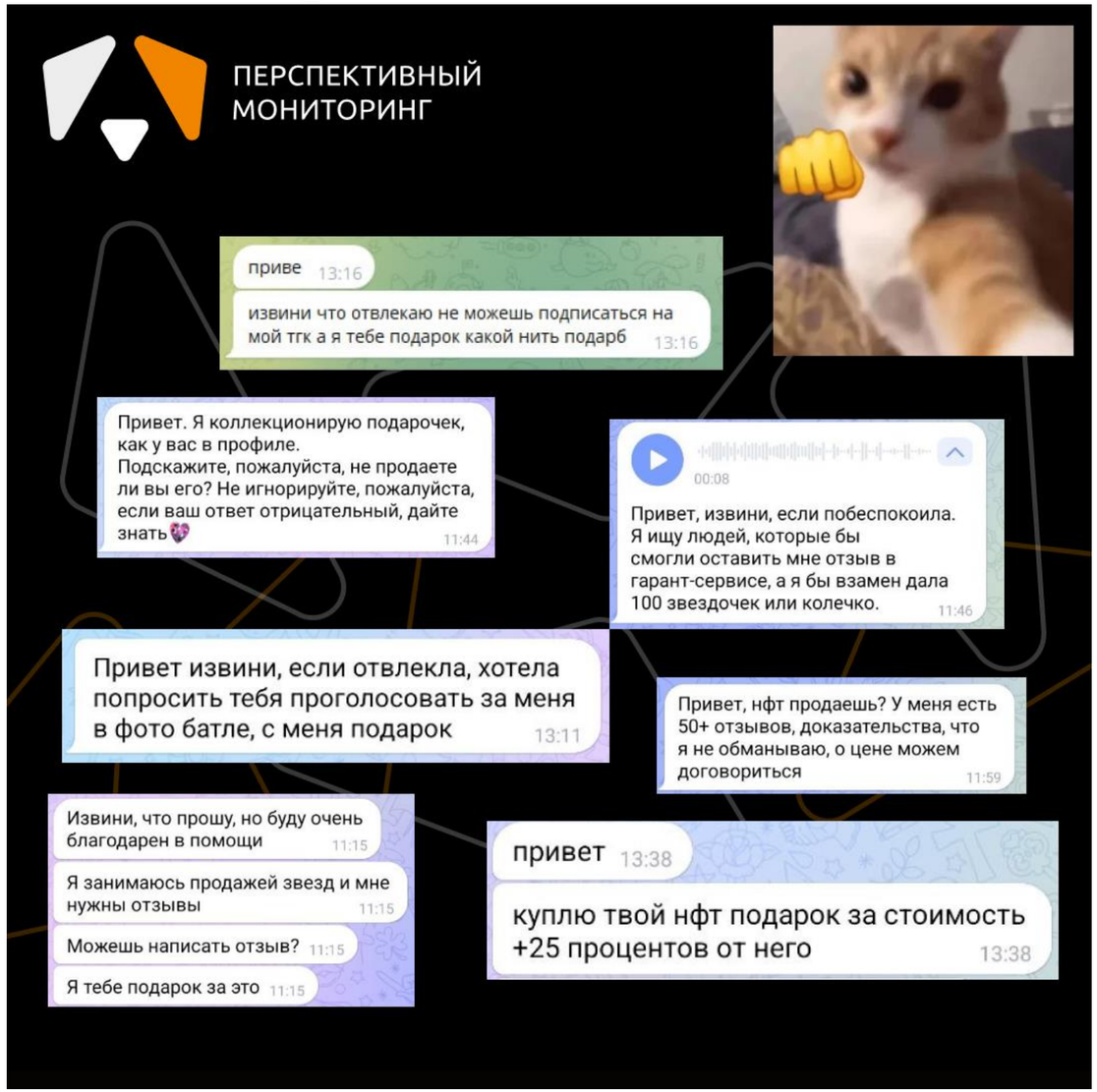
Публикуем идентификаторы компрометации встреченного нами образца ВПО

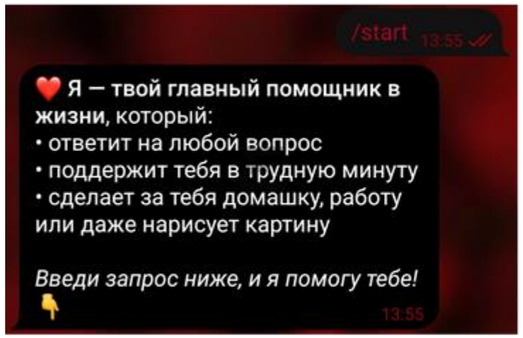


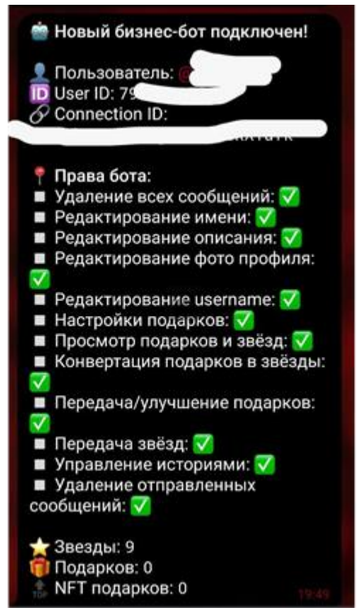




TelegramNFT







TelegramNFT

некоторые методы, необходимые для понимания работы инструментов:

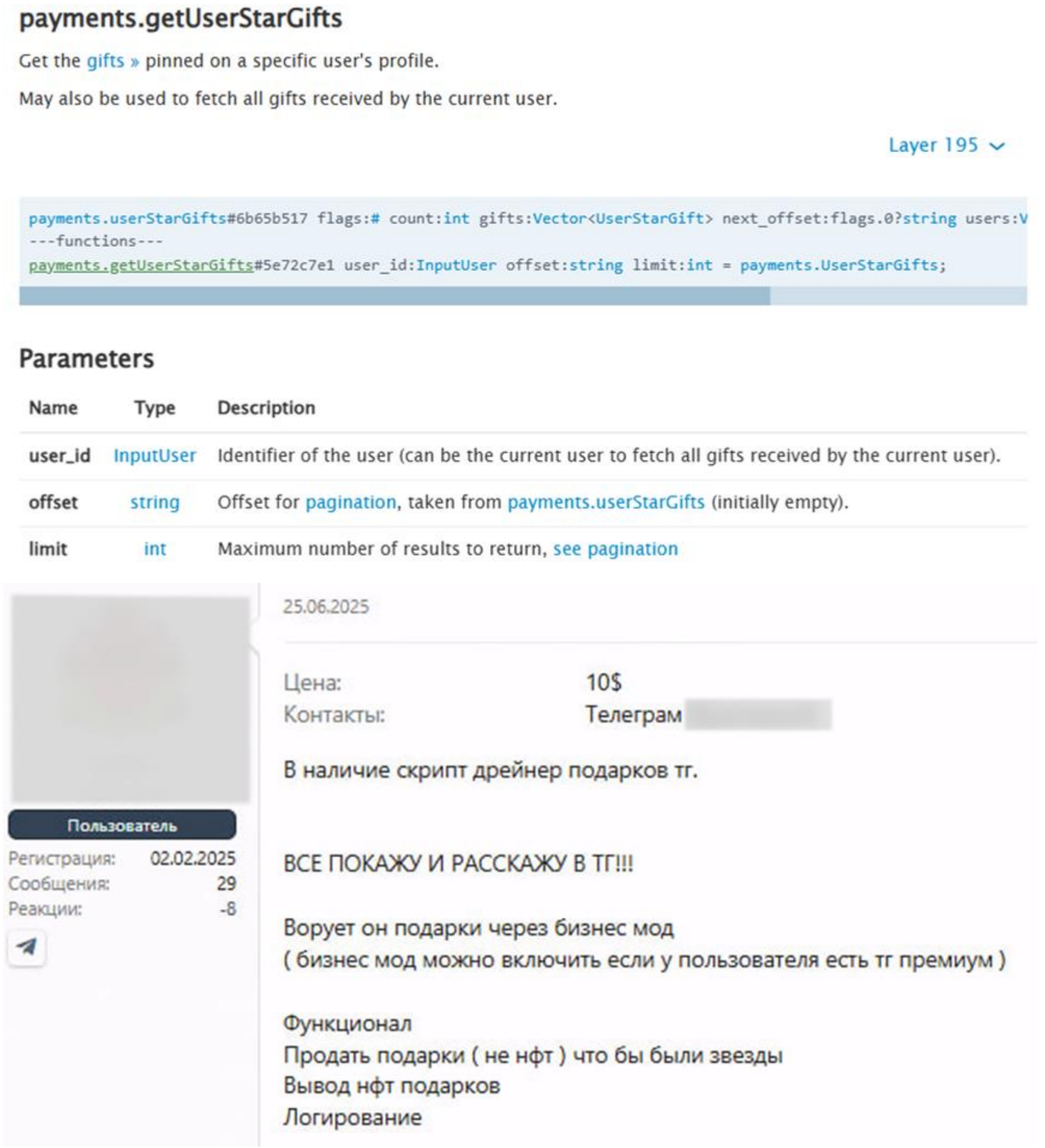
•*BusinessConnection* — описывает связь бота с бизнес-аккаунтом.

•*GetBusinessAccountGifts* — возвращает подарки, полученные и принадлежащие управляемому бизнес-аккаунту;

•*transferBusinessAccountStars* и *GetBusinessAccountStarBalance* — переводит Telegram Stars с баланса бизнес-аккаунта на баланс бота, что позволяет боту проводить транзакции;

•*transferGift* — передаёт принадлежащий владельцу уникальный подарок другому пользователю;

•*convertGiftToStars* и *UpgradeGift* — обеспечивает взаимодействие с подарками, в том числе конвертацию обычных подарков в звёзды или улучшение редких подарков до уникальных.



payments.getUserStarGifts

Get the gifts » pinned on a specific user's profile.

May also be used to fetch all gifts received by the current user.

Layer 195

```
payments.userStarGifts#6b65b517 flags:# count:int gifts:Vector<UserStarGift> next_offset:flags.0?string users:V
---functions---
payments.getUserStarGifts#5e72c7e1 user_id:InputUser offset:string limit:int = payments.UserStarGifts;
```

Parameters

Name	Type	Description
user_id	InputUser	Identifier of the user (can be the current user to fetch all gifts received by the current user).
offset	string	Offset for pagination, taken from payments.userStarGifts (initially empty).
limit	int	Maximum number of results to return, see pagination

25.06.2025

Цена: 10$

Контакты: Телеграм

В наличие скрипт дрейнер подарков тг.

ВСЕ ПОКАЖУ И РАССКАЖУ В ТГ!!!

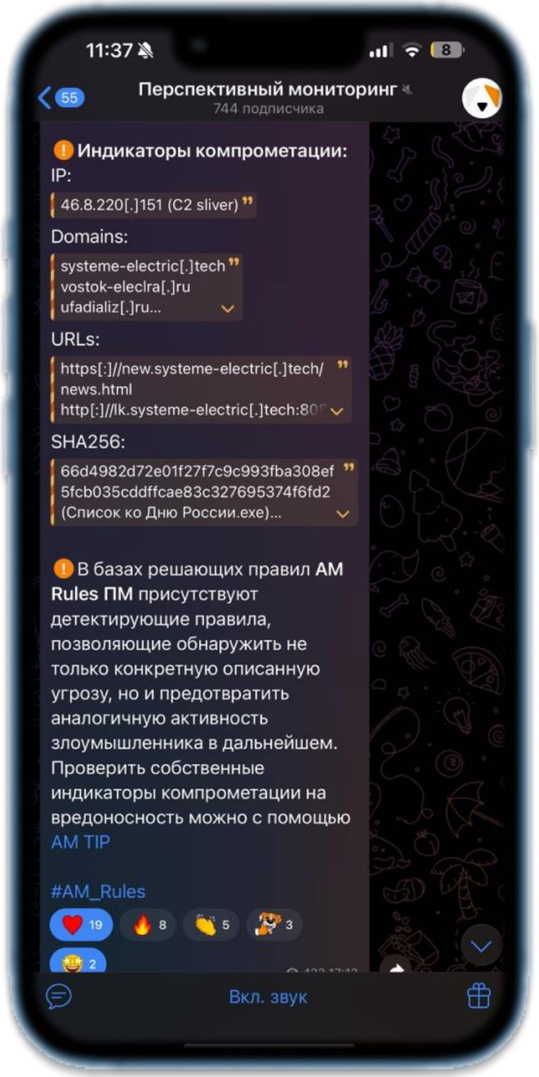
Ворует он подарки через бизнес мод
(бизнес мод можно включить если у пользователя есть тг премиум)

Функционал
Продать подарки (не нфт) что бы были звезды
Вывод нфт подарков
Логирование

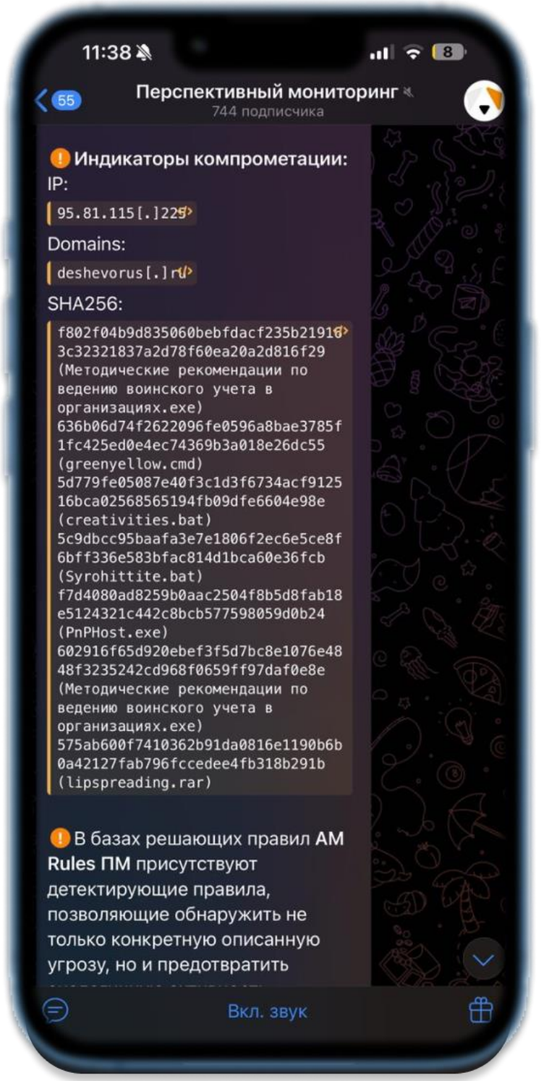
Пользователь

Регистрация: 02.02.2025
Сообщения: 29
Реакции: -8

Наши исследования



Ранее неизвестное ВПО GemoDL



Новые модификации ВПО, связанные с APT-группировкой Core Werewolf

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

@PM_PUBLIC

amonitoring.ru

Слепнев Артур Павлович

Старший аналитик данных

Artur.Slepnev@amonitoring.ru

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA

NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ

GLOBAL DIGITAL SPACE

CISOCLUB

РУТОКЕН КОМПАНИЯ АКТИВ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АВАНГАРД

ARinteg

АТБ ЭЛЕКТРОНИКА

infotecs {/-cademy}

merlion

УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС