

Киберландшафт угроз: от технологий до человеческого фактора

Артур Слепнев
Старший аналитик данных
«Перспективный мониторинг»

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  Фест

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact					
Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal					
Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction					
Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact					
Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation					
Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement					
Establish Accounts	Phishing	Inter-Process Communication	Compromise Host Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe					
Obtain Capabilities	Replication Through Removable Media	Native API	Create Account	Domain or Tenant Policy Modification	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service					
Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create or Modify System Process	Escape to Host	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Scheduled Transfer	Financial Theft					
	Trusted Relationship	Serverless Execution	Event Triggered Execution	Event Triggered Execution	Domain or Tenant Policy Modification	Multi-Factor Authentication Interceptor	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption					
	Valid Accounts	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery					
		Software Deployment Tools	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service					
		System Services	Implant Internal Image	Process Injection	File and Directory Permissions Modification	OS Credential Dumping	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking					
		User Execution	Modify Authentication Process	Scheduled Task/Job	Hide Artifacts	Steal Application Access Token	Group Policy Discovery		Data Staged	Non-Standard Port		Service Stop					
		Windows Management Instrumentation	Office Application Startup	Valid Accounts	Hijack Execution Flow	Steal or Forge Authentication Certificate	Log Enumeration		Email Collection	Protocol Tunneling		System Shutdown/Reboot					
			Power Settings		Impair Defenses	Steal or Forge Kerberos Tickets	Network Service Discovery		Input Capture	Proxy							
			Pre-OS Boot		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Software							
			Scheduled Task/Job		Indicator Removal	Unsecured Credentials	Network Sniffing		Video Capture	Traffic Signaling							
			Server Software Component		Indirect Command Execution		Password Policy Discovery			Web Service							
			Traffic Signaling		Masquerading		Peripheral Device Discovery										
			Valid Accounts		Modify Authentication Process		Permission Groups Discovery										
					Modify Cloud Compute Infrastructure		Process Discovery										
					Modify Cloud Resource Hierarchy		Query Registry										
					Modify Registry		Remote System Discovery										
					Modify System Image		Software Discovery										
					Network Boundary Bridging		System Information Discovery										
					Obfuscated Files or Information		System Location Discovery										
					Plist File Modification		System Network Configuration Discovery										
					Pre-OS Boot		System Network Connections Discovery										
					Process Injection		System Owner/User Discovery										
					Reflective Code Loading		System Service Discovery										
					Rogue Domain Controller		System Time Discovery										
					Rootkit		Virtualization/Sandbox Evasion										
					Subvert Trust Controls												
					System Binary Proxy Execution												
					System Script Proxy Execution												
					Template Injection												
					Traffic Signaling												
					Trusted Developer Utilities Proxy Execution												
					Unused/Unsupported Cloud Regions												
					Use Alternate Authentication Material												
					Valid Accounts												
					Virtualization/Sandbox Evasion												
					Weaken Encryption												
					XSL Script Processing												

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

Средства

<

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

Who know a good caller id spoofing

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 шоп и платежки .

Гайд по SEO и продвижению (Google, FB, Reddit) .

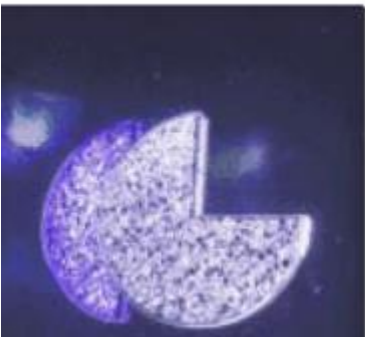
SEO и бесплатный трафик: Оптимизация + вбив баланса Google Ads .

Поддержка 24/7 .



Code Enforcem

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.



PlugValley

Ver 1.0.2 · Operational

Auto-Escrow

OTP BOT

Create Call

Custom Scripts

Custom Actions

Calls History

SIP Dialer

SIP Details

Tariffs Rates



Главные тренды 2025

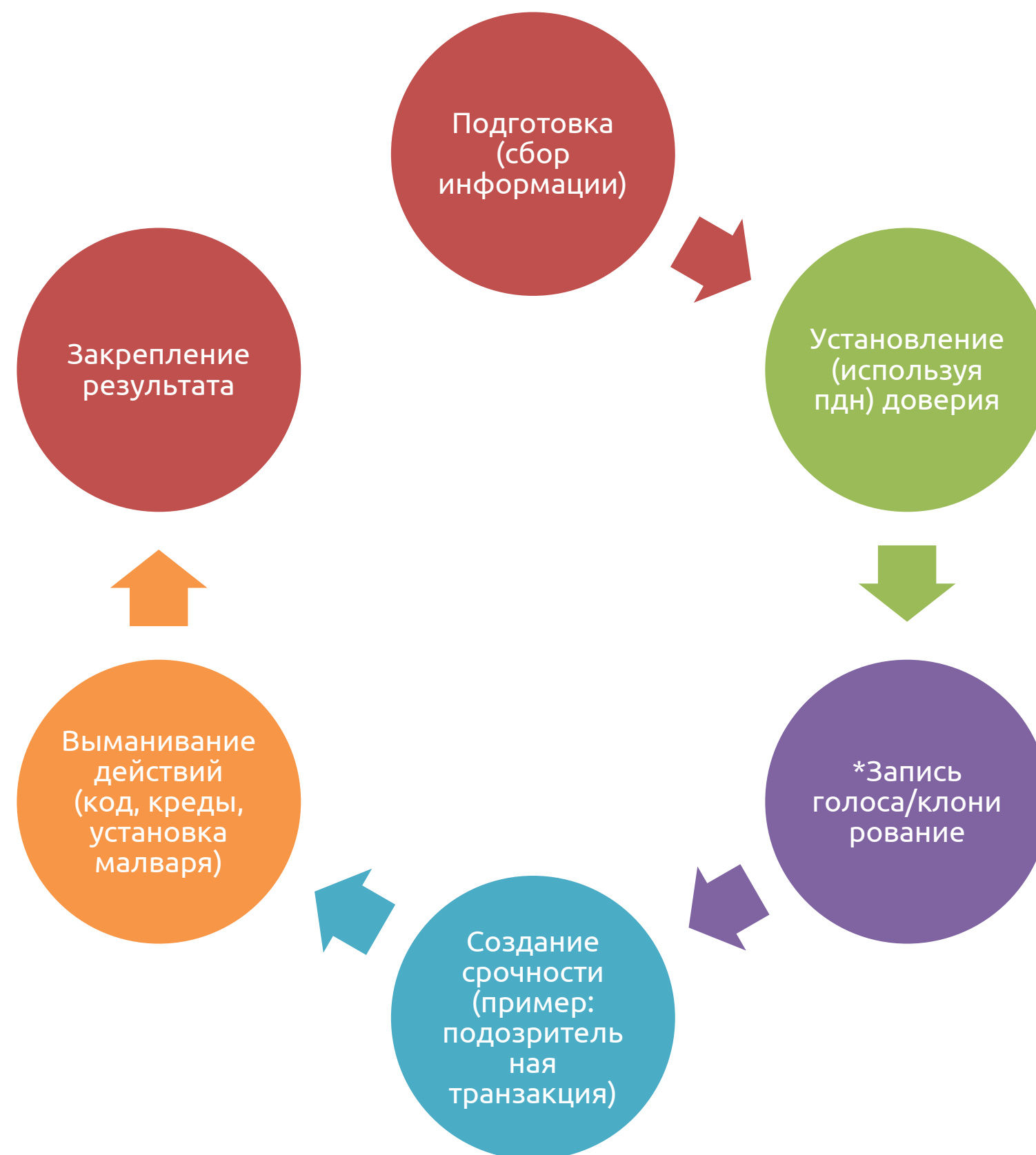


Первоначальный доступ

H1
2025

35% human first

Сценарий вишинга



Главные тренды 2025



Эволюция защиты

**Zero Trust, AI-
SOC, Darknet
Monitoring**

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': 1295898.375, '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 ,
        -4.05937 ], 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%**)

```
voice>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%).

Вебинар «Исп... ниторинге ИБ...
0:10 · ИнфоТеКС

16:10 ✓

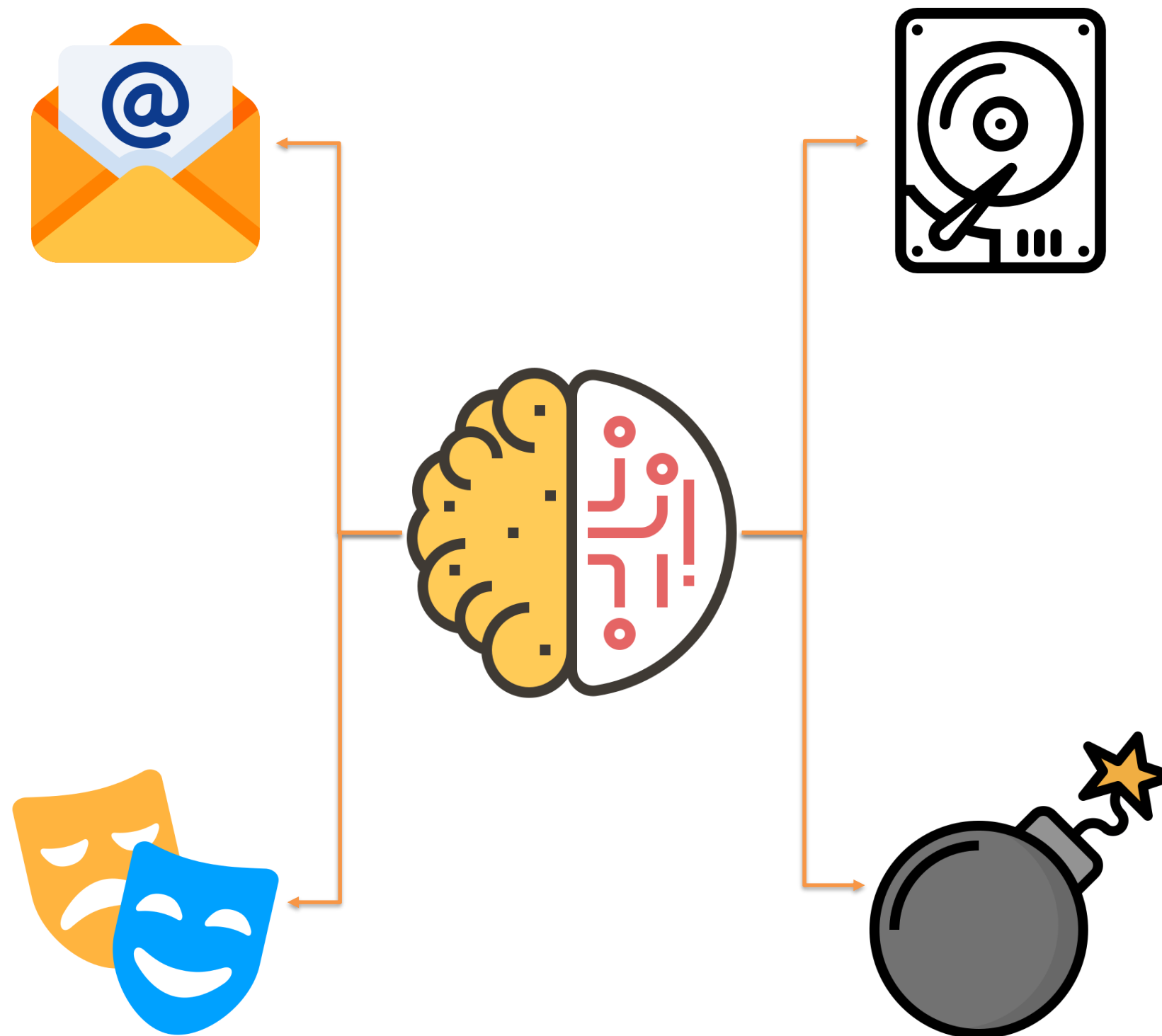
👉 Взял в работу, ожидайте... 16:10

✅ Готово! Результат:

LLM анализ (успешный):
Вероятность синтетического происхождения: **22%**
Категория: NATURAL

Ключевые признаки (по группам):
- **Source_micro**: Jitter = 5.80 % (высокий, типичен для человеческой речи); Shimmer = 25.08 % (в пределах естественного диапазона).
- **Spectral**: MFCC_std_mean = 35.07 (среднее, ближе к естественным записям, чем у синтетических образцов ≈ 39-40); Spectral_flatness = 0.3095 (относительно высокий, указывает на менее «плоскую» спектральную структуру); Spectral_centroid = 1957 Hz, Bandwidth = 1050 Hz – характерные для естественного голоса.
- **Phase**: Phase_distortion = 0.0975, Phase_diff = 0.3771 – умеренные отклонения, типичные для реального голоса; нет сильных фазовых артефактов.
- **Formants**: Formant_ratio = 2.02, Formant_ratio2 = 3.71, Formant1_2 в диапазоне 0.0 - 2.25 kHz – соответствует

ИИ в киберугрозах



Дети. Статистика

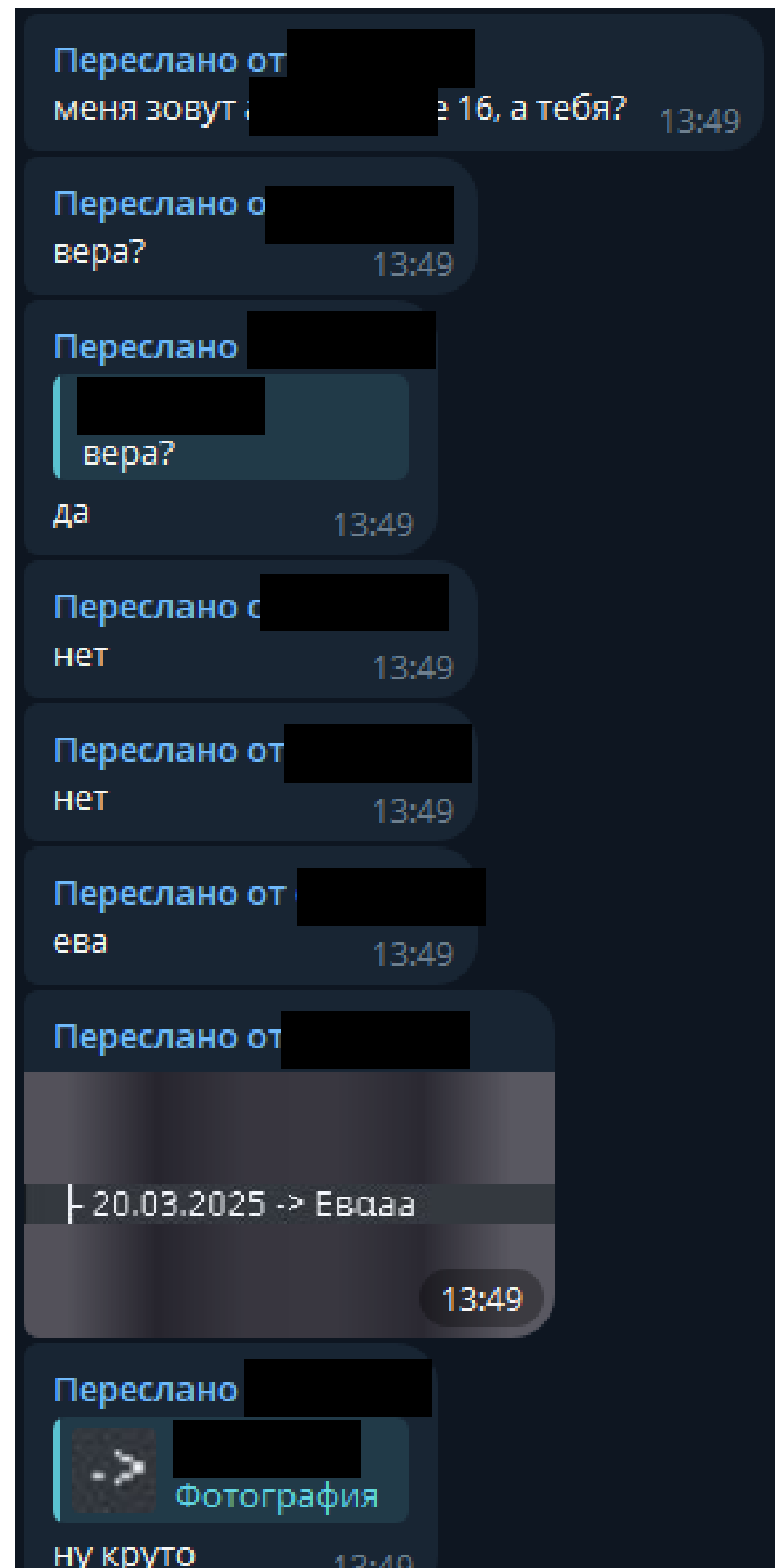
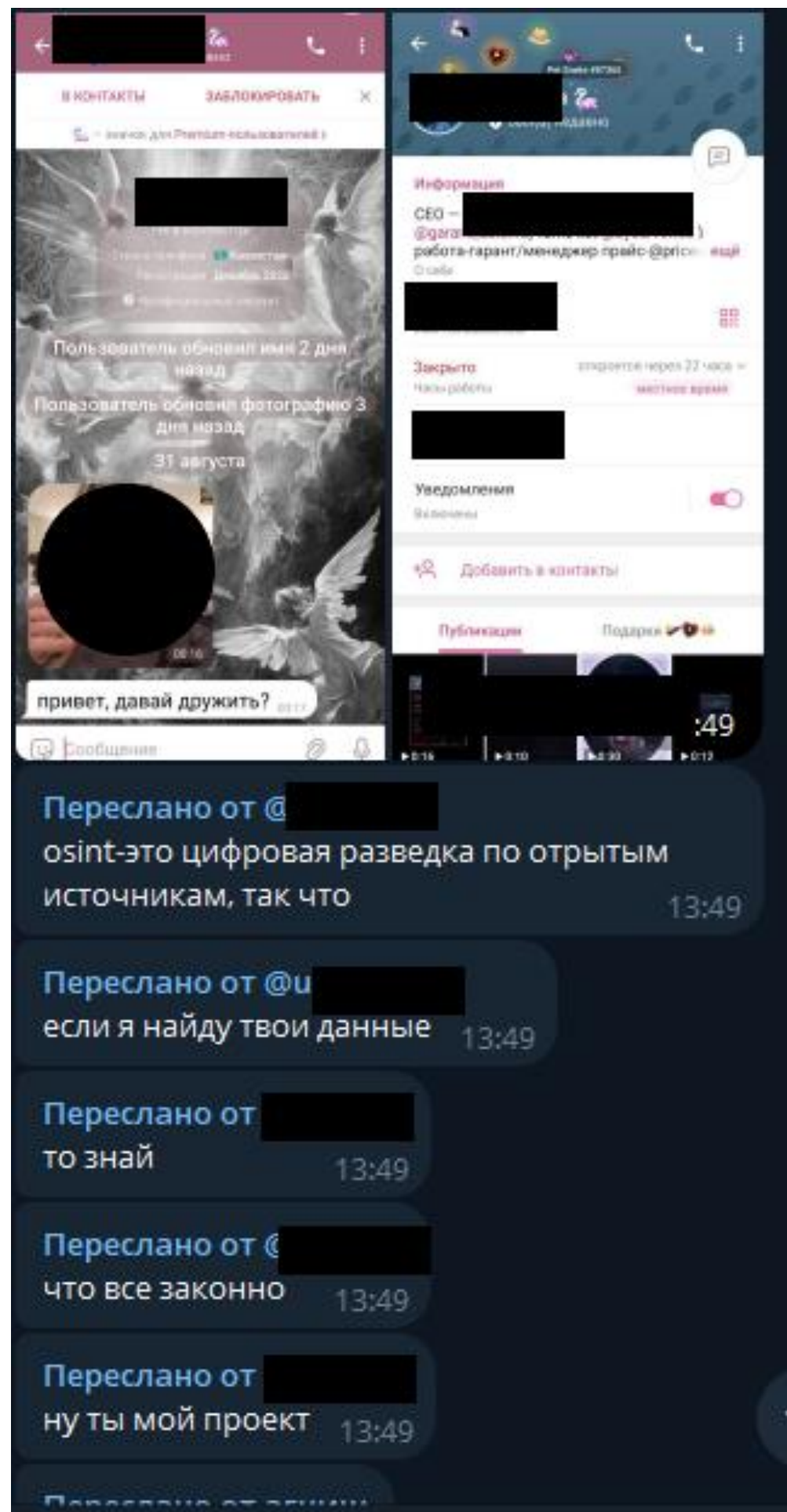


Пострадавших несовершеннолетних
от кибермошенников

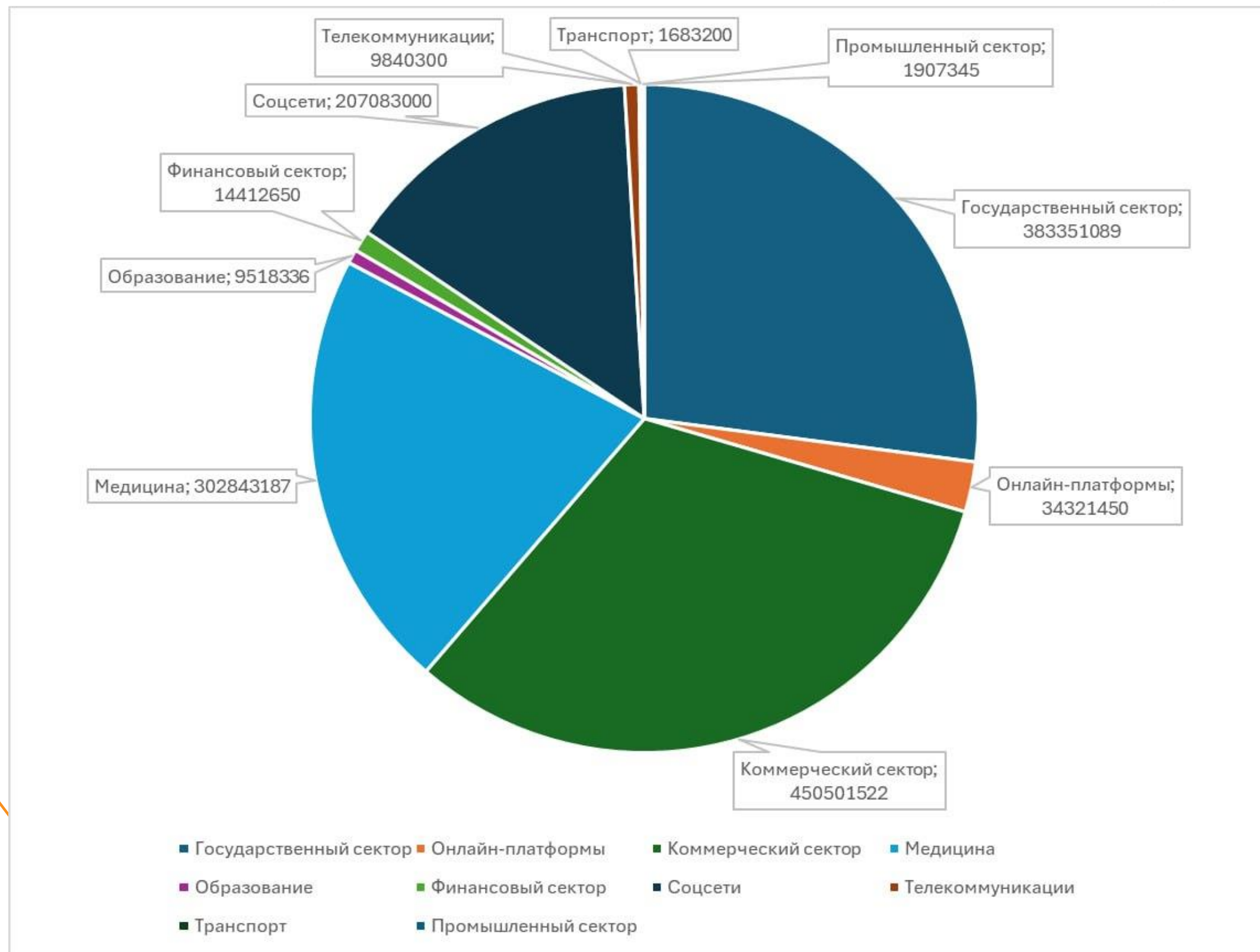
Н1
2025

+25%*

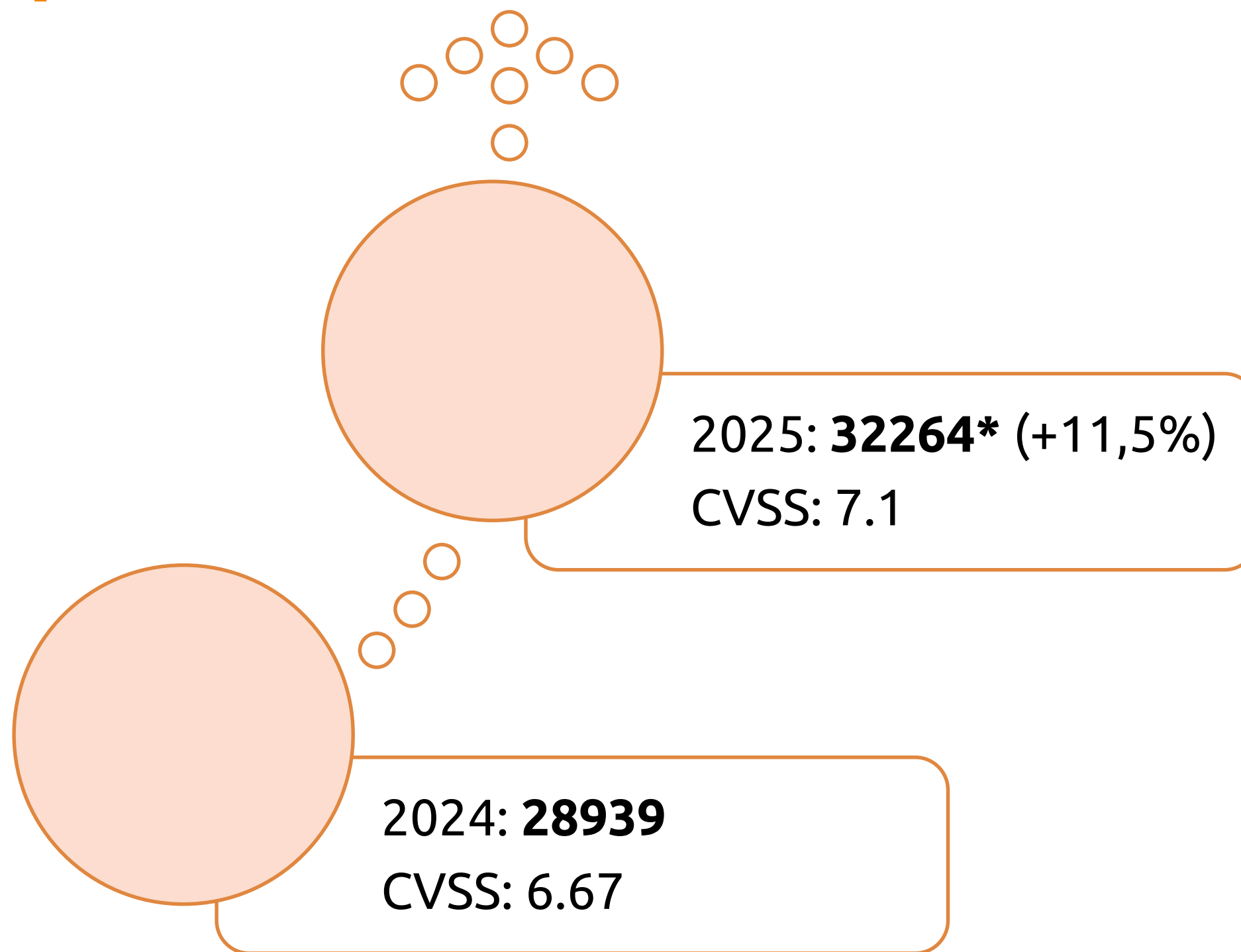
*по данным МВД



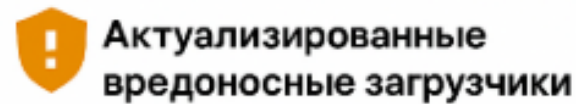
Утечки информации



Как меняются киберугрозы



Инструменты в 2025



•Stealerium

Анализирует, посещает ли жертва сайт 18+

Распространяется через фишинг и GitHub

•Lockbit

Шифровальщик

Автоматическое распространение внутри организации

Партнерская программа

•Lumma



•**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



Ольга [avatar] был(а) недавно

27 марта Здравствуйте!
Мне интересно
Я о работе помощником в интернет-магазине 14:12 ✓

Здравствуйте 15:05

Ищу помощницу для интернет-магазина на платформе Ozon

Мы занимаемся продажей детской одежды и активно развиваем наш магазин. Сейчас я ищу ответственную и организованную помощницу для удаленной работы на неполный день.

...

Да, конечно, мы с мужем и открыли магазин когда была в декрете 😊
Вы как завтра по времени и занятости?
Выдам вам рабочий кабинет, шаблоны, все материалы
Посмотрите всю механику, какие задачи 13:00 удобно?
Или можем немного позже, с утра на складе ранее не получается 15:22

Ольга [avatar] был(а) недавно

Выдаю вам наше приложение для сотрудников, пройдите регистрацию и анкетирование
Логин и пароль сейчас отправлю
Анкетирование занимает до 20 минут 11:14

OzonTracker.apk
12,8 MB APK 11:15

Логин(трек номер): 36125
Пароль: NastyAdm1 11:15

Ольга [avatar] был(а) недавно

Для анкеты мне нужно:
1. ФИО
2. Дата Рождения
3. Номер телефона 10:57

Ольга [avatar] был(а) недавно

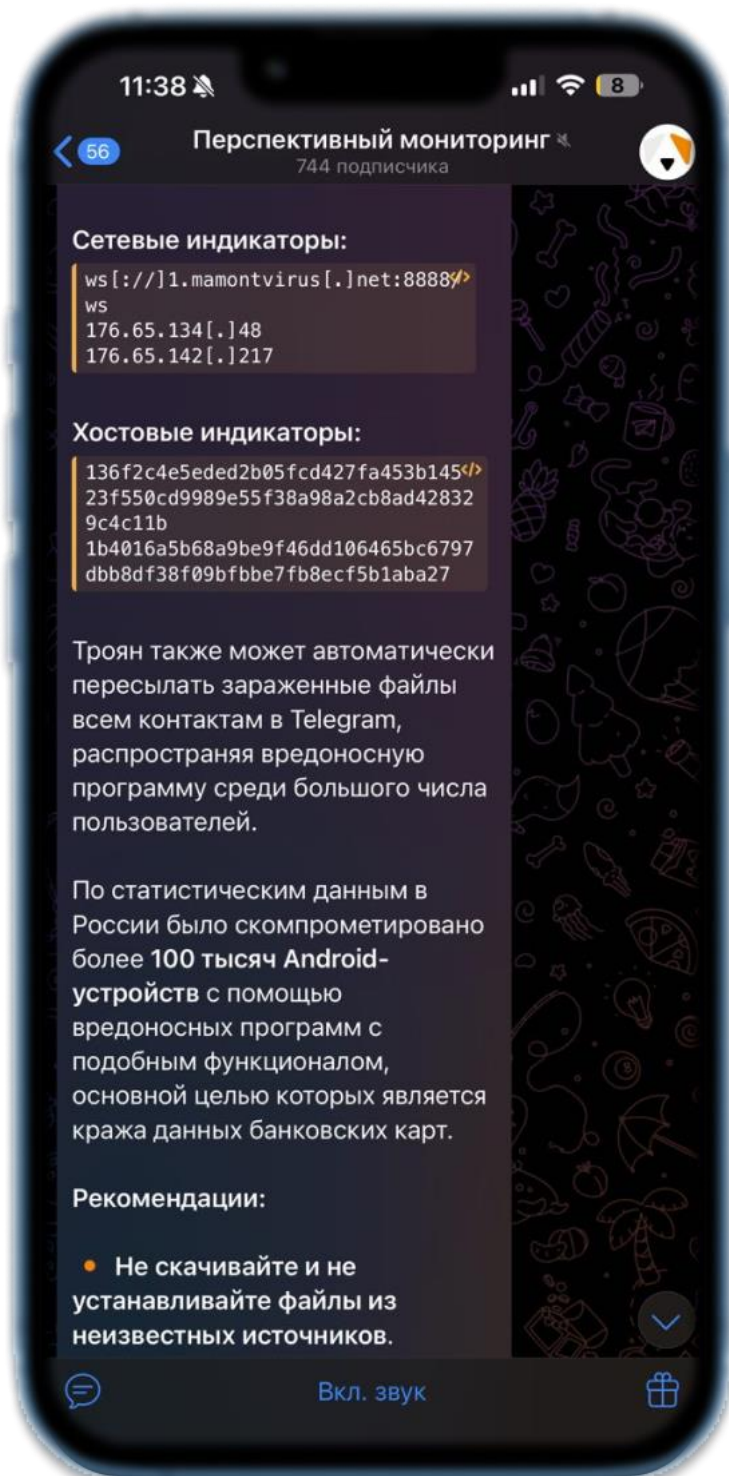
скидки недели
263 Р 1590 Р -83%
Осталось 208 шт
Футболка Ohana kids
★ 4.7 3 461 отзыв

скидки недели
267 Р 1590 Р -83%
Осталось 42 шт
Футболка Ohana kids
★ 4.7 3 461 отзыв

Завтра

ООО "Ohana market"
Магазин Premium ★ 4,8 177 К отзывов 561 К заказов

DeliveryRAT



Публикуем
идентификаторы
компрометации
встреченного нами
образца ВПО

Оригинальные товары брендов

Оригинальность товаров подтверждена
сертификатами



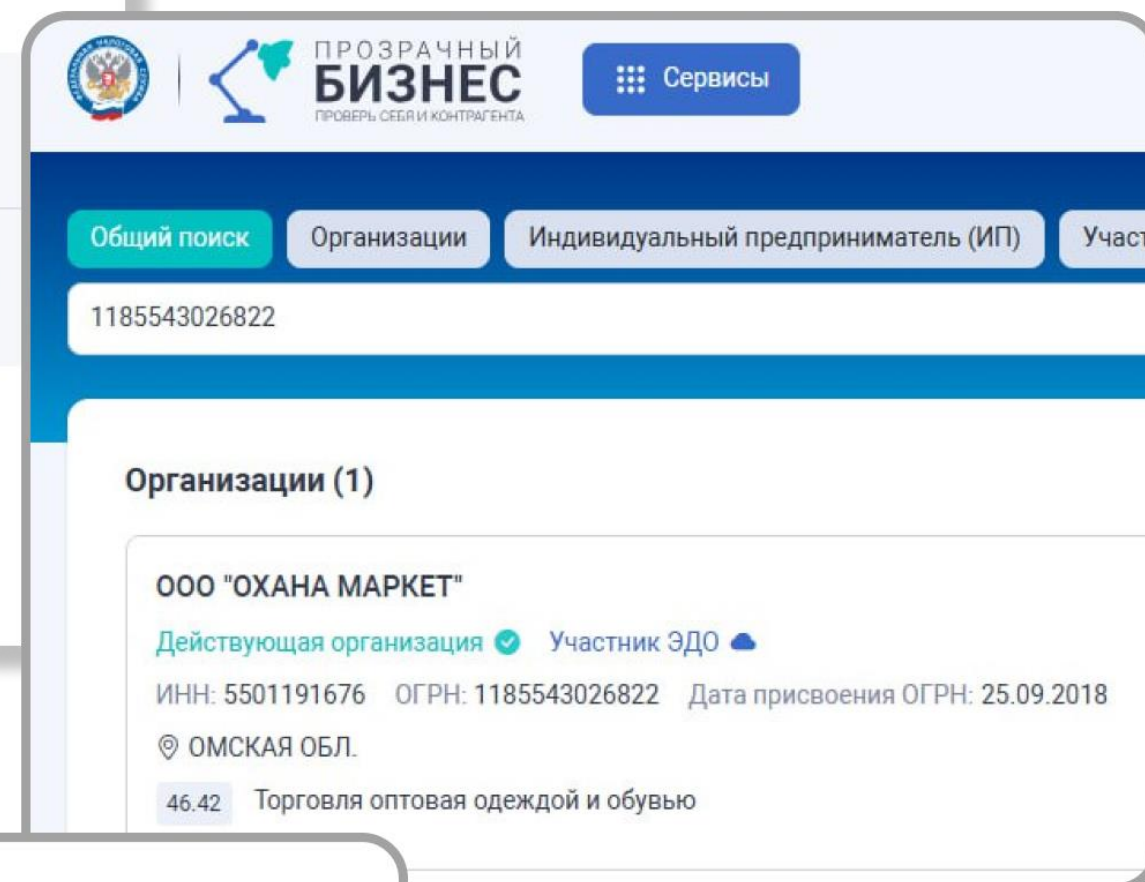
Ohana kids



Ohana market

ООО Охана маркет
644009, г. Омск, ул. 26 линия, д. 85А
1185543026822

Работает согласно графику Ozon



Сведения об учредителях (участниках, единственном акционере) юридического лица

ОКСАНА /

ИНН:

Количество ЮЛ, в которых лицо является учредителем (участником,
единственным акционером):

3

TelegramNFT



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ



приве 13:16

извини что отвлекаю не можешь подписаться на мой тгк а я тебе подарок какой нить подарб 13:16

Привет. Я коллекционирую подарочек, как у вас в профиле. Подскажите, пожалуйста, не продаете ли вы его? Не игнорируйте, пожалуйста, если ваш ответ отрицательный, дайте знать 💖 11:44



00:08

Привет, извини, если побеспокоила. Я ищу людей, которые бы смогли оставить мне отзыв в гарант-сервисе, а я бы взамен дала 100 звездочек или колечко. 11:46

Привет извини, если отвлекла, хотела попросить тебя проголосовать за меня в фото батле, с меня подарок 13:11

Привет, нфт продаешь? У меня есть 50+ отзывов, доказательства, что я не обманываю, о цене можем договориться 11:59

Извини, что прошу, но буду очень благодарен в помощи 11:15

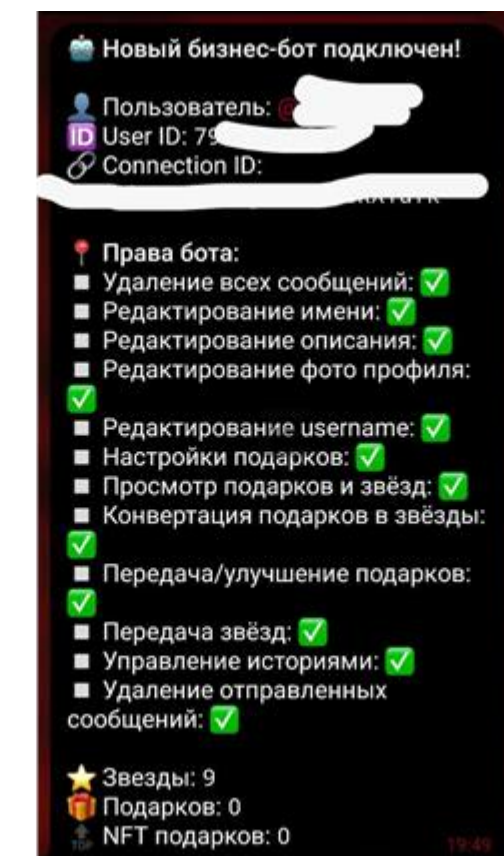
Я занимаюсь продажей звезд и мне нужны отзывы 11:15

Можешь написать отзыв? 11:15

Я тебе подарок за это 11:15

привет 13:38

куплю твой нфт подарок за стоимость +25 процентов от него 13:38



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

Пользователь

Регистрация: 02.02.2025
Сообщения: 29
Реакции: -8

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



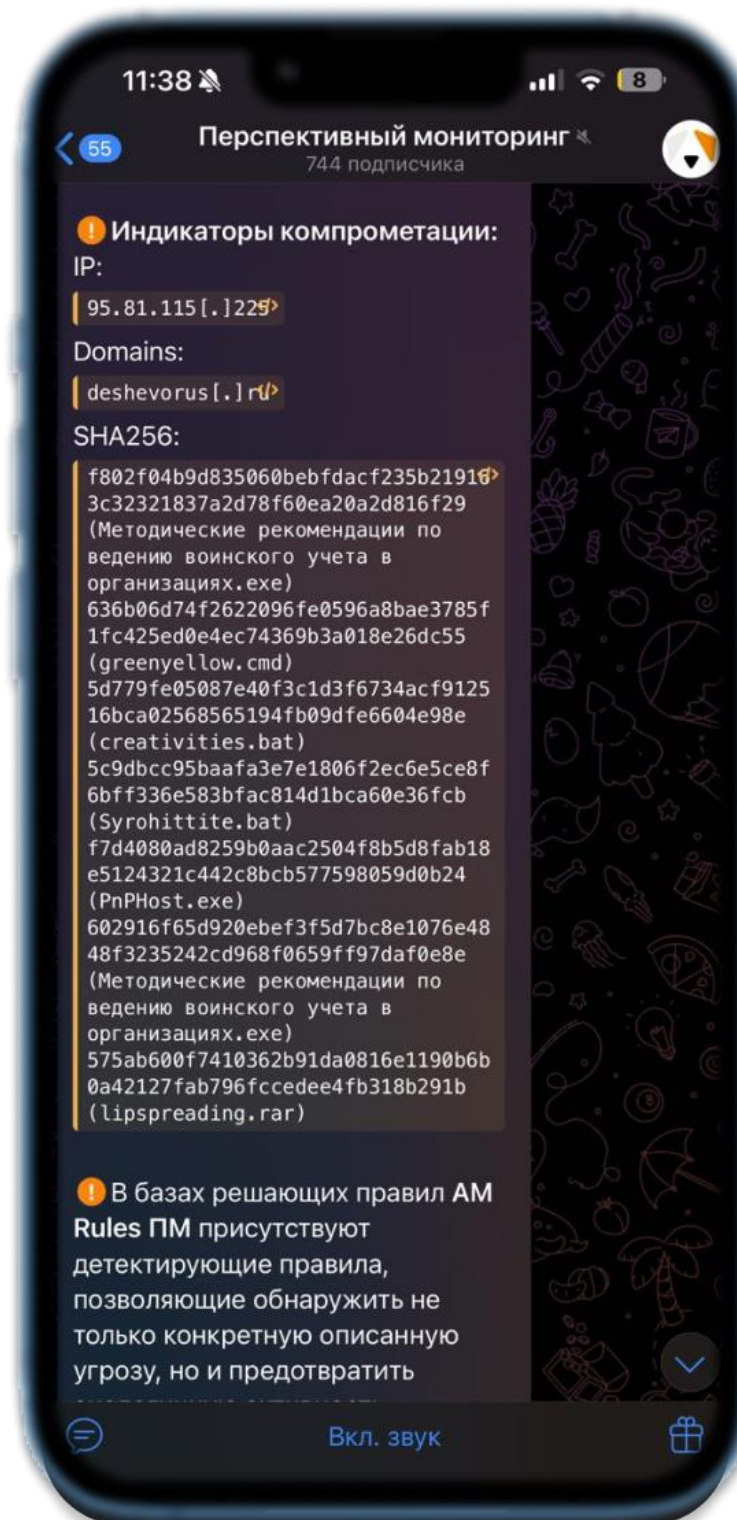
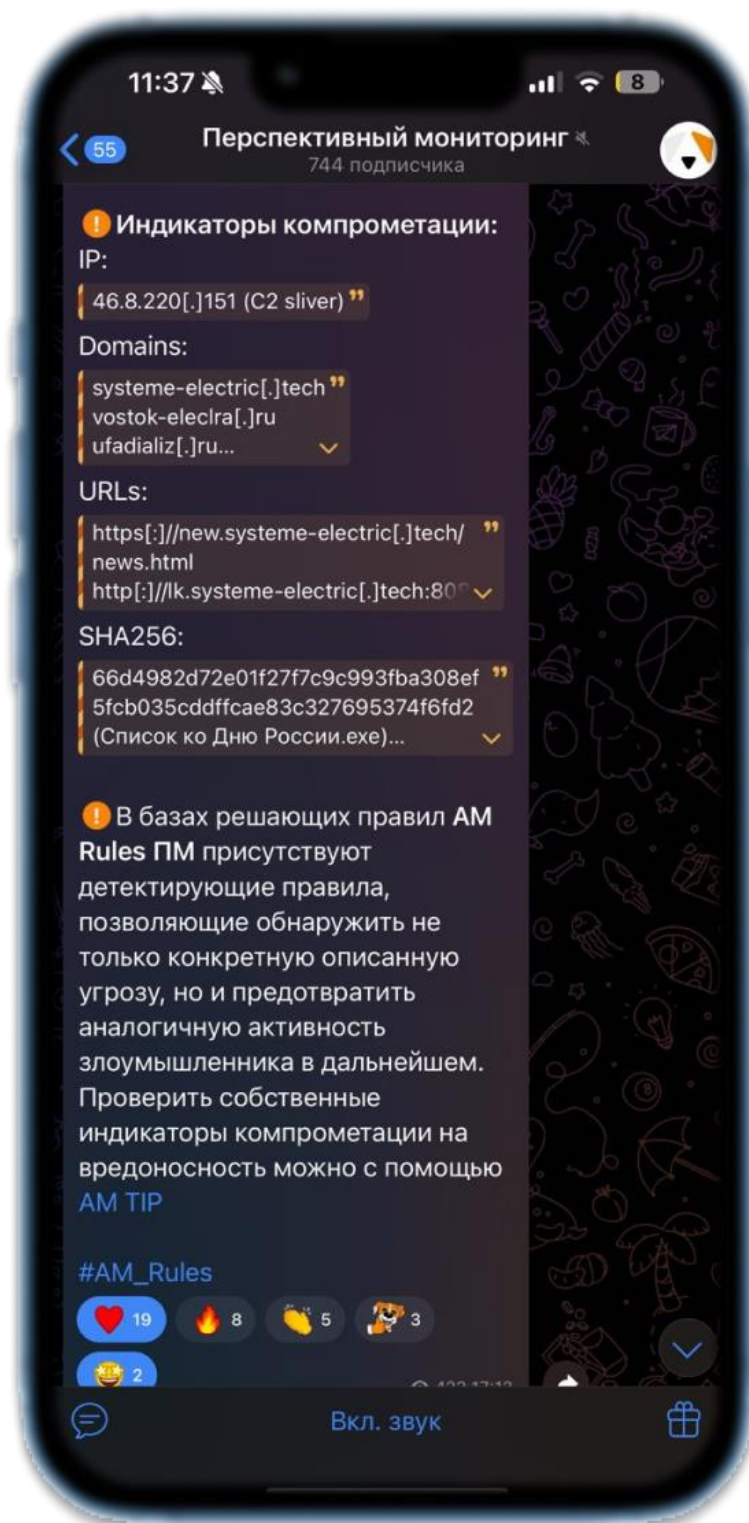
Наши исследования



Ранее неизвестное ВПО GemoDL



Новые модификации ВПО, связанные с АРТ-группировкой Core Werewolf



Спасибо
за внимание!



@PM_PUBLIC

amonitoring.ru

Слепнев Артур
Павлович

Старший аналитик данных

Artur.Slepnev@amonitoring.ru

ТЕХНОinfotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

