

**От фейка
к безопасности:
как OSINT сохранит
ваш капитал**



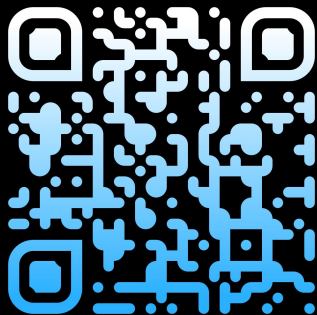
Докладчик: [angkasawan](#)

\$ whoami

Специалист по расследованию
киберпреступлений

Автор докладов по этой теме на OSINT
Mindset, PHDays, OFFZONE и
OSINTomático

Увлекаюсь Web3 безопасностью



О чем поговорим

Как организован современный скам

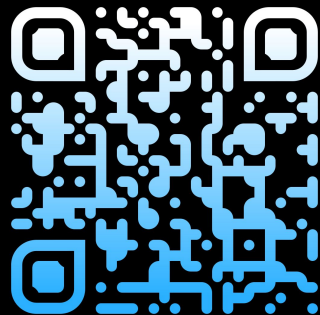
Известные схемы развода

Какие технические нюансы позволяют злодеям красть крипту

Способы выявления фейков

Как проверять веб-сайты на фишинг

Что делать если все таки обвели



вот бы мне мальчика

который напишет

Здравствуйте. Посмотрел вашу научную работу. Такой ерунды я конечно давно не встречал. Но выбирать было не из чего и комиссия отобрала ее на конференцию. На следующей неделе поедете выступать с докладом

Куда целят



Скам, нацеленный на конкретную личность

Скам, нацеленный на группу лиц без
личного контакта



Структура схемы



Арбитраж криптовалюты

Суть развода – вилка в курсе валюты на разных обменниках

Зачастую под эти цели создается специальный фишинговый сайт «слоупок». Это создает видимость того, что вы сами контролируете свои средства

Чтобы противостоять – нужно уметь определять фейковые аккаунты и липовые сайты-обменники

Со слов потерпевшего:

"Реклама в инсте - арбитраж крипты. Тыкаю, там пишет человек, дружелюбно, все дела. Перешли в телегу. Рассказал схему - перегоняем крипту по сигналу через обменник слоупок, получаем 2-3 процента с депозита. Провели 2 пробных за 100 баксов, получила 107. Класс, офигенно. Завела больше, при первой же сделке зависают в обменнике монеты DASH. Поддержка обменника говорит 48 часов на зеркальную транзакцию вам, т.е. отправьте столько же, тогда вся сумма вернётся. На бинансе кнопку возврата или отмены транзакции не работают. В телеграммах нет телефонов, конечно же"

12:58 PM



Реклама



В г Барнаул Илон Маск раздает деньги. Доступ открыт 54 минуты

7 ч 25 мин назад

Дрейнеры

Суть развода: заставить человека подключить свой кошелек к фишинговому сайту, к которому подключен дрейнер

Как только вы подтвердите транзакцию или согласитесь на подпись - произойдет неизбежное

Добрый день, я не разбираюсь в смарт контрактах и меня на этом обманули.

Человек предложил обменять usdt на usd, но попросил сначала адрес для проверки, а потом проверить на данном сайте (<https://crystblock.com/>) мой кошелек.

При проверке вышел запрос на вызов смарт контракта eth, я его одобрил и все usdt списались в его пользу

Мой адрес кошелька

0x4200000000000000000000000000000000000000

На этот кошелек ушли все usdt (1795,50)

0x4200000000000000000000000000000000000000

Можно ли вернуть деньги или нет?

← 14 6:52 AM

preloaded intentionally.

⑦ If u need this product. Write me telegram: @t_refresh.

⑦ Connection wallet failed. Error: Error: No CLV Wallet found

⚠ DevTools failed to load source map: Could not load content for <https://crystblock.com/s.map>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE

⚠ The resource <https://crystblock.com/licuvar/themes/webcase/app/static/fonts/svgfont.wo> preload but not used within a few seconds from the window's load event. Please make su



1000 = 1...



В общем ситуация тупая 9:05 AM

Мне менеджер отписал что нам бабки в USDT TRC 20 перевели 9:06 AM

По ошибке больше чем нужно 9:06 AM

Мол надо отправить обратнос разницец 9:06 AM

я глянул, ну мол вроде да 9:06 AM

есть аткое 9:06 AM

а оказалось что точка и запятая не одно и тоже 9:06 AM

на деле нам перевели 2 с лишним бакса 9:07 AM

а не 2к 9:07 AM

а отправил я нахзад 2к 9:07 AM

0x5030fe...903A55FE



0x46cf79...210A0de2

1,000

0xdeD353...df2e6D46



Coinbase: Commerce F...

1.426

► From 0xdeD353...df2e6D46 To 0x2784df...436D0490 For 141.174 (\$141.01) ◀

► From 0xdeD353...df2e6D46 To Coinbase: Commerce Fee 3 For 1.426 (\$1.42)

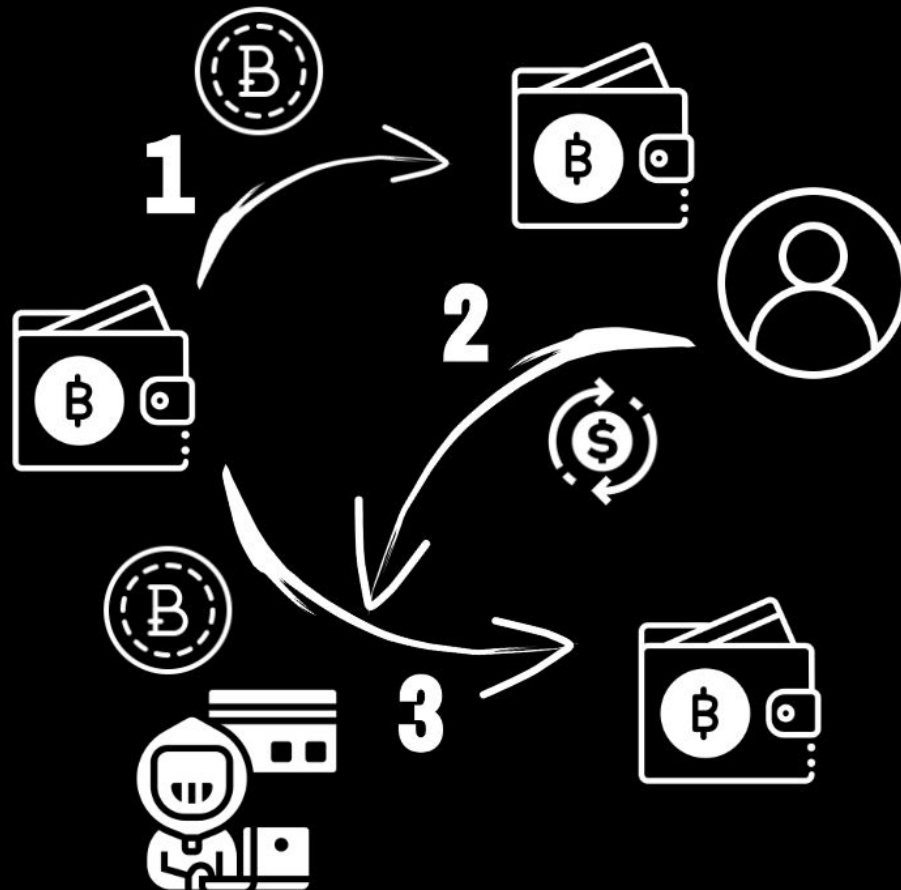


Транзакции с нулевой комиссией

Мошенник отправляет транзакцию на ваш адрес, но ставит минимальную комиссию

Вы, не дождавшись включения транзакции в блок, отправляете скамеру в фиате

Мошенник сразу же перебивает свою старую транзакцию на ваш адрес. Он отправляет те же средства себе, но уже с высокой комиссией



Проверяем размер комиссии



OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



Advanced Details

Hash	5e69-edde	Block ID	799,419
Position	13	Time	19 Jul 2023 08:24:36
Age	15m 31s	Inputs	1
Input Value	0.00010241 BTC \$3.07	Outputs	1
Fee	0.00009695 BTC \$2.90	Output Value	0.00000546 BTC \$0.16
Fee/VB	<u>68.759 sat/vByte</u>	Fee/B	34.625 sat/B
Weight	562	Size	280 Bytes
Coinbase	No	Weight Unit	17.251 sat/WU
RBF	No	Witness	Yes
Version	1	Locktime	0
		BTC Price	\$29,953.64

Overview

JSON

From

1 [bc1pru0lxm34udfyza9gg4g3epnpazhww2k2z4aazr7pxt...](#)
0.00010241 BTC • \$3.07

To

1 [bc1phh85galupjksjcwfcc5s67xzmsqtpxjrdxj3lcy924zrhylg...](#)
0.00000546 BTC • \$0.16

Фейковый токен

Вариаций масса: от попыток свапа на настоящий до ссылки на фиш в названии

Количество владельцев – не показатель надежности!

Большое количество транзакций от разных аккаунтов – более менее показатель!

Листинг на DEX тоже показатель:
dexscreener.com



⚠ This token is reported to have been used for misleading people into believing it was sent from well-known ad

ERC-20

Phish / Hack

Overview

MAX TOTAL SUPPLY
151,799 ERC-20 TOKEN* ⓘ

HOLDERS
6,013 (0.00%)

TOTAL TRANSFERS
6,001 ⓘ

Market

FULLY DILUTED MARKET CAP ⓘ
\$0.00

CIRCULATING SUPPLY MARKET CAP
-

Transfers

Holders

Info

Contract

Analytics

Comments

📊 Token Holders Chart

Top 1,000 holders (From a total of 6,013 holders)

BEP-20

Cross-Chain

Overview

MAX TOTAL SUPPLY
999,999,999,999,999 空投网址 bsc20.lol
(CSupply: 999,999,999,9...)

Частный случай: стейкинг



Видим ввод с биржи MEXC, затем USDT переводятся на смарт-контракт злоумышленника. Вместо настоящих USDT мнутся фейковые токены под видом стейкинга

Null: 0x000...000	IN	[redacted]	1,616.38	ERC20 ***
[redacted]	OUT	[redacted]	1,616.38	Binance-Peg ... (BSC-US.
MEXC 6	IN	[redacted]	1,616.38	Binance-Peg ... (BSC-US.
Null: 0x000...000	IN	[redacted]	10,580.14	ERC20 ***
[redacted]	OUT	[redacted]	10,580.14	Binance-Peg ... (BSC-US.
MEXC 6	IN	[redacted]	10,580.14	Binance-Peg ... (BSC-US.

Стилеры

Продаются/арендуются по модели MaaS (Malware as a Service)

Крадут ключи и сид фразы от кошельков

Требуется время на брутфорс

Можно успеть перевести средства на новый счёт

Пример развода

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



Checking

Thanks that you notice we are constantly pushing updates hahah

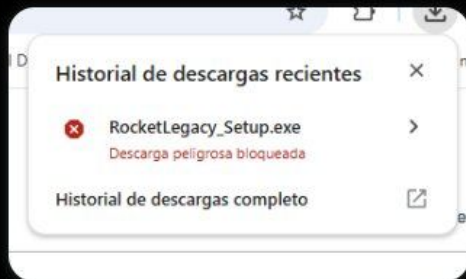
Sat 2:59 PM

haha it worked, but it is detected as malware

Sat 3:04 PM

Can you send a screenshot

Sat 3:05 PM



Sat 3:05 PM

The Download page doesnt work either

And the Click here button below doesnt work either



Sat 3:01 PM

Проверяем вредонос

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



Самый простой способ: грузить на [VirusTotal](#). В случае NDA лучше грузить хэш:

Linux: md5sum "path/to/file"

MacOs: md5 "path/to/file"

Windows: certutil -hashfile "path/to/file" MD5

The screenshot shows the VirusTotal analysis interface for a file named 'Minecraft.exe'. The file's MD5 hash is 'a1a6920b3aebaa71f88a202adc24ff85b28ca4b8518f1f868586104658997175'. The file size is 131.48 KB, and it was last analyzed 11 months ago. The analysis shows that 49 out of 72 security vendors flagged the file as malicious. The file is categorized as a trojan, specifically a data stealer. The 'Security vendors' analysis section lists several vendors that have detected the file as malicious, including AhnLab-V3, ALYac, Alibaba, and Antiy-AVL.

Community Score: 49 / 72

File Hash: a1a6920b3aebaa71f88a202adc24ff85b28ca4b8518f1f868586104658997175

File Name: Minecraft.exe

Size: 131.48 KB

Last Analysis Date: 11 months ago

File Type: EXE

Security Vendors: 49/72 security vendors flagged this file as malicious

Threat Categories: trojan

Family Labels: msil, datastealer, stealer

Security vendors' analysis:

Vendor	Detection
AhnLab-V3	Trojan.Win.Evital.C5576833
Alibaba	TrojanPSW:MSIL/Stealgen.2d07f8c7
ALYac	Trojan.MSIL.Stealer.gen
Antiy-AVL	Trojan[PSW]/MSIL.CoinStealer

Что же делать?



OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



ОСИНТИТЬ!!!

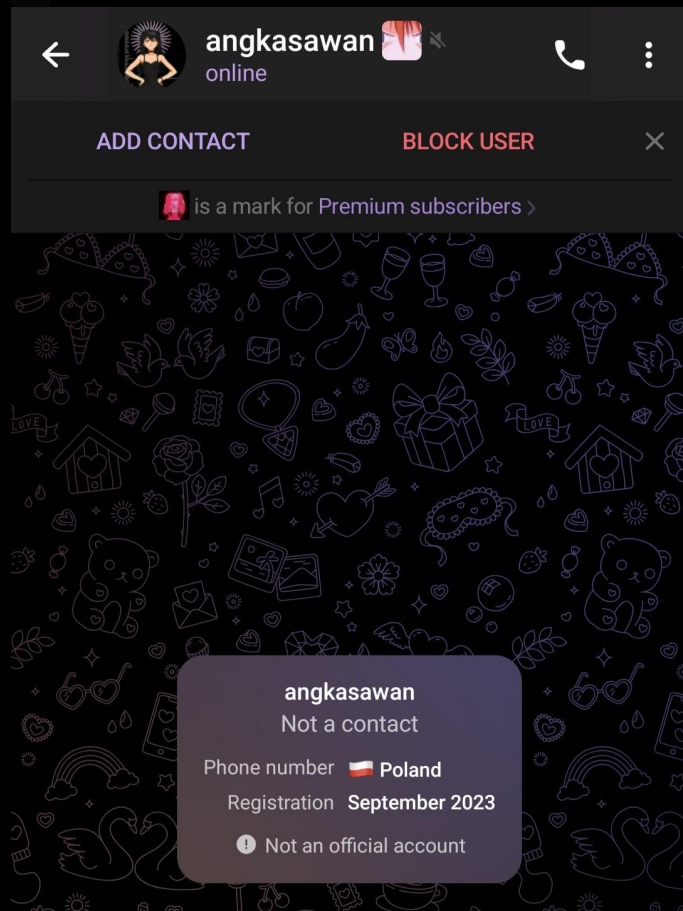
OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan

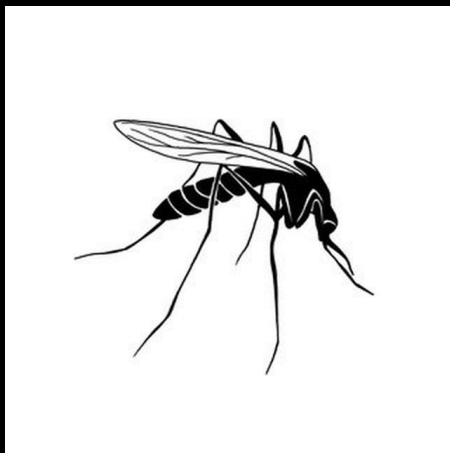
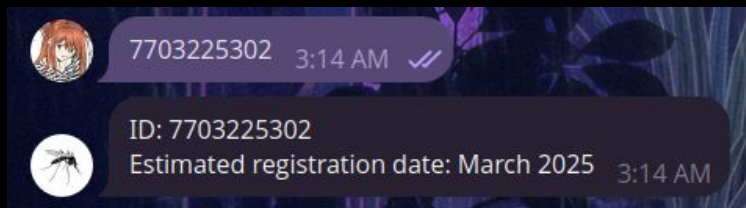


Если у вас мобильная версия и аккаунт вам написал первый вам покажут страну номера и примерную дату регистрации



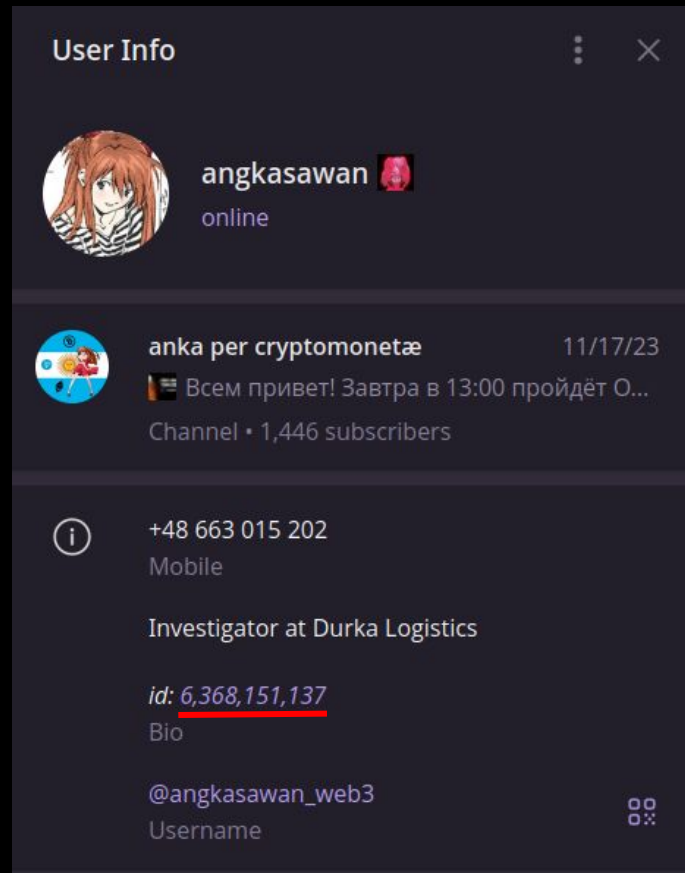
Узнаем Telegram ID

Settings > Advanced > Experimental Settings > Show Peer IDs in Profile.



@regdate_clone_bot

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan

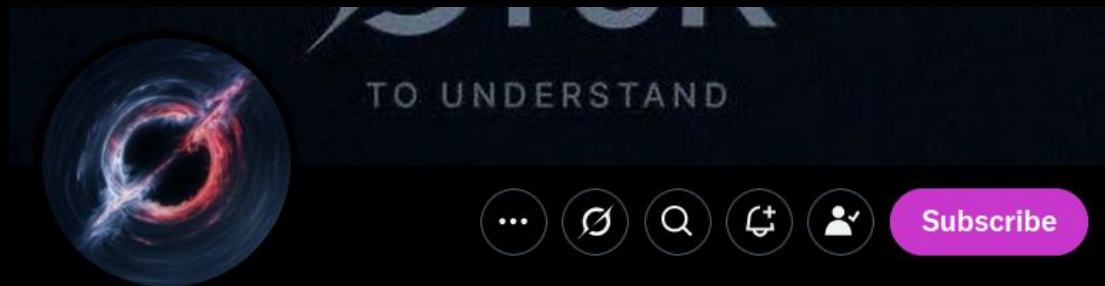


Остальные соцсети

regvk.com

[VKHistoryRobot](#)

Встроенные функции соцсетей



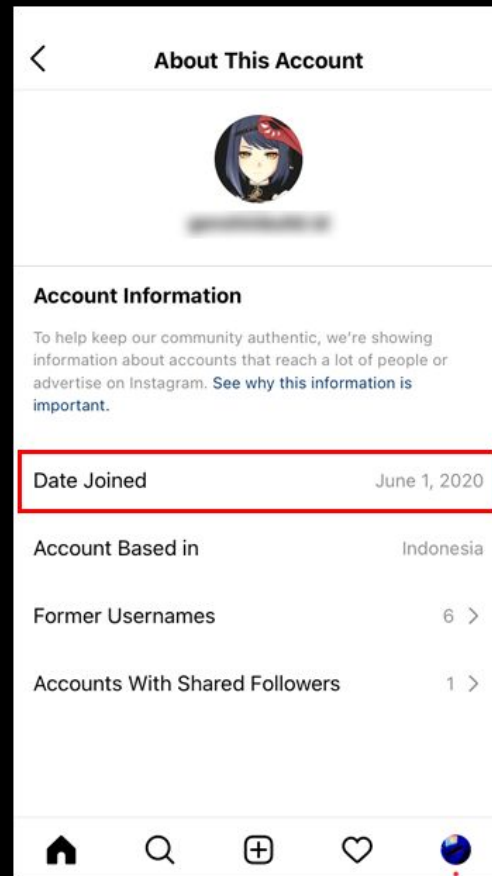
Elon Musk  

@elonmusk

 Joined June 2009

1,078 Following 219.1M Followers

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan

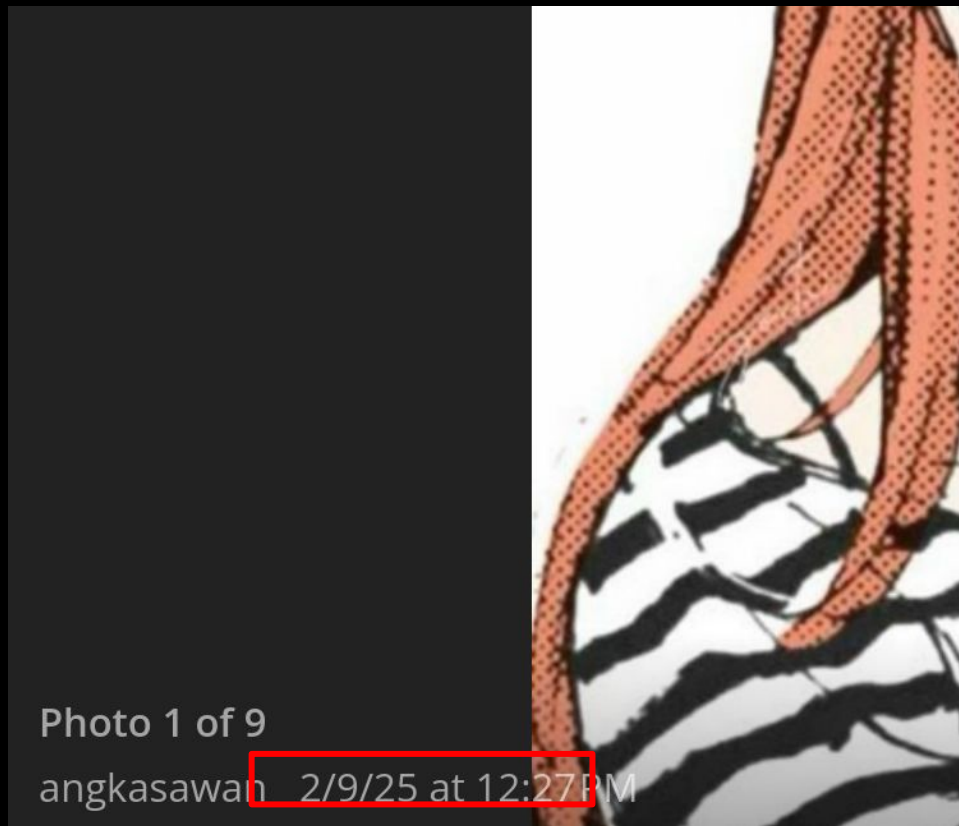


Дата загрузки аватаров

Обычно на фейках одна аватарка, либо все аватарки загружены за малый промежуток времени



OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



Лицо на фотографиях

search4faces.com

facecheck.id

findclone.ru

[Yandex](https://yandex.ru)

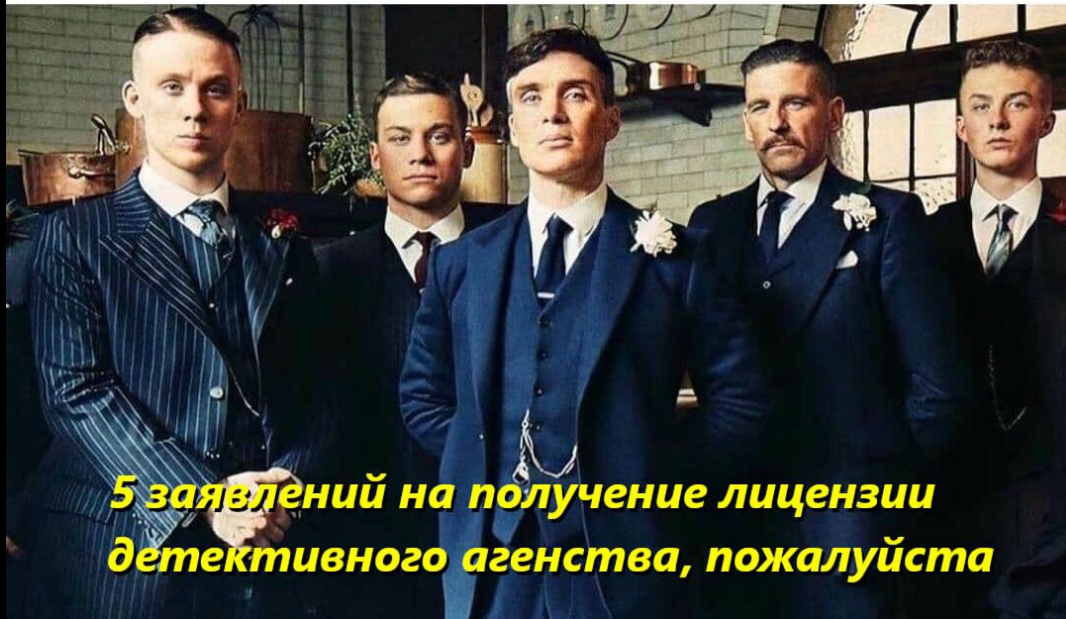
[Google](https://www.google.com) (только поиск оригинала!)

pimeyes.com

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



Когда с кентами в баре
нашли инсту девушки через
яндекс картинки:



**5 заявлений на получение лицензии
детективного агентства, пожалуйста**

Как же я люблю бтс

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



search4faces

[Главная](#)

[Поиск](#)

[О нас](#)

[FAQ](#)

[Контакты](#)

[API](#)

[Русский](#) ▼

Совпадения



Иван Сафронов

совпадение: 98.95%

39 лет [1.1.1984]

Россия [Москва]

[Профиль](#)

[Фото](#)



Олег Тольятти

совпадение: 98.58%

Россия [Санкт-Петербург]

[Профиль](#)

[Фото](#)



Татьяна Тарновская

совпадение: 97.66%

[4.4]

Россия [Москва]

[Профиль](#)

[Фото](#)



Выявляем нейронки

Hive Moderation

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



 HIVE MODERATION

HomeProductsInsightsCase StudiesDocumentationPricingContact UsLog In

See our AI-Generated Content Detection tools in action

Upload image, audio or video here to test our model in real-time!

Supports png, jpeg, jpg, webp, x-matroska, quicktime, avi, wmv, h264, mp4, webm, flac, mp3, mpeg, ogg, wav, x-msvideo, x-matroska, x-ms-wmv, mov, x-wav, x-m4a, x-flac, wav, mkv. Use is subject to this site's [Terms of Service](#).



Upload

RESULT

The input is: likely to contain AI-generated or deepfake content

96.7%

BY CLASSES

Classes	Score
ai_generated	0.96
stablediffusion	0.85
flux	0.08
not_ai_generated	0.03
none	0.03
stablediffusionxl	0.01

Ищем интересы и чаты



Telesint



TgScanRobot



FunStat

Ищем сообщения
пользователя в чатах

Открытые группы [39]:

@yearnfinance yearn.finance (YFI)
@recruiterynvn Cộng đồng Recruitery Việt Nam
@binance_api_english Binance API (English Only)
@marginuggroupchat Margin - Trade Coin Underground
@margin_atm MarginATM - Chat
@catboost_en CatBoost
@ampleforth Ampleforth Protocol
@forexvietnams Forex CJC - Kiếm tiền cùng tôi
@whalecharts whalechart 🐳
@xbnquest XBN Airdrop
@ftx_vietnam_official FTX - Sàn Giao Dịch - Official VN 🇻🇳
@themiscommunity Themis Protocol Community
@stackschat Stacks
@polkastarter Polkastarter
@nmr_official Numerai
@ctovietnam CTO VIETNAM NETWORK
@poolzofficialcommunity Poolz - Official
@rmpltg RMPL
@phemex_en Phemex English
@xbtafrica Genius | AI Nexus africa
@xencryptotalk XEN Crypto

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



19 февр. Работа в Эстонии.. (14)
19 февр. Венгрия Жильё I Р.. (9)
19 февр. Работа Варшава (6)
19 февр. Работа Германия (11)
19 февр. Будва | Черногори.. (1)
19 февр. тбилиси работа (2)
19 февр. ❤️ Тель-Авив 24 И.. (3)
18 февр. Испания Жильё I Р.. (1)
17 февр. Работа и Ваканси.. (82)
17 февр. Дубай РАБОТА: Вак.. (4)
17 февр. Работа в Казахстане (8)
17 февр. |Италия |Работа| (7)
17 февр. Дубай | ОАЭ - Раб.. (2)
17 февр. Ереван | Армения.. (2)
17 февр. 🇸🇰 🇷🇺 🇧🇪 Бирж.. (3)
13 февр. Бельгия Жильё I Р.. (4)
13 февр. Анталья | Турция.. (5)
13 февр. РАБОТА | | ВСЯ ИСП.. (1)

Ищем по никнейму

Мошенник всегда использует уникальный никнейм

А если не использует, то мы его легко найдем

Лучший инструмент: Maigret

[@osint_maigret_bot](https://t.me/@osint_maigret_bot)

github.com/soxoj/maigret

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал



```
asuka@langley:~$ maigret angkasawan2007
[-] Starting a search on top 500 sites from the Maigret database...
[!] You can run search by full list of sites with flag '-a'
[*] Checking username angkasawan2007 on:
[+] YouTube: https://www.youtube.com/angkasawan2007
[+] GitHubGist [GitHub]: https://gist.github.com/angkasawan2007
[+] Telegram: https://t.me/angkasawan2007
    |__fullname: angkasawan
    |__image: https://cdn4.telegram-cdn.org/file/bdYlDN0e43FB0uipzP0CU9hRFxhq
Y0lyqU-a7jrjHWcNbDyVZ39NzSQP2SMCv2MlSgz78zeg885idQ0KmHfz1WX5lJjsr2NrXgQwv
    |__bio: ankasavanka ch:
@anka_per_monetae
[+] GitHub: https://github.com/angkasawan2007
    |__uid: 138368236
    |__image: https://avatars.githubusercontent.com/u/138368236?v=4
    |__created_at: 2023-07-02T10:23:47Z
    |__follower_count: 0
    |__following_count: 0
    |__fullname: Daniel
    |__public_gists_count: 0
    |__public_repos_count: 0
    |__bio: Web3 security and OSINT investigations
[+] Blogger: https://angkasawan2007.blogspot.com
    |__blog_id: 7988468659040757520
    |__uid: 05976306605634261392
[+] Zhihu: https://www.zhihu.com/people/angkasawan2007
[+] Shutterstock: https://www.shutterstock.com/fi/g/angkasawan2007/about
[+] Pinterest: https://www.pinterest.com/angkasawan2007/
[+] YandexZenChannel [Yandex]: https://zen.yandex.ru/angkasawan2007
[+] authorSTREAM: http://www.authorstream.com/angkasawan2007/
[+] forums.imore.com: https://forums.imore.com/member.php?username=angkas
[+] Speedrun.com: https://speedrun.com/user/angkasawan2007
[+] TRASHBOX.RU: https://trashbox.ru/users/angkasawan2007
[+] AnimeNewsNetwork: https://www.animenewsnetwork.com/bbs/phpBB2/profile
[+] DonationsAlerts: https://www.donationalerts.com/r/angkasawan2007
[+] Ebay: https://ebay.com/usr/angkasawan2007
```


Анализ фишинговых сайтов

Регистрационные данные

Упоминания домена

Контактная информация и
другое содержимое сайта

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



если хотите со мной
познакомиться, то заполните
пожалуйста анкету

A simulated credit card registration form. The form is light gray with rounded corners. It contains the following fields and labels:

- Номер карты**: A large rectangular input field for the card number.
- Месяц**: A small rectangular input field for the month.
- Год**: A small rectangular input field for the year.
- Имя и фамилия владельца карты**: A rectangular input field for the cardholder's name.
- как на карте**: A small italicized label below the name field.
- CVC2/CVV2**: A label for the security code field.
- последние 3 цифры**: A label below the security code field.

Регистрационные данные

Протокол WHOIS и RDAP

Whois: DNSlytics

RDAP: Client RDAP

Смотреть только дату регистрации,
все остальное либо скрывается, либо
подделывается при регистрации
домена

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



Events:

registration:

12/6/2024, 8:44:32 PM

expiration:

12/6/2025, 8:44:32 PM

RDAP

Updated Date: 2024-07-23T08:00:46Z

Creation Date: 2002-08-22T18:26:40Z

Registry Expiry Date: 2025-08-22T18:26:42Z

WHOIS

Упоминания домена

OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



Google

"alphaexchangecoin.com"



Картинки

Видео

Новости

Покупки

Карты

Книги

Авиабилеты

Результатов: примерно 71, страница 2 (0,20 сек.)



kurs.expert

<https://kurs.expert> › [cherniy-spisok-obmennikov](#) ⋮

Черный список обменников - КурсЭксперт

<https://alphaexchangecoin.com/> Арбитражники почти все с кем созванивался имеют с ней дело. Sasha. 10 мая 2023, 00:58. Это и есть хорошо, сразу будете знать ...



telltrue.net

<https://telltrue.net> › [Письма читателей](#) ⋮

Арбитраж Криптовалют на стороне - TellTrue

5 мая 2023 г. — Использовали конечно же Binance, Trust Wallet и обменку alphaexchangecoin.com – этот сайт мне сразу не понравился, я даже погуглил, но не...

Поиск по содержимому

Контакты из политики конфиденциальности: почты, телефоны, имя компании, адреса

Логотипы сервиса: обычный поиск по картинке Google/Яндекс

Фавиконсы: Favihash, Favicorn



OSINT mindset conference #6
От фейка к безопасности: как OSINT сохранит ваш капитал
angkasawan



Google "alphaexchangecoin@gmail.com" X [Icons]

Картинки Видео Карты Новости Покупки Книги Авиабилеты

Результатов: примерно 3 (0,21 сек.)

Возможно, вы имели в виду: "**alpha exchange coin**@gmail.com"

alphaexchangecoin.com
<https://alphaexchangecoin.com> › [privacy-policy](#) ⋮

Политика Конфиденциальности

Вы имеете право запросить удаление Ваших персональных данных, отправив нам электронное письмо по адресу **alphaexchangecoin@gmail.com**.

yourchangecoin.com
<https://yourchangecoin.com> › [privacy-policy](#) ⋮

Политика Конфиденциальности

alphaexchangecoin@gmail.com. Данный запрос будет рассмотрен в срок до 30 календарных дней. Положительное решение об удалении данных может быть принято...

cryptocurrencyexchangecoin.com
<https://cryptocurrencyexchangecoin.com> › [privacy-po...](#) ⋮

Политика Конфиденциальности

alphaexchangecoin@gmail.com. Данный запрос будет рассмотрен в срок до 30 календарных дней. Положительное решение об удалении данных может быть принято...

Общие советы



1. Бесплатный сыр только в мышеловке. Никто не собирается вам помогать
2. Сохраняйте бдительность все время что вы общаетесь с незнакомыми людьми. Они вам не друзья
3. Постарайтесь как можно быстрее установить личность человека, который вам пишет. Хотя бы удостоверьтесь, что аккаунт не завели месяц назад
4. Внимательно анализируйте сайты про которые вам говорят незнакомые люди
5. Поставьте себе расширение, которое поможет обеспечить вам безопасность



Если произошло непоправимое

Переведите все средства на новый кошелек, если скомпрометирован сид

Сразу же удалите свежие approval от лица вашего адреса, например с помощью Revoke

Сообщите о мошенничестве

Поставьте уведомления на транзакции с адреса мошенника и отслеживайте их ход

Не медлите, когда мошенник захочет вывести в фиат ваши деньги

Подробный материал: [If you have been scammed...](#) от Officer

The End

СПАСИБО. ВОПРОСЫ?



https://t.me/anka_per_monetae



[osint_mindset.t.me](https://t.me/osint_mindset)



forum.osint-mindset.com