Discovering Scam Narratives on Social Media Platforms with Information Tracer

Zhouhan Chen
Founder, Safe Link Network

Anti Scam Research Group Meeting
January 24, 2023

Who am I

Zhouhan Chen

- PhD in Data Science @ New York University
- Cybersecurity researcher
- Founder @ Safe Link Network (https://safelink.network)
  - Built Information Tracer (https://informationtracer.com)
  - Built Malware Discoverer (https://malwarediscoverer.com)

Information Tracer provides automated data collection pipeline

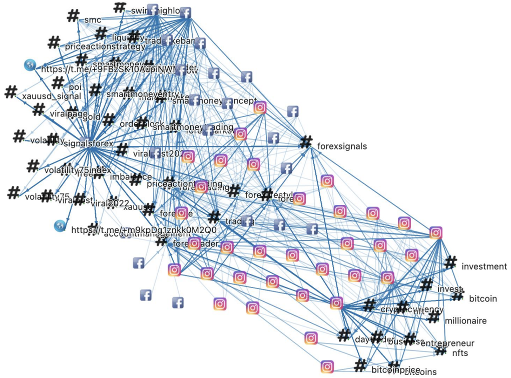
User input keywords

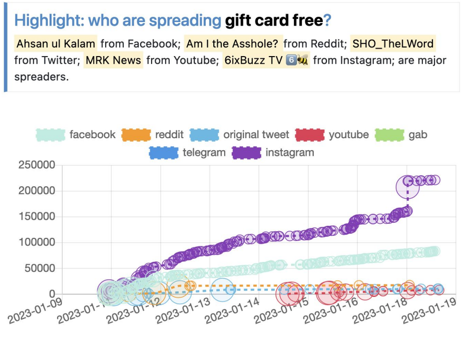
Collect posts

Generate intelligence

Share results

free giftcard





Highlight: who are spreading gift card free?

Ahsan ul Kalam from Facebook; Am I the Asshole? from Reddit; SHO_TheLWord from Twitter; MRK News from Youtube; 6ixBuzz TV 6️⃣🐝 from Instagram; are major spreaders.

To discover new scam narratives, we

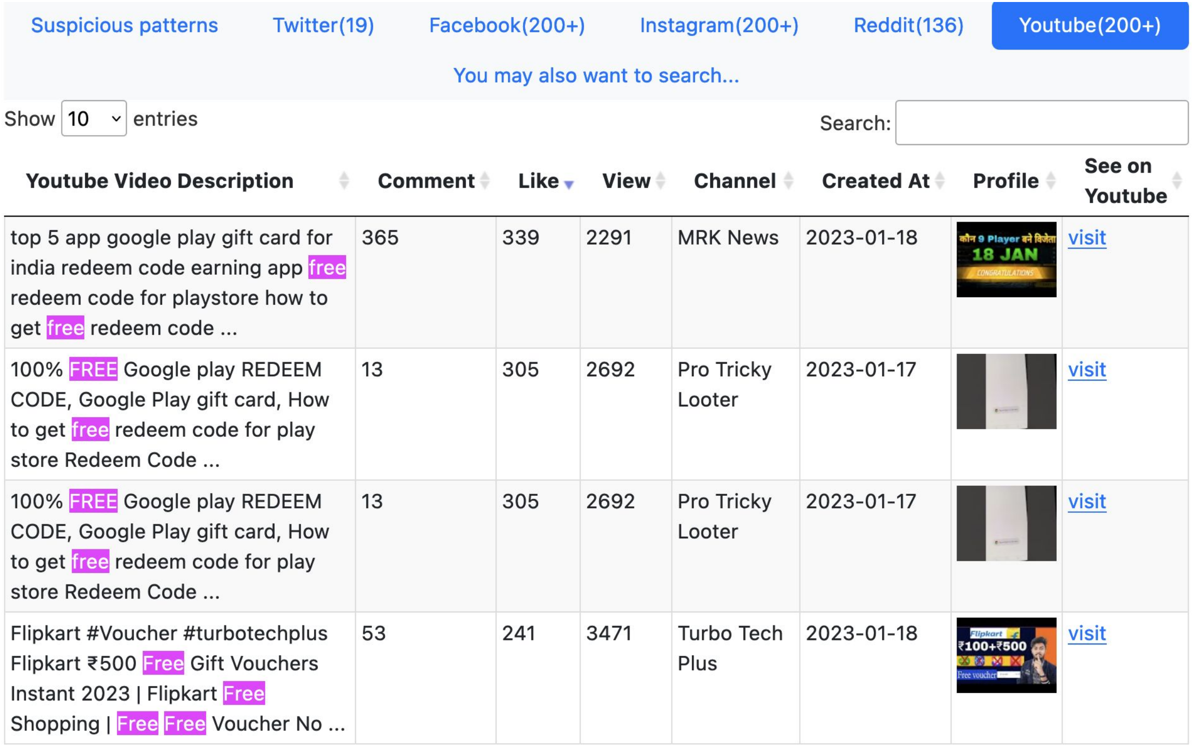
- Search for suspicious keywords
- Look at most popular posts from each platform
- Look at sharing network to identify coordinated groups
- Look at co-occurred URLs and check their reputations

We present three case studies based on three queries:

- **“free gift card”**
- “free livestream”
- “free crypto”

(data collected in January 2023)

YouTube is the top platform sharing suspicious “free gift card” narrative



Suspicious patterns Twitter(19) Facebook(200+) Instagram(200+) Reddit(136) Youtube(200+)

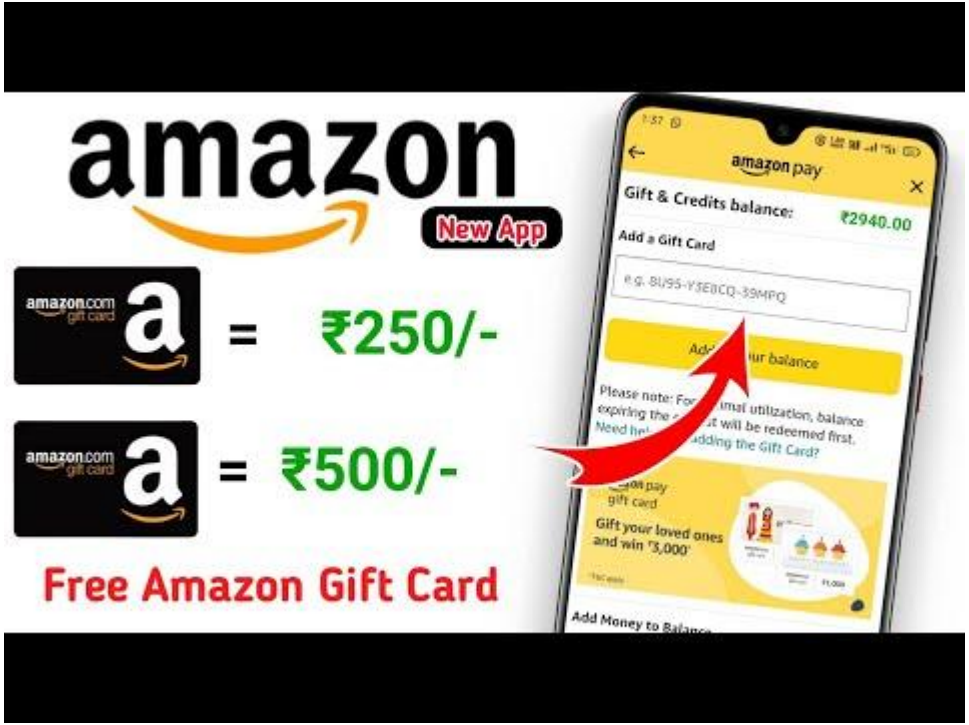
You may also want to search...

Show 10 entries

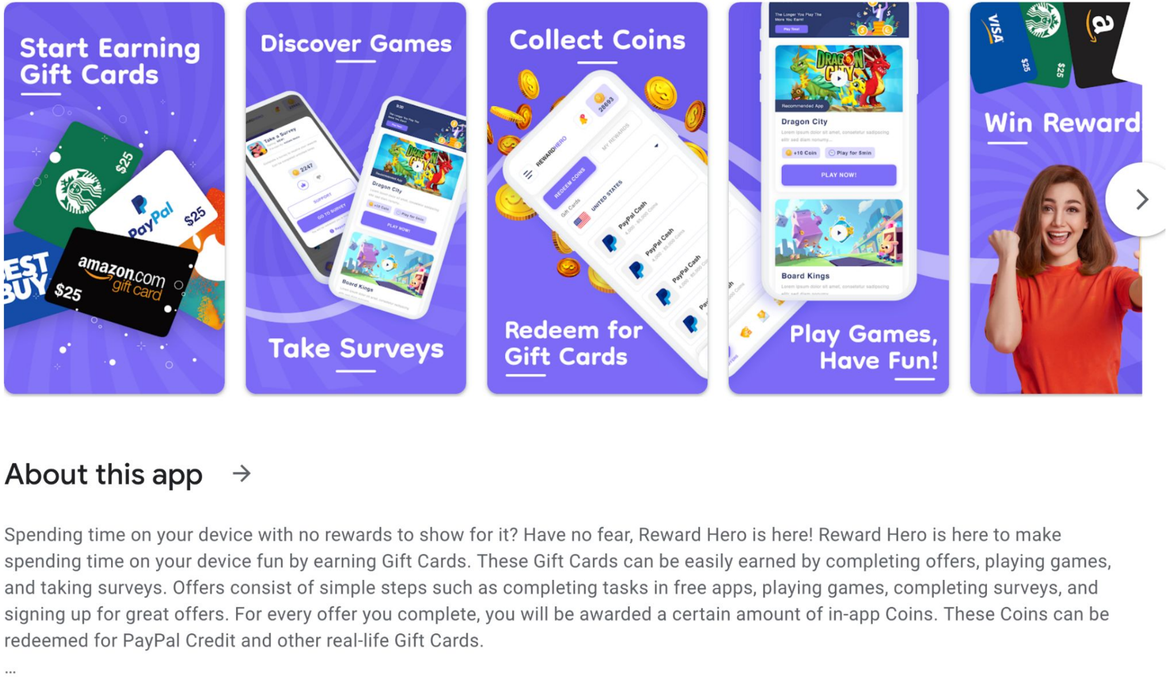
Search:

Youtube Video Description	Comment	Like	View	Channel	Created At	Profile	See on Youtube
top 5 app google play gift card for india redeem code earning app free redeem code for playstore how to get free redeem code ...	365	339	2291	MRK News	2023-01-18		visit
100% FREE Google play REDEEM CODE, Google Play gift card, How to get free redeem code for play store Redeem Code ...	13	305	2692	Pro Tricky Looter	2023-01-17		visit
100% FREE Google play REDEEM CODE, Google Play gift card, How to get free redeem code for play store Redeem Code ...	13	305	2692	Pro Tricky Looter	2023-01-17		visit
Flipkart #Voucher #turbotechplus Flipkart ₹500 Free Gift Vouchers Instant 2023 | Flipkart Free Shopping | Free Free Voucher No ...	53	241	3471	Turbo Tech Plus	2023-01-18		visit

YouTube is the top platform sharing suspicious “free gift card” narrative



Users are told to download apps, complete tasks, and earn gift cards

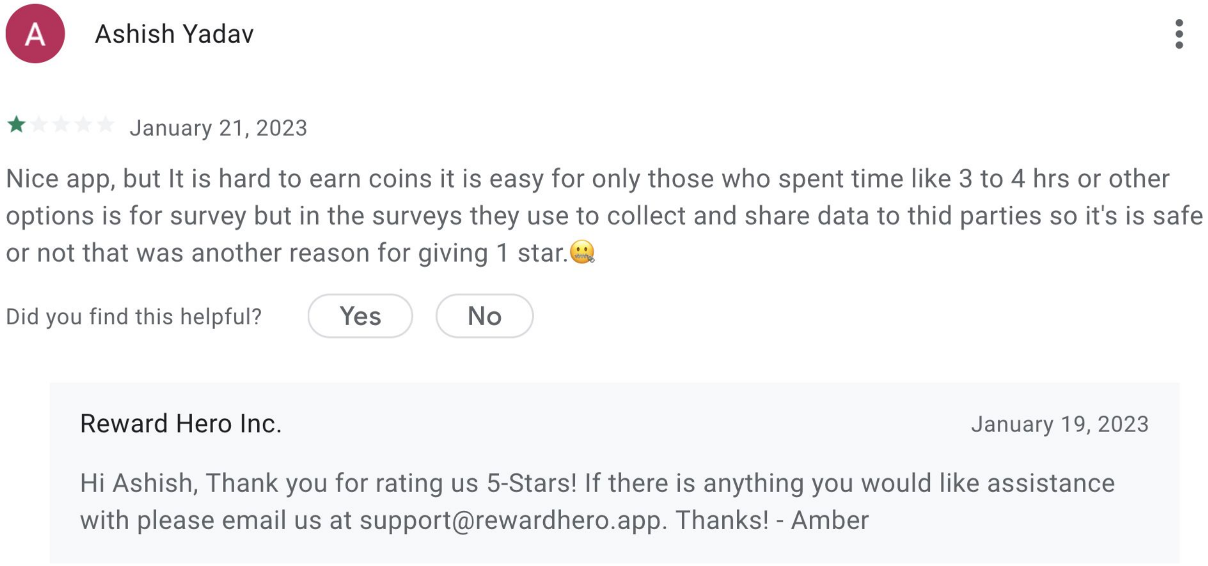


About this app →

Spending time on your device with no rewards to show for it? Have no fear, Reward Hero is here! Reward Hero is here to make spending time on your device fun by earning Gift Cards. These Gift Cards can be easily earned by completing offers, playing games, and taking surveys. Offers consist of simple steps such as completing tasks in free apps, playing games, completing surveys, and signing up for great offers. For every offer you complete, you will be awarded a certain amount of in-app Coins. These Coins can be redeemed for PayPal Credit and other real-life Gift Cards.

...

In reality, many users were just sharing personal data



Ashish Yadav

★☆☆☆☆ January 21, 2023

Nice app, but It is hard to earn coins it is easy for only those who spent time like 3 to 4 hrs or other options is for survey but in the surveys they use to collect and share data to thid parties so it's is safe or not that was another reason for giving 1 star.🤐

Did you find this helpful?

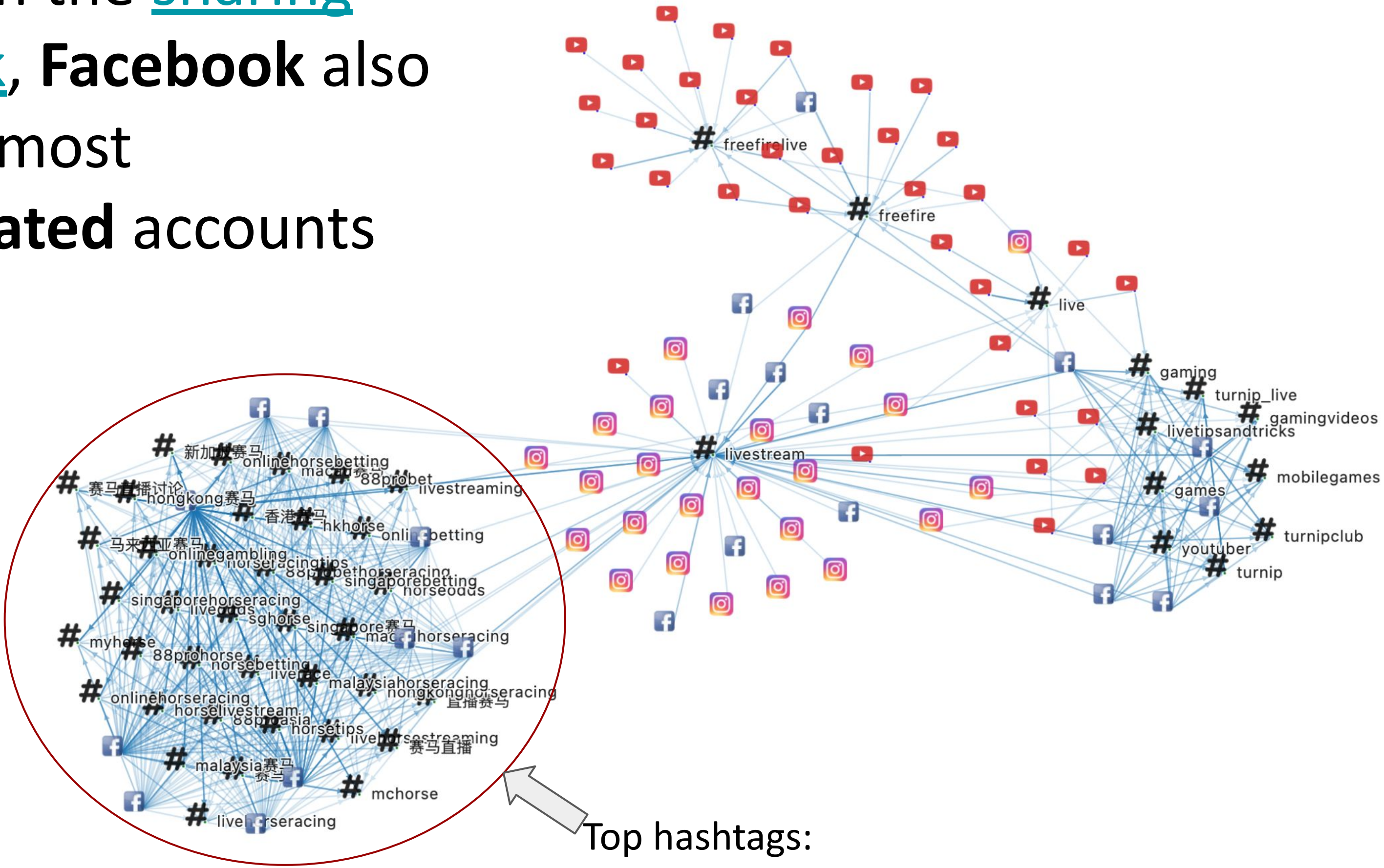
Reward Hero Inc. January 19, 2023

Hi Ashish, Thank you for rating us 5-Stars! If there is anything you would like assistance with please email us at support@rewardhero.app. Thanks! - Amber

We present three case studies based on three queries:

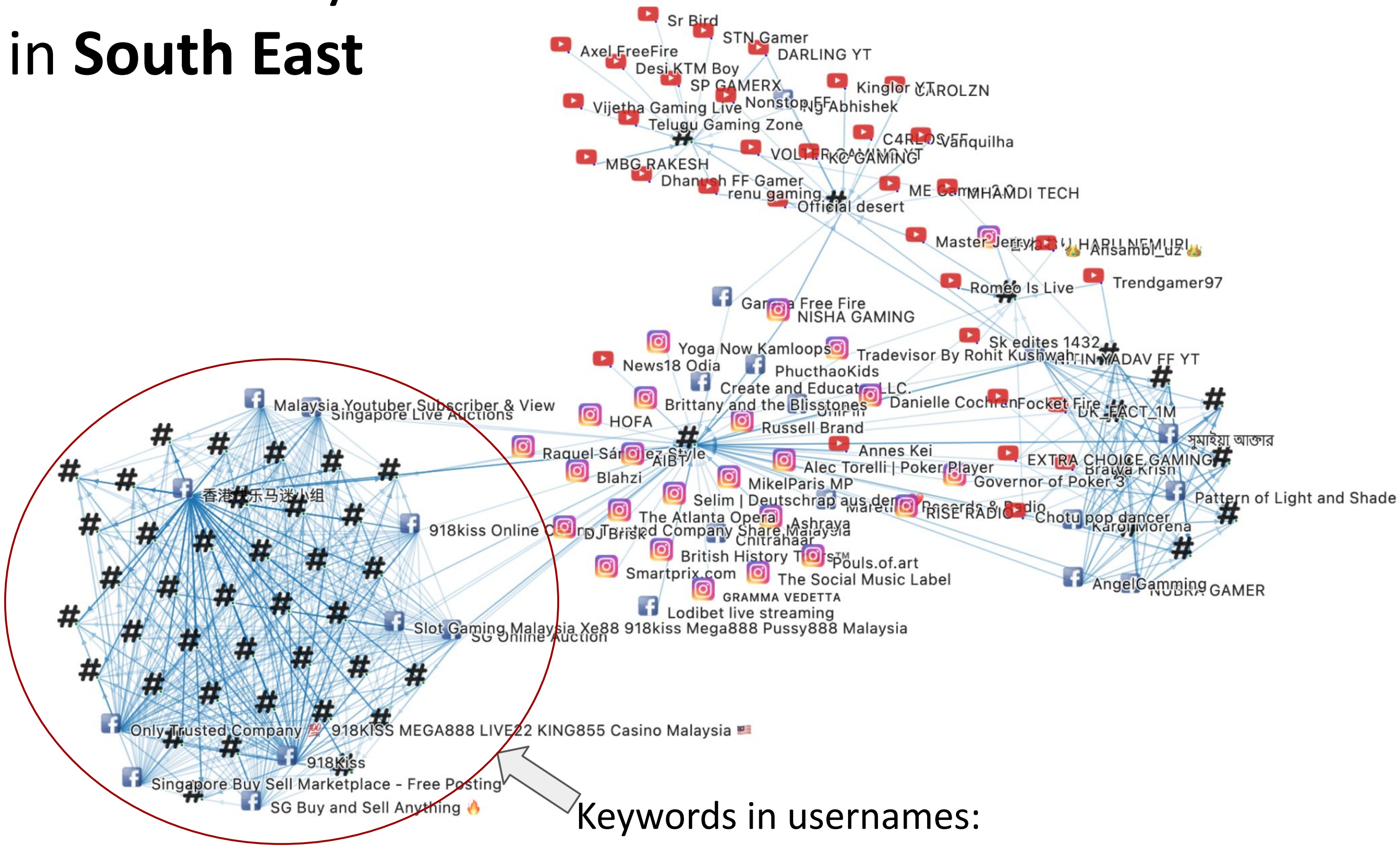
- “free gift card”
- **“free livestream”**
- “free crypto”

Based on the sharing network, **Facebook** also has the most **coordinated** accounts



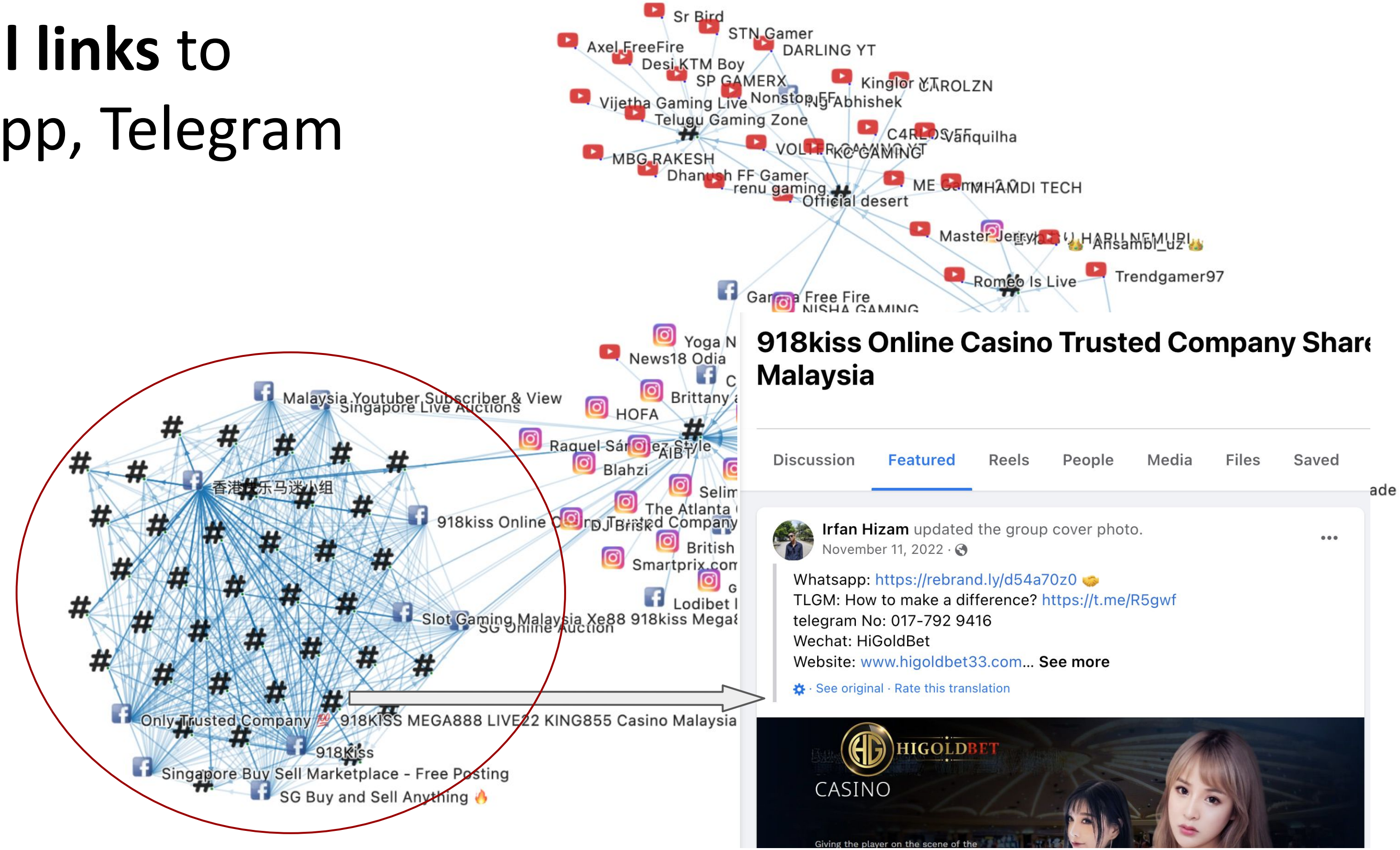
Top hashtags:
horse racing, horse betting, …

Those accounts likely operate in **South East Asia**



Keywords in usernames:
Malaysia, Singapore, …

Their posts contain **external links** to Whatsapp, Telegram



918kiss Online Casino Trusted Company Share Malaysia

Discussion | **Featured** | Reels | People | Media | Files | Saved

Irfan Hizam updated the group cover photo.
November 11, 2022 · 🌐

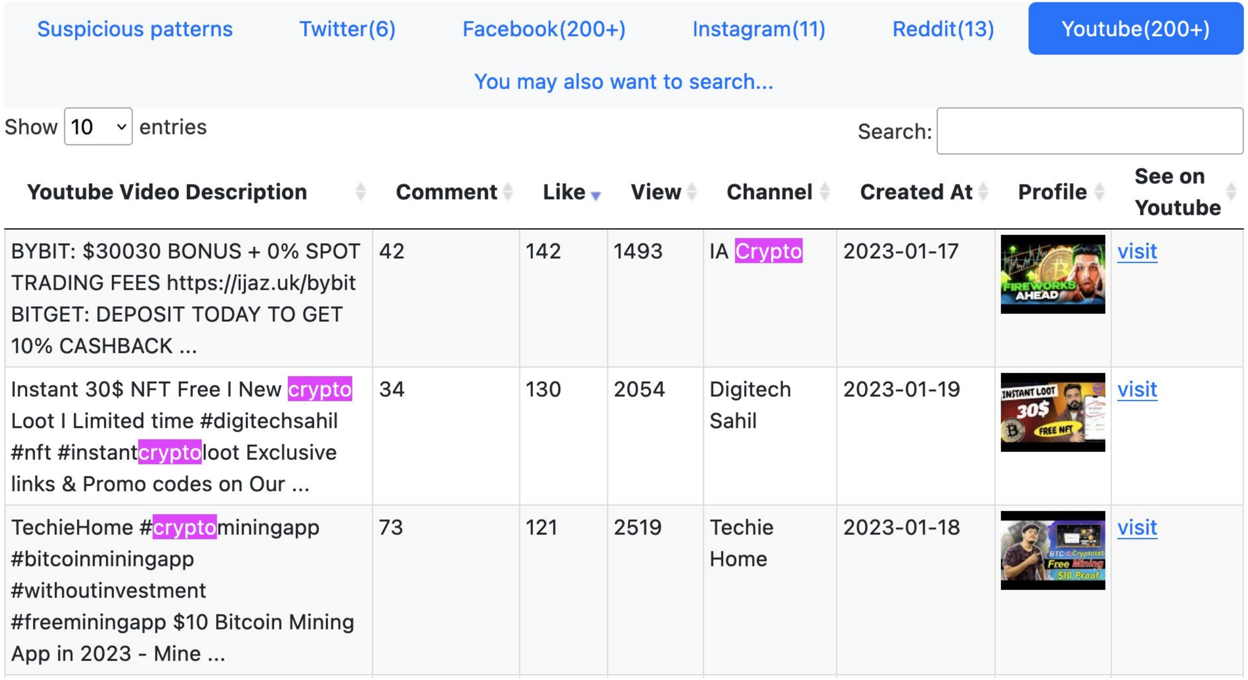
Whatsapp: https://rebrand.ly/d54a70z0 🤝
TLGM: How to make a difference? https://t.me/R5gwf
telegram No: 017-792 9416
Wechat: HiGoldBet
Website: www.higoldbet33.com... **See more**

⚙ · See original · Rate this translation

We present three case studies based on three queries:

- “free gift card”
- “free livestream”
- **“free crypto”**

Facebook, YouTube both have multiple “free crypto” scams



Suspicious patterns Twitter(6) Facebook(200+) Instagram(11) Reddit(13) Youtube(200+)

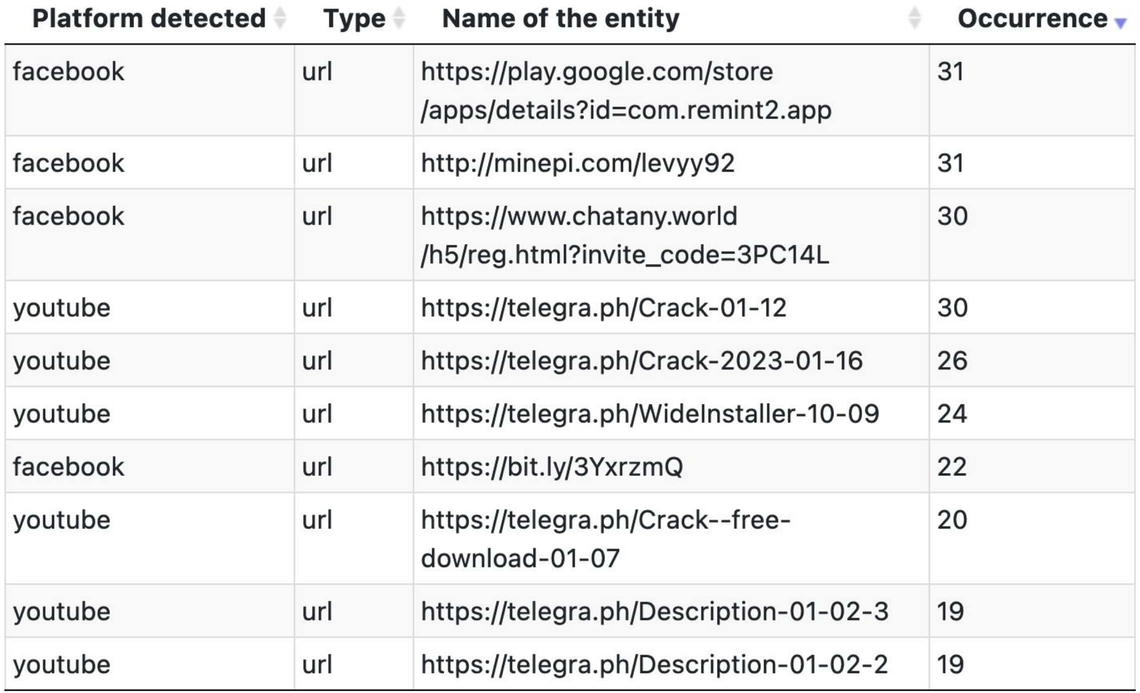
You may also want to search...

Show 10 entries

Search:

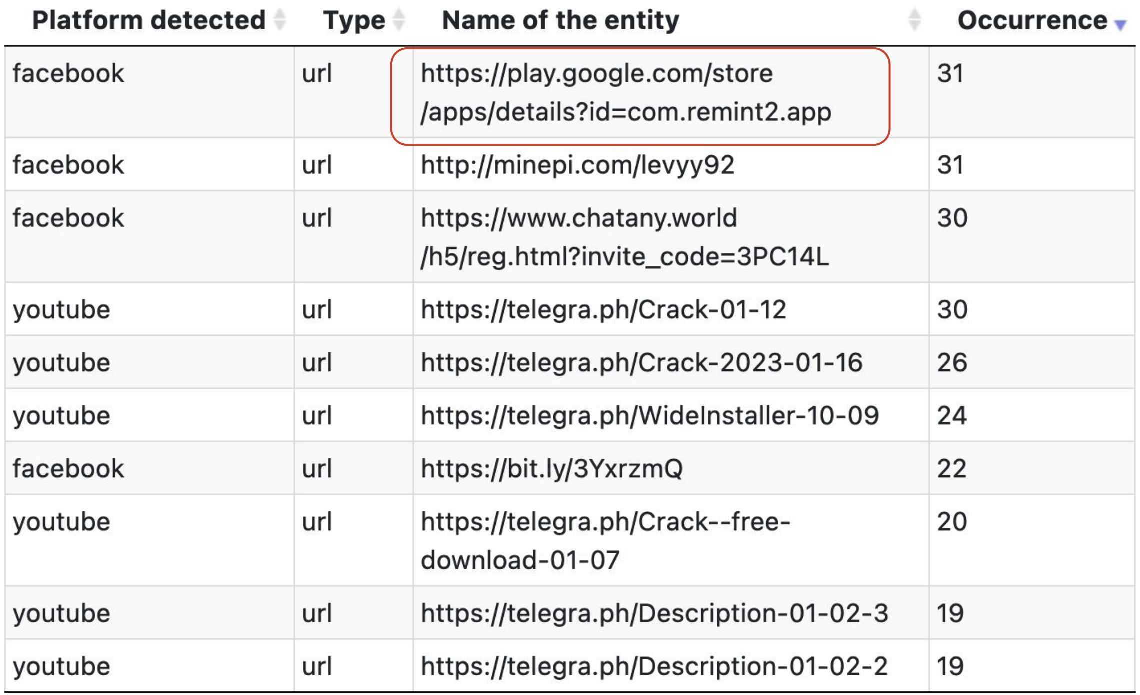
Youtube Video Description	Comment	Like	View	Channel	Created At	Profile	See on Youtube
BYBIT: $30030 BONUS + 0% SPOT TRADING FEES https://ijaz.uk/bybit BITGET: DEPOSIT TODAY TO GET 10% CASHBACK ...	42	142	1493	IA Crypto	2023-01-17		visit
Instant 30$ NFT Free I New crypto Loot I Limited time #digitechsahil #nft #instantcryptoloot Exclusive links & Promo codes on Our ...	34	130	2054	Digitech Sahil	2023-01-19		visit
TechieHome #cryptominingapp #bitcoinminingapp #withoutinvestment #freeminingapp $10 Bitcoin Mining App in 2023 - Mine ...	73	121	2519	Techie Home	2023-01-18		visit

We extract all URLs from “free crypto” posts, sort them by occurrence, and investigate top-shared URLs



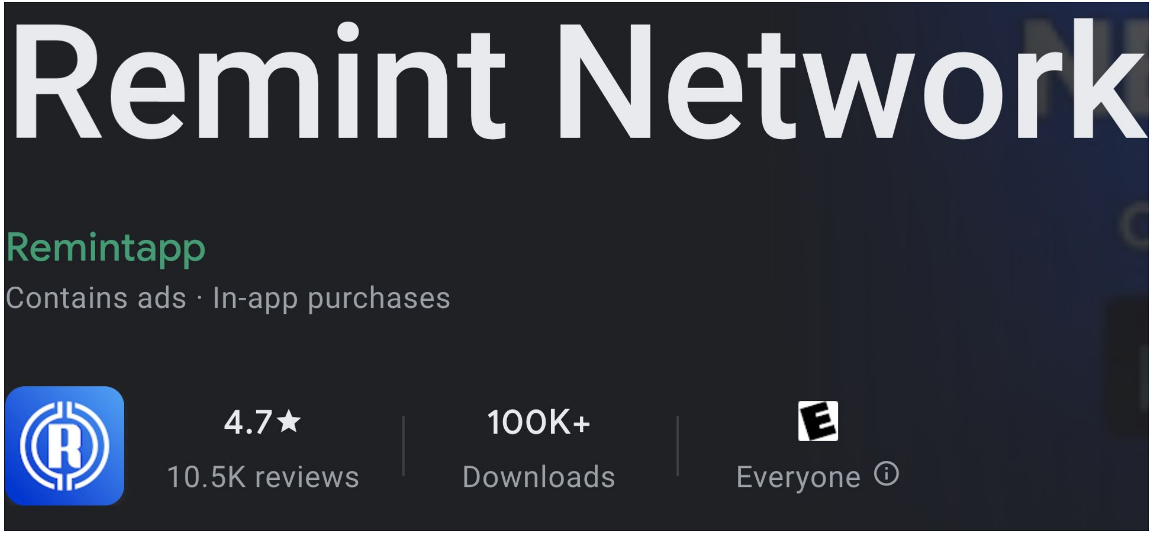
Platform detected	Type	Name of the entity	Occurrence
facebook	url	https://play.google.com/store /apps/details?id=com.remint2.app	31
facebook	url	http://minepi.com/levyy92	31
facebook	url	https://www.chatany.world /h5/reg.html?invite_code=3PC14L	30
youtube	url	https://telegra.ph/Crack-01-12	30
youtube	url	https://telegra.ph/Crack-2023-01-16	26
youtube	url	https://telegra.ph/WideInstaller-10-09	24
facebook	url	https://bit.ly/3YxrzmQ	22
youtube	url	https://telegra.ph/Crack--free-download-01-07	20
youtube	url	https://telegra.ph/Description-01-02-3	19
youtube	url	https://telegra.ph/Description-01-02-2	19

We extract all URLs from “free crypto” posts, sort them by occurrence, and investigate top-shared URLs



Platform detected	Type	Name of the entity	Occurrence
facebook	url	https://play.google.com/store /apps/details?id=com.remint2.app	31
facebook	url	http://minepi.com/levyy92	31
facebook	url	https://www.chatany.world /h5/reg.html?invite_code=3PC14L	30
youtube	url	https://telegra.ph/Crack-01-12	30
youtube	url	https://telegra.ph/Crack-2023-01-16	26
youtube	url	https://telegra.ph/WideInstaller-10-09	24
facebook	url	https://bit.ly/3YxrzmQ	22
youtube	url	https://telegra.ph/Crack--free-download-01-07	20
youtube	url	https://telegra.ph/Description-01-02-3	19
youtube	url	https://telegra.ph/Description-01-02-2	19

Scam narrative: download mobile app to mine crypto and make money



Remint Network

Remintapp

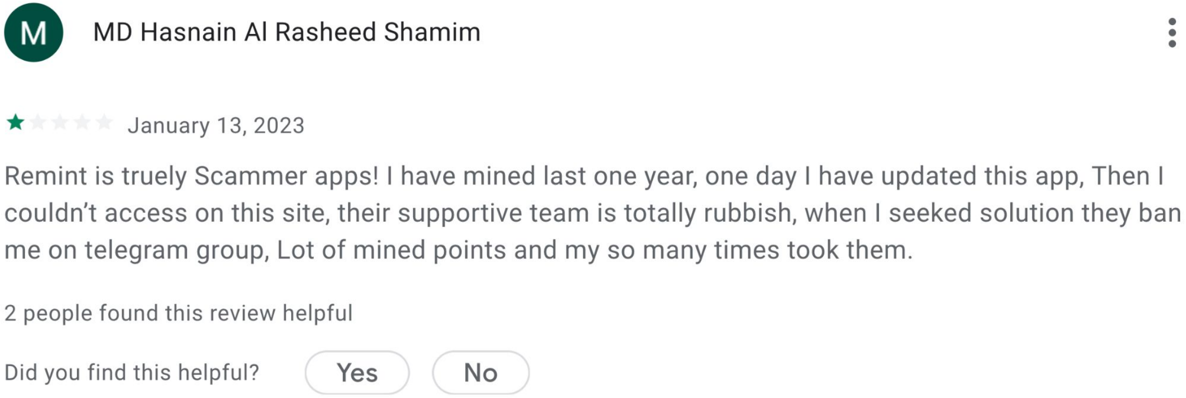
Contains ads · In-app purchases

4.7★
10.5K reviews

100K+
Downloads

E
Everyone ⓘ

Those apps do not work



MD Hasnain Al Rasheed Shamim

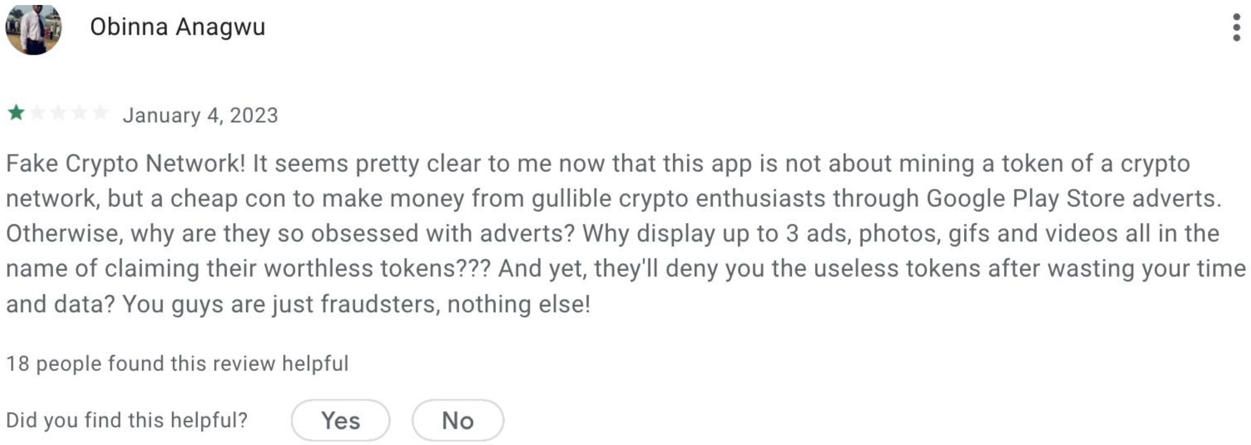
★☆☆☆☆ January 13, 2023

Remint is truely Scammer apps! I have mined last one year, one day I have updated this app, Then I couldn’t access on this site, their supportive team is totally rubbish, when I seeked solution they ban me on telegram group, Lot of mined points and my so many times took them.

2 people found this review helpful

Did you find this helpful?

There is no crypto at all



Obinna Anagwu

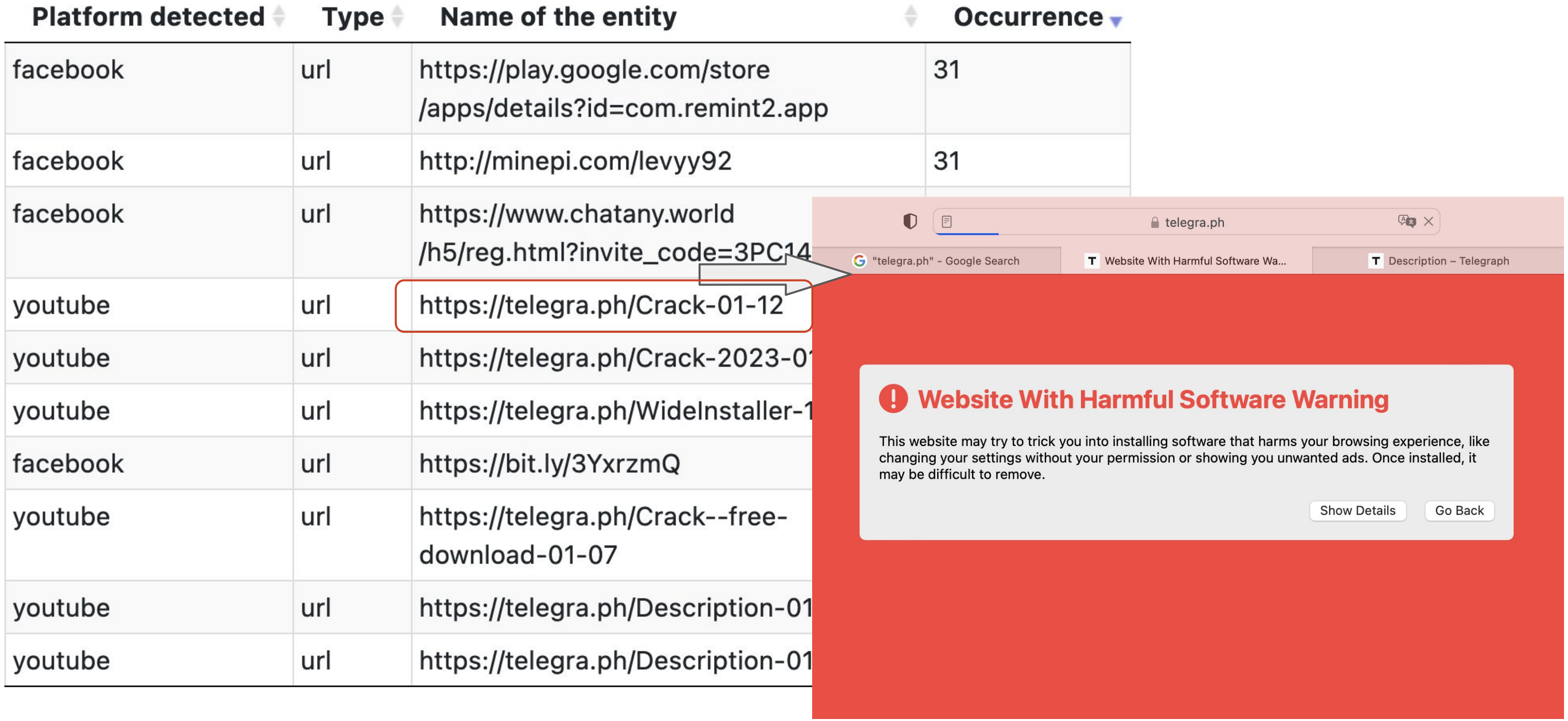
★☆☆☆☆ January 4, 2023

Fake Crypto Network! It seems pretty clear to me now that this app is not about mining a token of a crypto network, but a cheap con to make money from gullible crypto enthusiasts through Google Play Store adverts. Otherwise, why are they so obsessed with adverts? Why display up to 3 ads, photos, gifs and videos all in the name of claiming their worthless tokens??? And yet, they'll deny you the useless tokens after wasting your time and data? You guys are just fraudsters, nothing else!

18 people found this review helpful

Did you find this helpful?

Some URLs (from telegra[.]ph) are already blocked by Safari



Platform detected	Type	Name of the entity	Occurrence
facebook	url	https://play.google.com/store /apps/details?id=com.remint2.app	31
facebook	url	http://minepi.com/levyy92	31
facebook	url	https://www.chatany.world /h5/reg.html?invite_code=3PC14	
youtube	url	https://telegra.ph/Crack-01-12	
youtube	url	https://telegra.ph/Crack-2023-01	
youtube	url	https://telegra.ph/WideInstaller-1	
facebook	url	https://bit.ly/3YxrzmQ	
youtube	url	https://telegra.ph/Crack--free-download-01-07	
youtube	url	https://telegra.ph/Description-01	
youtube	url	https://telegra.ph/Description-01	

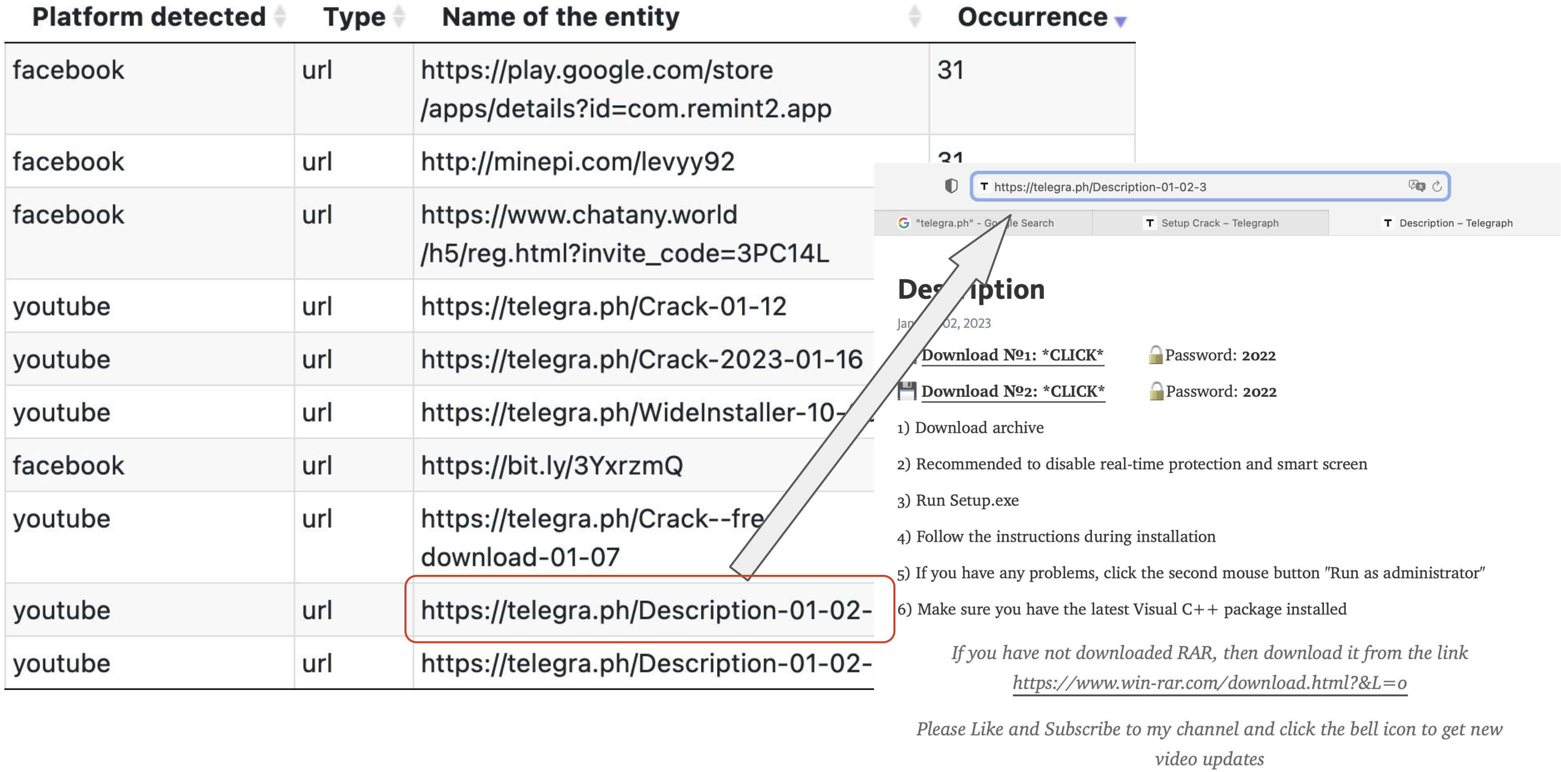
telegra.ph

"telegra.ph" - Google Search | Website With Harmful Software Wa... | Description – Telegraph

Website With Harmful Software Warning

This website may try to trick you into installing software that harms your browsing experience, like changing your settings without your permission or showing you unwanted ads. Once installed, it may be difficult to remove.

Some URLs (also from telegra[.]ph) are **not blocked** (we discovered those malicious links **earlier than browser**)



Platform detected	Type	Name of the entity	Occurrence
facebook	url	https://play.google.com/store /apps/details?id=com.remint2.app	31
facebook	url	http://minepi.com/levyy92	31
facebook	url	https://www.chatany.world /h5/reg.html?invite_code=3PC14L	
youtube	url	https://telegra.ph/Crack-01-12	
youtube	url	https://telegra.ph/Crack-2023-01-16	
youtube	url	https://telegra.ph/WideInstaller-10-	
facebook	url	https://bit.ly/3YxrzmQ	
youtube	url	https://telegra.ph/Crack--fre download-01-07	
youtube	url	https://telegra.ph/Description-01-02-	
youtube	url	https://telegra.ph/Description-01-02-	

https://telegra.ph/Description-01-02-3
"telegra.ph" - Google Search
Setup Crack – Telegraph
Description – Telegraph

Description

Jan 02, 2023

Download №1: *CLICK* 🔒Password: 2022

💾 Download №2: *CLICK* 🔒Password: 2022

1) Download archive

2) Recommended to disable real-time protection and smart screen

3) Run Setup.exe

4) Follow the instructions during installation

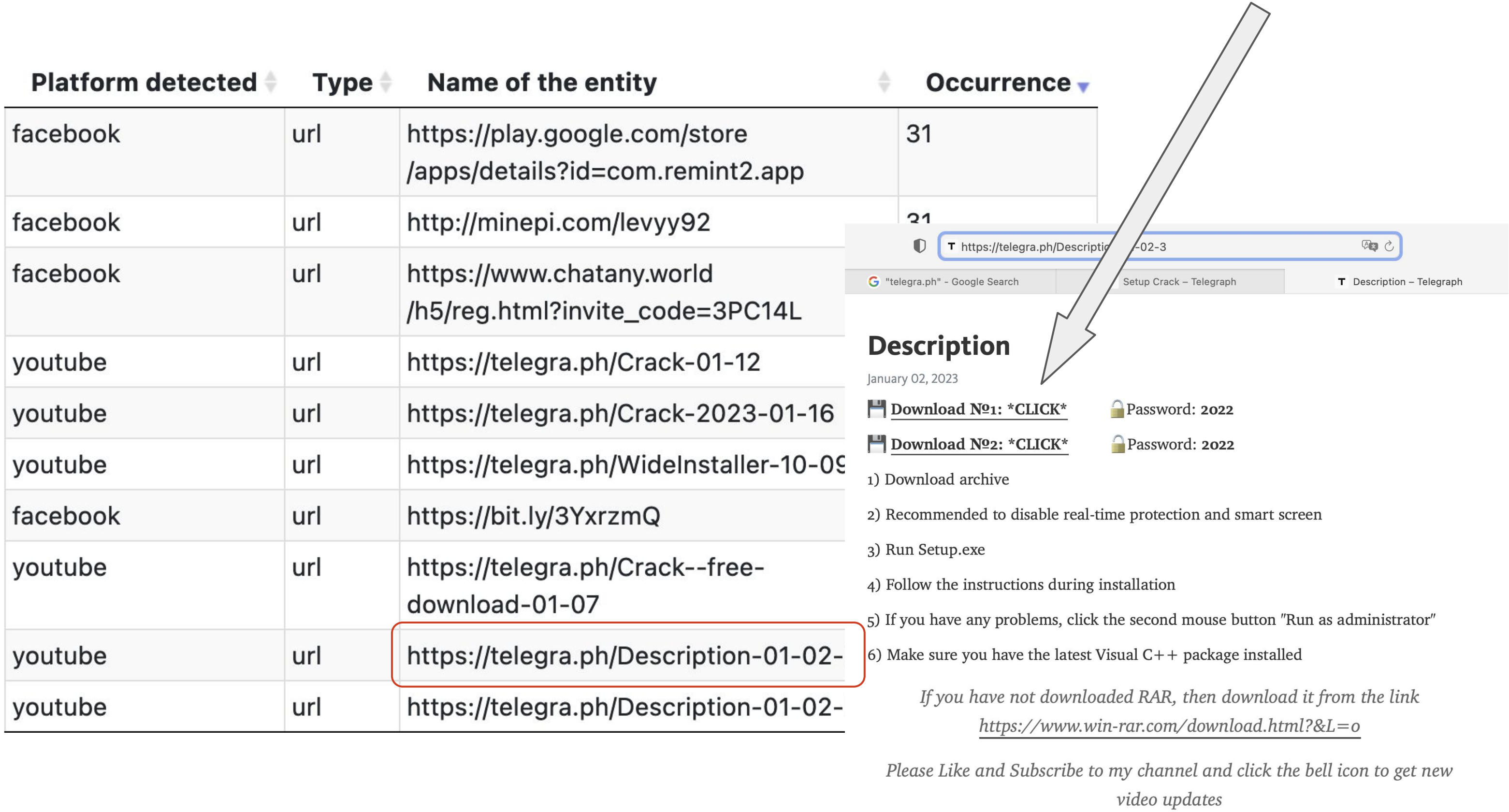
5) If you have any problems, click the second mouse button "Run as administrator"

6) Make sure you have the latest Visual C++ package installed

If you have not downloaded RAR, then download it from the link https://www.win-rar.com/download.html?&L=0

Please Like and Subscribe to my channel and click the bell icon to get new video updates

To get malicious payloads, we need to follow more redirection



Platform detected	Type	Name of the entity	Occurrence
facebook	url	https://play.google.com/store /apps/details?id=com.remint2.app	31
facebook	url	http://minepi.com/levyy92	31
facebook	url	https://www.chatany.world /h5/reg.html?invite_code=3PC14L	
youtube	url	https://telegra.ph/Crack-01-12	
youtube	url	https://telegra.ph/Crack-2023-01-16	
youtube	url	https://telegra.ph/WideInstaller-10-0	
facebook	url	https://bit.ly/3YxrzmQ	
youtube	url	https://telegra.ph/Crack--free-download-01-07	
youtube	url	https://telegra.ph/Description-01-02-	
youtube	url	https://telegra.ph/Description-01-02-	

https://telegra.ph/Descriptio -02-3
"telegra.ph" - Google Search
Setup Crack – Telegraph
Description – Telegraph

Description

January 02, 2023

💾 Download №1: *CLICK* 🔒Password: 2022

💾 Download №2: *CLICK* 🔒Password: 2022

1) Download archive

2) Recommended to disable real-time protection and smart screen

3) Run Setup.exe

4) Follow the instructions during installation

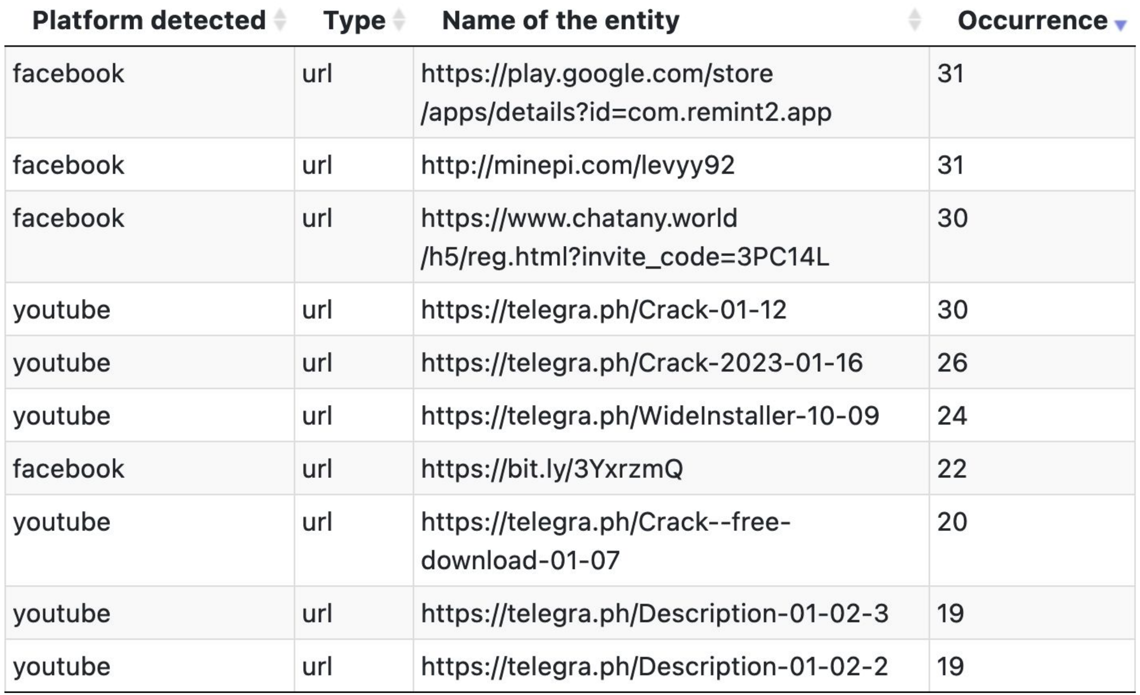
5) If you have any problems, click the second mouse button "Run as administrator"

6) Make sure you have the latest Visual C++ package installed

If you have not downloaded RAR, then download it from the link https://www.win-rar.com/download.html?&L=0

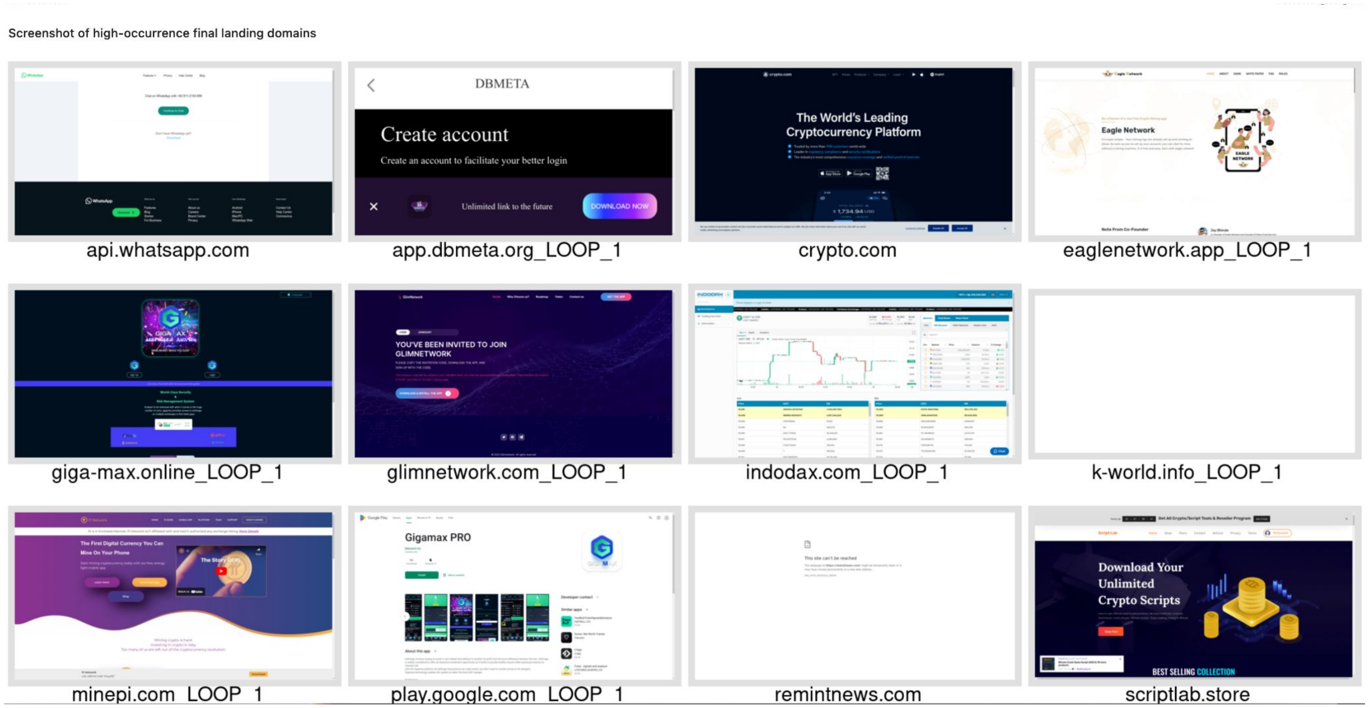
Please Like and Subscribe to my channel and click the bell icon to get new video updates

Final note: is there an easy way to visualize all those URLs, instead of copy-and-paste?



Platform detected	Type	Name of the entity	Occurrence
facebook	url	https://play.google.com/store/apps/details?id=com.remint2.app	31
facebook	url	http://minepi.com/levyy92	31
facebook	url	https://www.chatany.world/h5/reg.html?invite_code=3PC14L	30
youtube	url	https://telegra.ph/Crack-01-12	30
youtube	url	https://telegra.ph/Crack-2023-01-16	26
youtube	url	https://telegra.ph/WideInstaller-10-09	24
facebook	url	https://bit.ly/3YxrzmQ	22
youtube	url	https://telegra.ph/Crack--free-download-01-07	20
youtube	url	https://telegra.ph/Description-01-02-3	19
youtube	url	https://telegra.ph/Description-01-02-2	19

Researchers can use *Malware Discoverer* to automatically capture screenshots of many URLs, saving some time…



Screenshot of high-occurrence final landing domains

api.whatsapp.com

app.dbmeta.org_LOOP_1

crypto.com

eaglenetwork.app_LOOP_1

giga-max.online_LOOP_1

glimnetwork.com_LOOP_1

indodax.com_LOOP_1

k-world.info_LOOP_1

minepi.com_LOOP_1

play.google.com_LOOP_1

remintnews.com

scriptlab.store

DBMETA
Create account
Create an account to facilitate your better login
Unlimited link to the future
DOWNLOAD NOW
The World's Leading Cryptocurrency Platform
Eagle Network
YOU'VE BEEN INVITED TO JOIN GLIMNETWORK
The First Digital Currency You Can Mine On Your Phone
Gigamax PRO
This site can't be reached
Download Your Unlimited Crypto Scripts
BEST SELLING COLLECTION

Discussion

- Are those narratives same across channels?
- What else do you want to search?
- Remediation: what do we do when we find malicious URLs/users?

Thanks for listening!

https://informationtracer.com

Email: zhouhan.chen@nyu.edu