Stony Brook University PragSec Lab Ethos

Like, Comment, Get Scammed:
Characterizing Comment Scams on Media Platforms

Xigao Li, Amir Rahmati, Nick Nikiforakis

Introducing Comment Scams

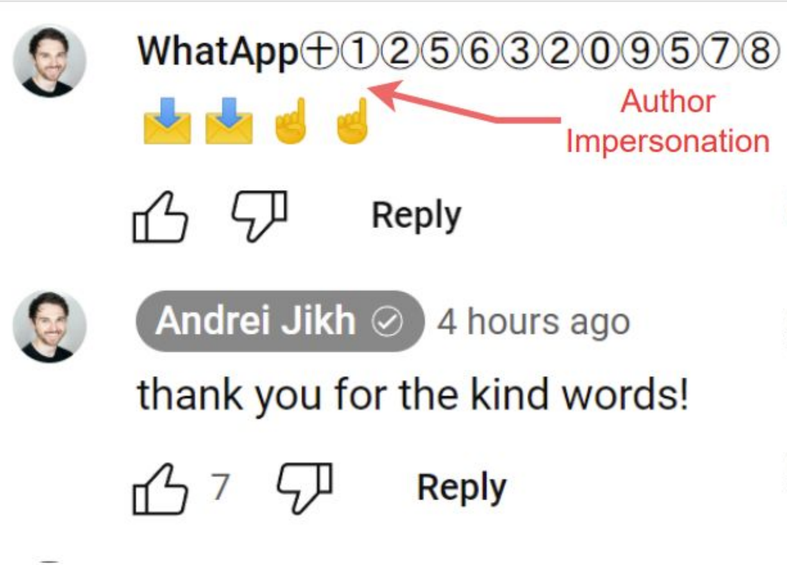
Comment scam on media platforms

- Comments or replies, enticing users to contact them through messages
- Solicit a chance to win a gift or investment opportunities
- Example: *“TextMe on WhatsApp (555)-5555”*

.

Example of Comment Scam

- **Scammers apply multiple tactics to evade platform restrictions**



WhatApp⊕①②⑤⑥③②⓪⑨⑤⑦⑧

📩📩☝☝

Author Impersonation

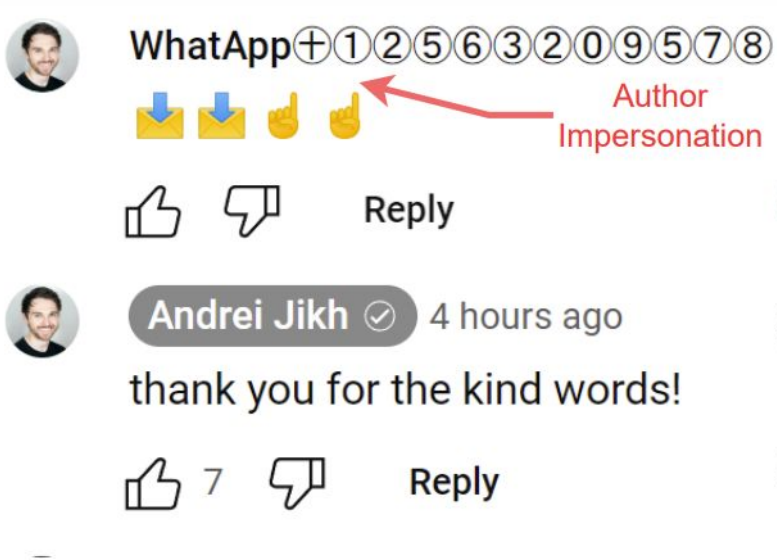
Andrei Jikh ✓ 4 hours ago

thank you for the kind words!

(a)

Example of Comment Scam

- **Scammers apply multiple tactics to evade platform restrictions**



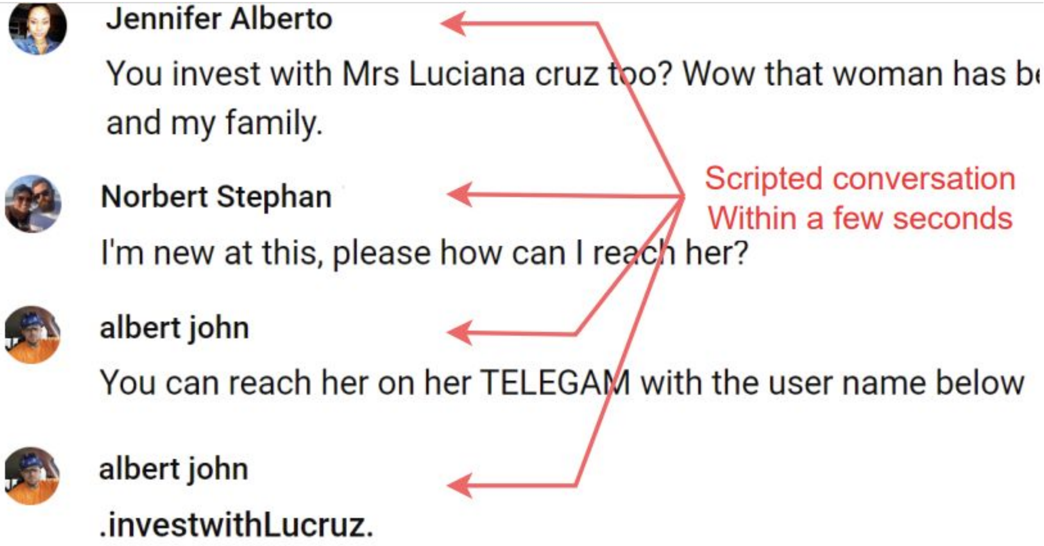
WhatApp⊕①②⑤⑥③②⓪⑨⑤⑦⑧
📩📩☝☝

Author Impersonation

Andrei Jikh ✓ 4 hours ago

thank you for the kind words!

(a)



Jennifer Alberto
You invest with Mrs Luciana cruz too? Wow that woman has b
and my family.

Norbert Stephan
I'm new at this, please how can I reach her?

albert john
You can reach her on her TELEGAM with the user name below

albert john
.investwithLucruz.

Scripted conversation
Within a few seconds

(b)

Overview

- Build a reliable infrastructure monitoring YouTube comments
    - Monitor past and new videos in popular YouTube channels
    - Periodically take snapshots of comment sections
- Design heuristic filters to identify scam comments
- Interact with actual Scammers via Text Messages
    - Reveal scammers’ tactics and monetization techniques

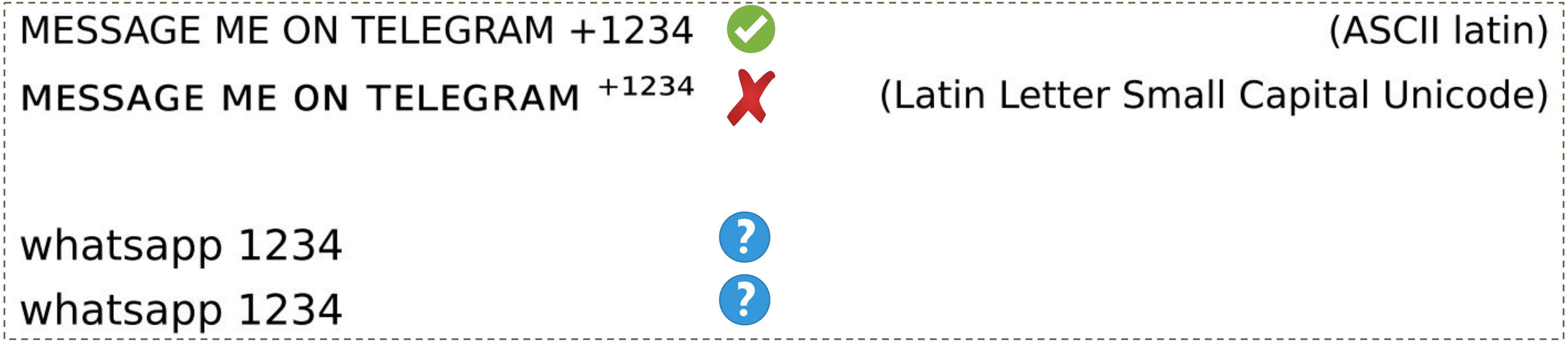
Dataset Collection

- Measurement range: October 1st, 2022 to March 31st, 2023
- Monitored Channels: 20
    - Cooking / Sports / Finance etc.
- Videos: 8,226
- Captured comments: 8.8 Million
- Filtered scam comments: 206K (2.34% of total comments)

Comment Scam Features

- **Textual -** Scammers use Visually Similar Symbols (VSS) to evade automated detection systems
- **Graphical -** Scammers apply similar profile images to impersonate channel owners
- **Temporal -** Scammers split the conversation and even contact phone numbers, and use multiple accounts to post them together to form a fabricated short story

Comment Scam Features



MESSAGE ME ON TELEGRAM +1234 ✓ (ASCII latin)

ᴍᴇssᴀɢᴇ ᴍᴇ ᴏɴ ᴛᴇʟᴇɢʀᴀᴍ ⁺¹²³⁴ ✗ (Latin Letter Small Capital Unicode)

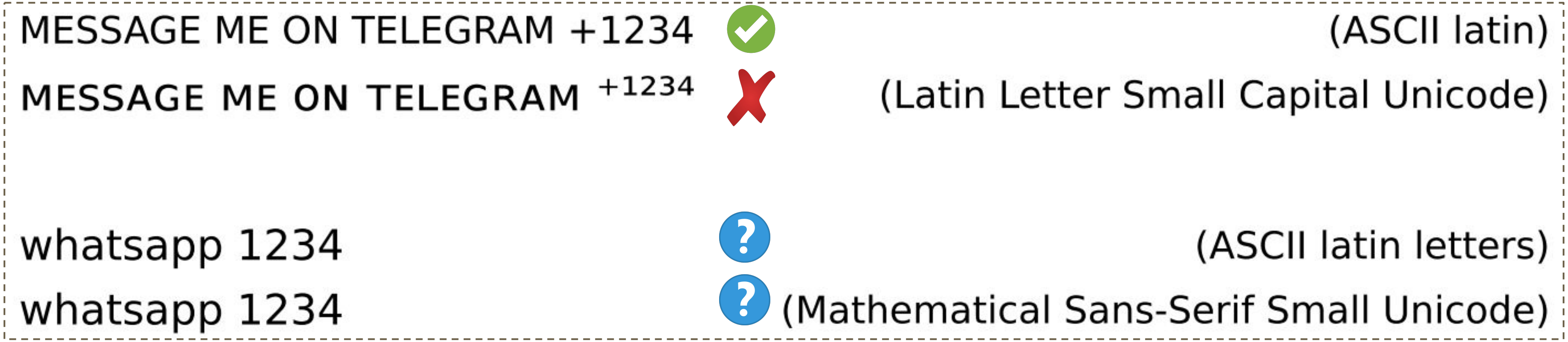
whatsapp 1234 ?

whatsapp 1234 ?

Visually Similar Symbols (VSS)

- a **(U+0061) vs a (U+1D5BA)**

Comment Scam Features



MESSAGE ME ON TELEGRAM +1234 ✓ (ASCII latin)

ᴍᴇꜱꜱᴀɢᴇ ᴍᴇ ᴏɴ ᴛᴇʟᴇɢʀᴀᴍ ⁺¹²³⁴ ✗ (Latin Letter Small Capital Unicode)

whatsapp 1234 ? (ASCII latin letters)

𝗐𝗁𝖺𝗍𝗌𝖺𝗉𝗉 𝟣𝟤𝟥𝟦 ? (Mathematical Sans-Serif Small Unicode)

Visually Similar Symbols (VSS)

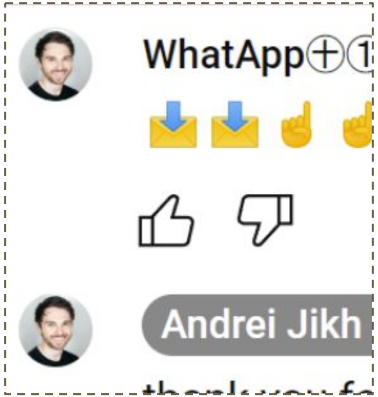
- a **(U+0061) vs 𝖺 (U+1D5BA)**

Comment Scam Features

- **Textual -** Scammers use Visually Similar Symbols (VSS) to evade automated detection systems
- **Graphical -** Scammers apply similar profile images to impersonate channel owners
- **Temporal -** Scammers split the conversation and even contact phone numbers, and use multiple accounts to post them together to form a fabricated short story

Comment Scam Features

- **Graphical -** Scammers apply similar profile images to impersonate channel owners
  - Difficult to distinguish in the view of inexperienced users
  - Perceptual hashing to compare with channel owners



WhatApp⊕1

📩📩☝☝

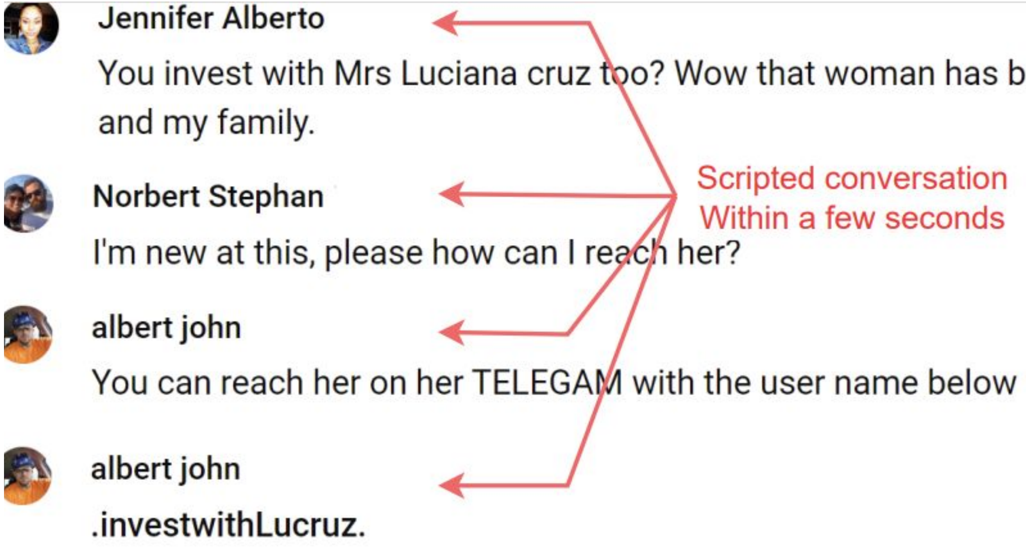
Andrei Jikh

Comment Scam Features

- **Textual -** Scammers use Visually Similar Symbols (VSS) to evade automated detection systems
- **Graphical -** Scammers apply similar profile images to impersonate channel owners
- **Temporal** - Scammers split the conversation and even contact phone numbers, using multiple accounts to form a fabricated short story

Comment Scam Features

- **Temporal -** Scammers fabricate story and use multiple accounts to post them at the same time
  - Multiple accounts used
  - Most difficult to detect



Jennifer Alberto

You invest with Mrs Luciana cruz too? Wow that woman has b and my family.

Norbert Stephan

I'm new at this, please how can I reach her?

albert john

You can reach her on her TELEGAM with the user name below

albert john

.investwithLucruz.

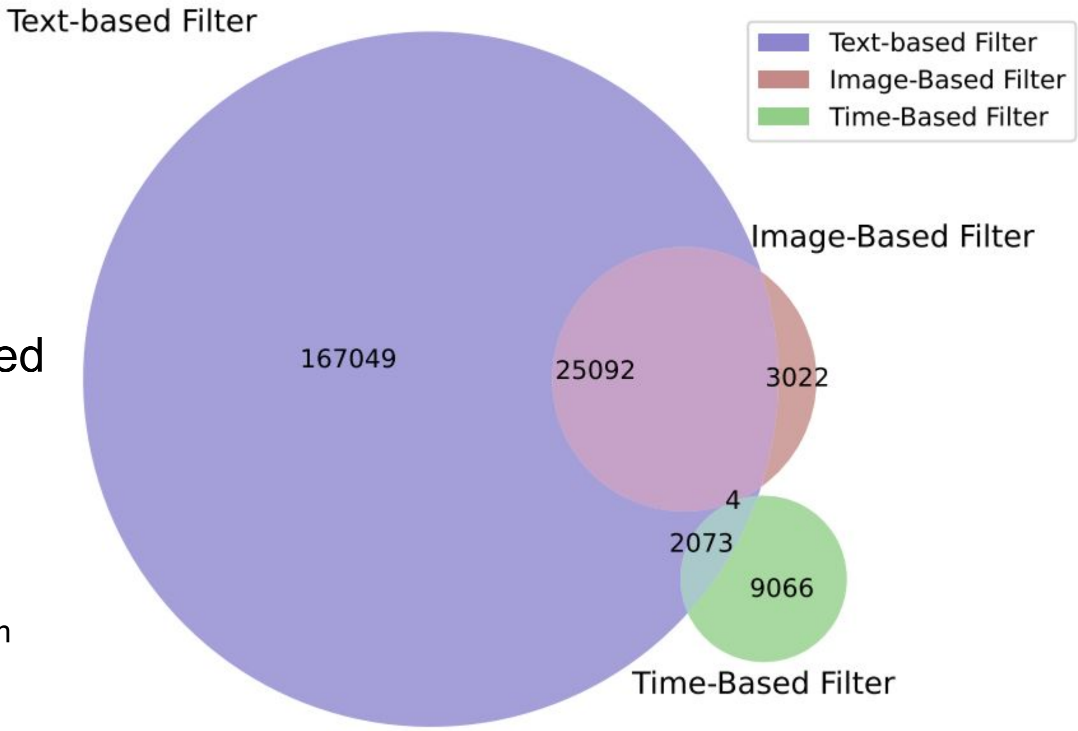
Scripted conversation
Within a few seconds

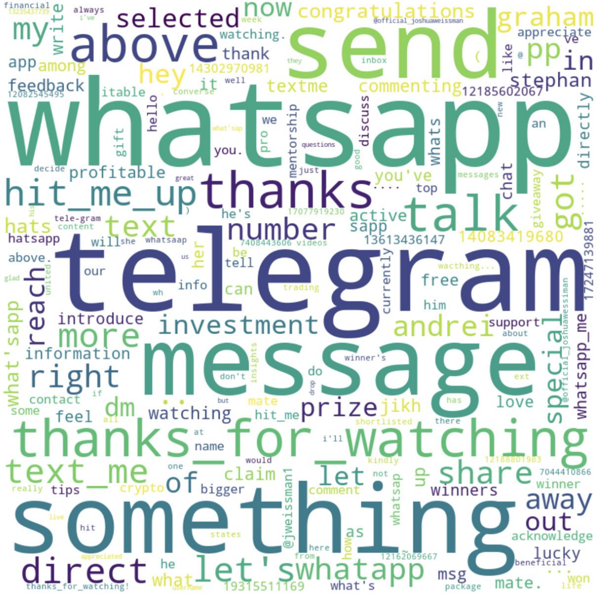
(b)

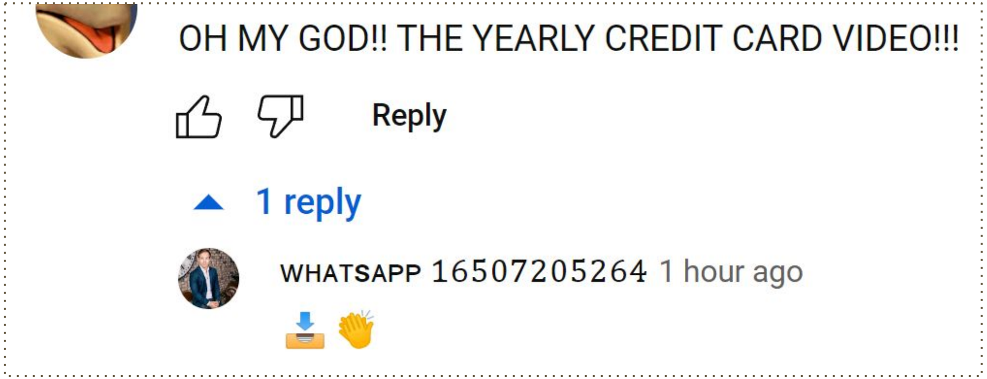
Filter results

- Text-based filters captured the majority of scam comments
- A single comment can be labelled with multiple filters
- Filters have intersections

  (Scammers use multiple ways to evade platform restrictions)







OH MY GOD!! THE YEARLY CREDIT CARD VIDEO!!!

Reply

1 reply

WHATSAPP 16507205264 1 hour ago

📥👏

Scammer text

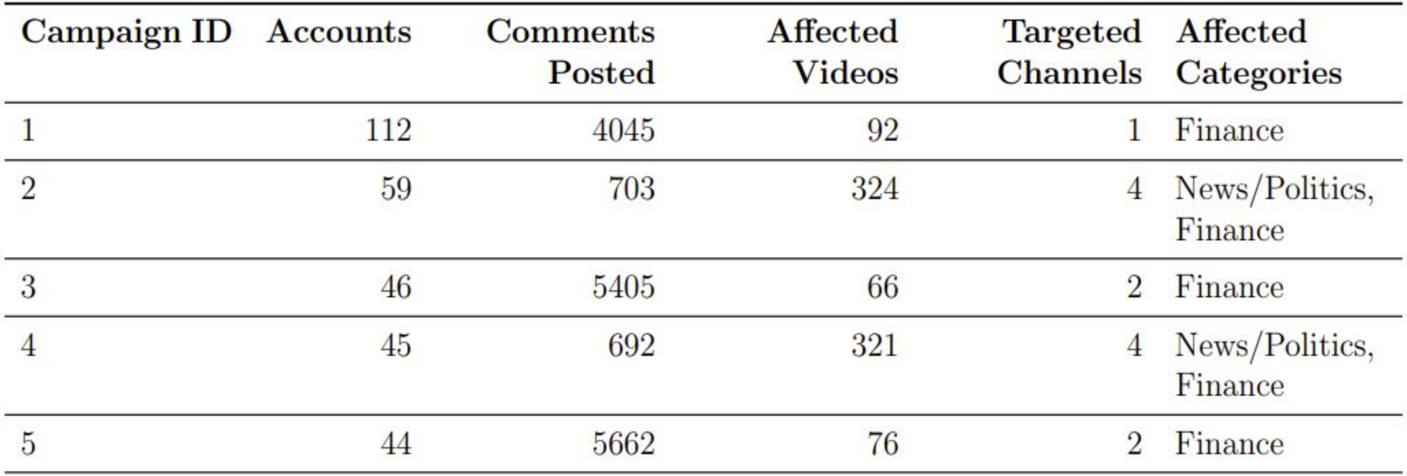
- Convey general information (no specific target)
- Entice users to contact them (on other platforms)
- Impersonate or fabricate (increase credibility)
- Automated through scripts (widespread)

Scam Campaigns

Connect campaigns by phone numbers and account IDs

- If (YouTube) account A and B share same phone - cluster A/B into same campaign
- If account A have phone number X and Y - cluster X/Y into the same campaign
- Iterate until all clusters have stabilized

Scam Campaigns



Campaign ID	Accounts	Comments Posted	Affected Videos	Targeted Channels	Affected Categories
1	112	4045	92	1	Finance
2	59	703	324	4	News/Politics, Finance
3	46	5405	66	2	Finance
4	45	692	321	4	News/Politics, Finance
5	44	5662	76	2	Finance

- Largest campaign had 112 accounts
- Most widespread campaign targeted 324 videos
- Only 31.42% scam accounts were deactivated during study

Interacting with scammers

- IRB-approved study
- Pretend to be unaware users and send text messages to 50 scammers
- Explore scammer tactics and payment channels
- Platforms: WhatsApp and Telegram

Interactions (IRB-approved)

- Pretend to be unaware users (prospective victims)
  - Inexperienced with cryptocurrency / trading
- Answer scammers’ questions with polite/positive attitude
- Collect chat text records from scammers
  - Chat history - WhatsApp and Telegram
  - Websites
  - Payment channels

Scammer tactics / payment channels

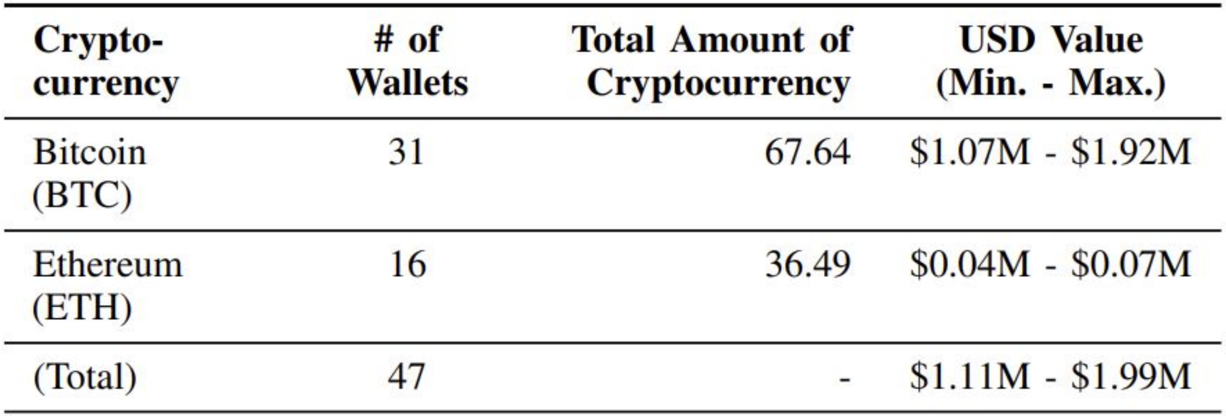
- **Cryptocurrency Investments (76%)**
  - Promise unrealistic high-yield investments (15% to 1300% weekly return)
  - Impersonation as a channel owner or broker
  - Entice users to transfer cryptocurrency to scammer’s wallet

- **Fake Prize (22%)**
  - Promise a prize (usually related to channel content)
  - Request shipping charges ($50 to $500)
- **Others (2%) -** a scammer offers paid courses

Funds stolen (cryptocurrency)

- Scammers prefer cryptocurrencies for investment payments - those wallets are publicly accessible on their blockchains
- Track scammer wallets found in interactions
- Calculate total amount of funds transferred to scammers' wallets

Funds stolen (cryptocurrency)



Crypto-currency	# of Wallets	Total Amount of Cryptocurrency	USD Value (Min. - Max.)
Bitcoin (BTC)	31	67.64	$1.07M - $1.92M
Ethereum (ETH)	16	36.49	$0.04M - $0.07M
(Total)	47	-	$1.11M - $1.99M

Millions of dollars (equivalent) were stolen by a small group of scammers

Summary

- Scammers post comment replies under popular YouTube channels
  - Multiple tactics to evade platform regulations
- 208K scam comments were captured in a 6-month period
- Users are enticed to reach out over different platforms (WhatsApp, Telegram)
- User Study: Interacted with 50 scammers
  - Millions of dollars were stolen by a small group of scammers via cryptocurrencies
- Crawler Code is accessible at: https://like-comment-get-scammed.github.io/

Like, Comment, Get Scammed:

Characterizing Comment Scams on Media Platforms

Xigao Li, Amir Rahmati, Nick Nikiforakis

https://like-comment-get-scammed.github.io/