Unveiling the Pig Butchering Scam: Deceptive Tactics Exposed

Analysis of Recurring Investment Scams that impersonate Major Brands, promoted through YouTube and Telegram Platforms since 2022

Author: Noel Varghese

INDUSTRY:
CYBERSECURITY & IT

REGION:
GLOBAL

White papers and reports can be downloaded from the CloudSEK website by visiting https://cloudsek.com/whitepapers-reports or by mailing to info@cloudsek.com.

Since 2022, CloudSEK's researchers have been tracking a wide net of investment scam instances, where registered trademarks and brand names of major global brands were being abused to propagate fraudulent investment and task-based reward schemes. Due to financially motivated threat actors being able to capitalize on the gullibility of humans with deposit - instant money return schemes, since the advent of COVID-19 Pandemic, it's no surprise that multiple complaints against some of the impersonated brands have propped up on social media and especially on unofficial Consumer Complaint boards on the Internet.

These schemes are also promoted in the guise of "Work from Home Jobs" and are primarily spread through ads on Facebook, Instagram and videos on Youtube. Youtube, as a medium, has started to be abused for targeted investment scam attempts against Organizations since 2022, according to our research, which corresponds with inputs from Google Trends. Over time, it progresses into an MLM Scheme requiring existing investors to refer acquaintances to gain referral bonuses and in hindsight, increasing the count of victims and the illicit proceeds harvested from the scam.

It is interesting to note that the Manufacturing, Energy and Technology industries were being actively targeted by this threat. Companies, who operate in this industry and whose trademarks are being abused to propagate these scams are not aware of such incidents, unless explicitly reported to them. Credibility, brand reputation and trust placed on the general public on these brands gets tarnished inadvertently through these scams. This is to iterate that any well established company, irrespective of industry can be targeted through such direct scams.

Telegram has emerged as a hotspot to increase the reach of such fraudulent investment ventures through channels run by Indian Youtubers. Additionally, proper due diligence is not followed by individuals to verify it's authenticity, before taking the fatal leap to financial obscurity.

Through our research, we have found that approximately 260 global companies with prominent presence in various industries have been subjected to such impersonation scams, during the timeline of our investigation . CloudSEK's analysis of similar incidents in the past suggests that the scam operations are orchestrated by Chinese masterminds.

This whitepaper will try to elucidate the efforts taken by scammers to land victims and the whole ecosystem of such fraudulent scams. It tries to stress the fact that any company with significant brand recognition should be wary of similar impersonation scams. By tracking such scam campaigns over time, it is evident that major brands from outside India have been affected by the active threat.

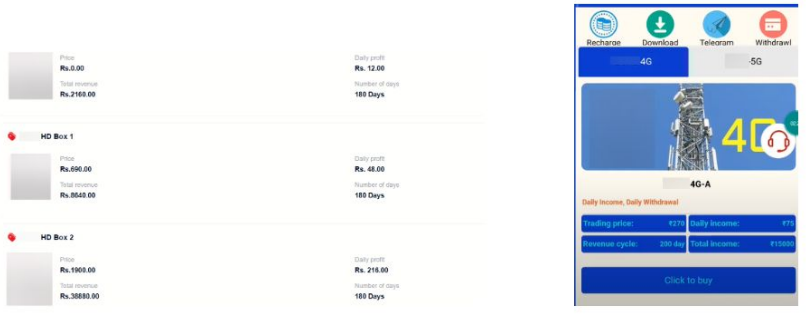


Figure 1 - Screenshots from Fraudulent Investment Scam Campaigns that were targeting Indian Telecom Giants

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

Promotion of fake Investment Scheme to Individuals : Through Messaging Platforms and Youtube

The initial discovery of the campaign, where Youtube Videos were propagating the scams was flagged by CloudSEK's contextual AI driven Digital Risk protection platform XVigil for multiple customers, whose brand names and logos were being misused to launch investment schemes without their knowledge. Indian YouTubers proceed to promote these scam websites on their Youtube channels and also ask the users to join their Telegram channels leading to the users becoming ingrained into the scam ecosystem where new *"investment platforms"* are promoted successively. This will be explained in detail, in the following section.

While conducting research on the topic, the researcher came across similar reviews/anecdotes shared by other individuals who have been trapped in similar scams in the past. It shows that Whatsapp and Emails have been used by scammers to touch base with victims, where an unintended message reaches the wrong recipient, leading to initiation of a conversation between the two individuals. Once a connection has been established, the subject of the investment scheme is subtly hinted at, with the scammer placing himself as a guarantee for the promised profits, once the initial deposit is made. This is a tactic which was explained by Trend Micro in their research blog centring around the same scam scenario.

This additionally shares an overlap with catfishing scams observed on social media, where fake personas are created to lure in unsuspecting people to invest in unknown and suspicious crypto pyramid or ponzi schemes. Instagram and Facebook Ads have been abused in the same manner to propagate such scams.

The attraction of making a quick buck, with promised returns within a certain time frame, leads people to invest blindly into the scheme. Factors such as Social Engineering the victim into making the investment, under false pretenses and lack of conducting proactive diligence on making sure whether the scheme is indeed legitimate, leads to people losing their savings overnight, to an impersonator venture.

These classes of scams can additionally be dubbed as "pig butchering", because pigs (swine) are provided copious amounts of food to eat, resulting in an accelerated rate of growth in order to slaughter them within a shorter amount of time. Correlating this with the concept of the class of scam being discussed in this whitepaper, scammers will try to net a lot of money from victims within a short period of time (through elaborate MLM schemes) before fleeing away.

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

Increased awareness among individuals about the adverse effects of responding to potential scam bait that reach them through social media and messaging platforms, have entertained discussions to spread warnings about new scam variants that people need to be aware of. Individuals have been forthcoming to share their harrowing experiences, often resulting in financial losses, after being ingrained into the scam ecosystem. In this vein, pig butchering scams and Work from Home scams can be categorized into the following:

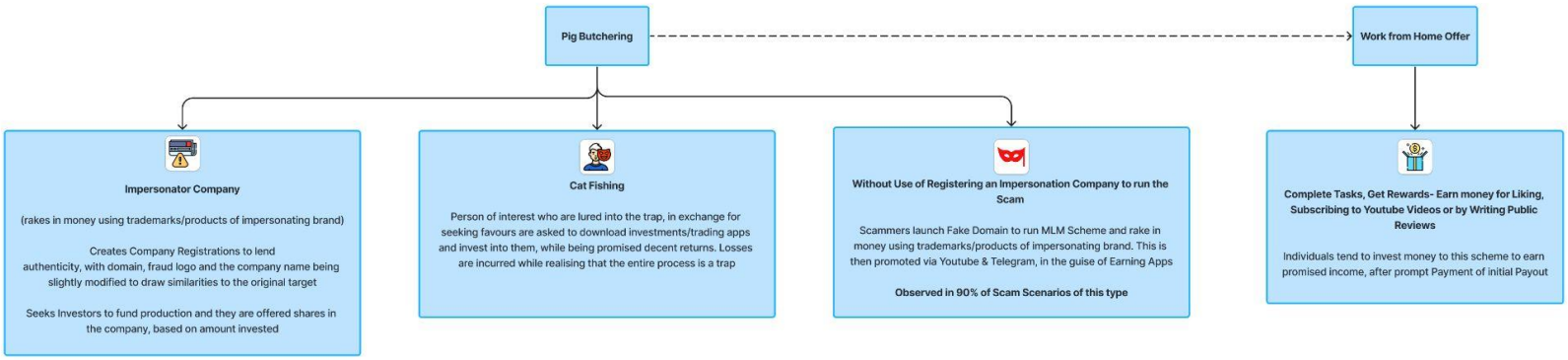


Figure 2 - Scam Tentacles of the same Class

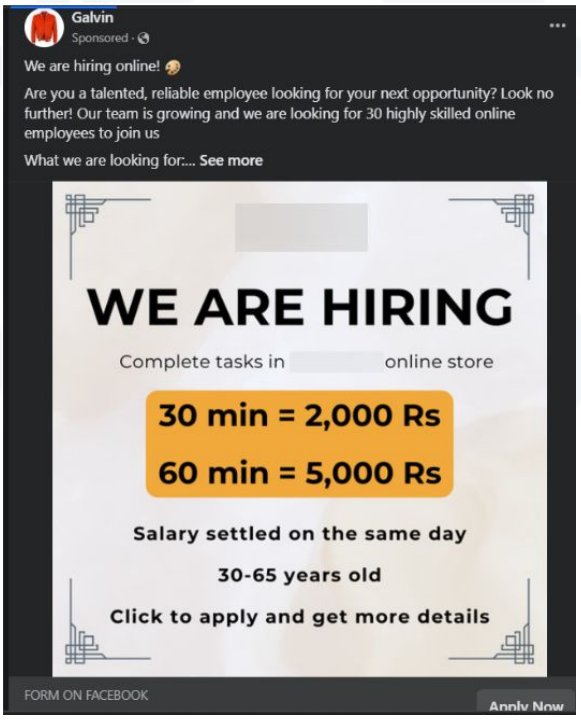


Figure 3 - Recruitment for Work from Home Opportunities on Facebook, promising astounding incentives in return for completing tasks

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

- The operation cycle begins by scammers identifying organizations with good industry presence and customer base to spread word about a potential investment scheme - centring around the target company/brand that they want to impersonate.

- These get picked up by numerous Indian Youtube channels that center their content around investment and financial planning. Since the content creators thrive on making income by creating content daily, similar schemes get picked up and a video is made.

- The propagation of these videos, which provides information about the investment structure, it's benefits and links to their Telegram Channel / Group. The bogus investment site, acting as a front for the scam, is embedded with referral codes, which is a common practice among apps to reward referrals. The content of the videos and graphics depicting an easy deposit-profit cycle entice gullible individuals to take the extreme step and invest.

- Appropriate disclaimers for users to invest at their own risk are shown, as the content creators are aware that such investment schemes are not trustworthy in the least sense, and to be free of any legal consequences caused by public uproar following an exit scam scenario. Yet, an influx of such schemes get promoted on their Telegram Channels as well as their YouTube Channels regularly, regardless of the harm caused by misinformation and foreseeable financial loss caused to the victims. These videos are being promoted on the platform by content creators who curate content around the topics of "Investment and Personal Finance".

- The aggressive nature in which these investment schemes get promoted is worrying, as referenced by the upload frequency on YouTube, which is synonymous with similar channels that use it as content. These channels usually have a subscriber count to the tune of thousands, which translates to the content reaching a very wide net of audience.

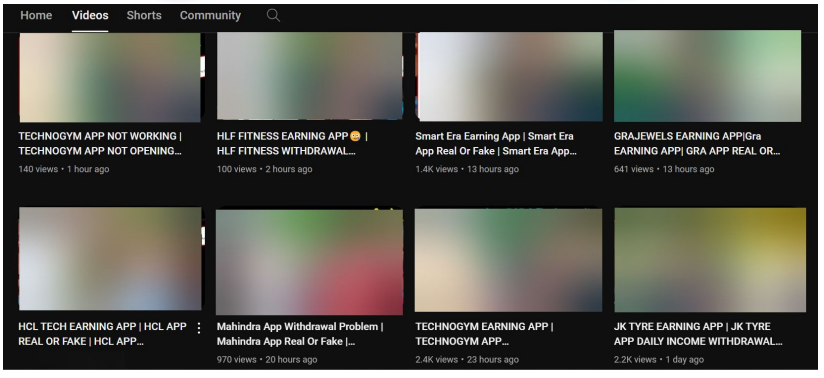


Figure 4- Catalog of videos promoting "earning apps", that are not affiliated to renowned organizations on YouTube

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

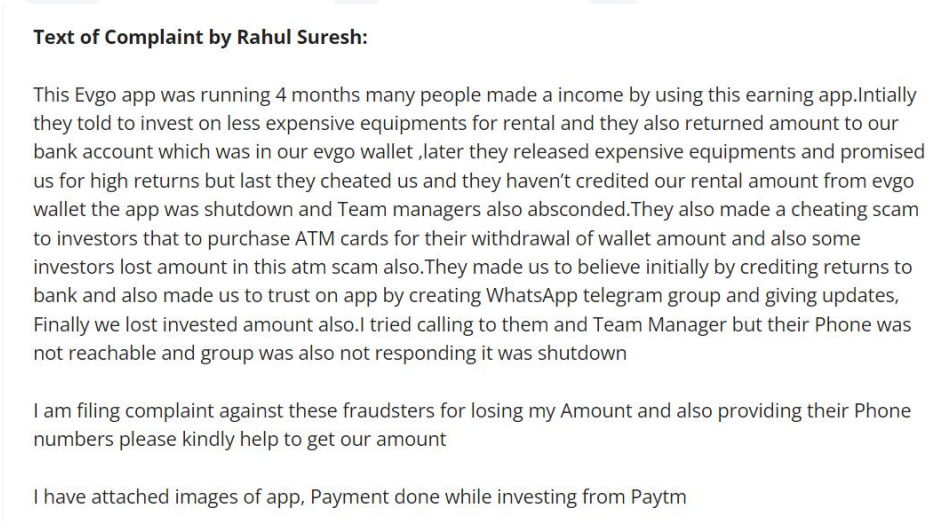
© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

- Victims create an account on the site and proceed to make an initial investment, expecting timely profits. More the invested amount, more are the expected/promised returns - that is obtained by purchasing fictional items offered for sale by the impersonator company, or by clearing VIP Levels that require a certain amount of accumulated deposit. To establish an air of authenticity and transparency, digital certificates or ID Cards are issued to the investors - in hindsight affirming that they are now a part of this scam cycle. [**See Appendix**]

- Each member who signs up for the phony scheme is provided with a referral code/link - which can be used to claim bonuses/commissions based on the number of individuals referred to the scam and who are willing to invest, with the blind faith of getting rich quickly.

- The grapple between investors and impersonator company occurs, when the promised return of invested amount is not being credited in a timely manner, or when assigned referral codes do not work - leading to frustrated patrons pushing videos on Youtube, leaving complaints on Online Consumer Forums or proceed to complain to the impersonated brand itself, in an attempt to forewarn other individuals that the scheme is fraudulent. The amount of misinformation conveyed throughout the entire scam cycle is frightening, which is another threat that needs to be combated against.

- What follows is an exit scam scenario, where the scammers flee with illicit funds invested in the he scam, along with PII submitted to the platform by investors, which can be used in malicious methods in the future. The cycle of impersonating another brand begins again.



Text of Complaint by Rahul Suresh:

This Evgo app was running 4 months many people made a income by using this earning app.Intially they told to invest on less expensive equipments for rental and they also returned amount to our bank account which was in our evgo wallet ,later they released expensive equipments and promised us for high returns but last they cheated us and they haven't credited our rental amount from evgo wallet the app was shutdown and Team managers also absconded.They also made a cheating scam to investors that to purchase ATM cards for their withdrawal of wallet amount and also some investors lost amount in this atm scam also.They made us to believe initially by crediting returns to bank and also made us to trust on app by creating WhatsApp telegram group and giving updates, Finally we lost invested amount also.I tried calling to them and Team Manager but their Phone was not reachable and group was also not responding it was shutdown

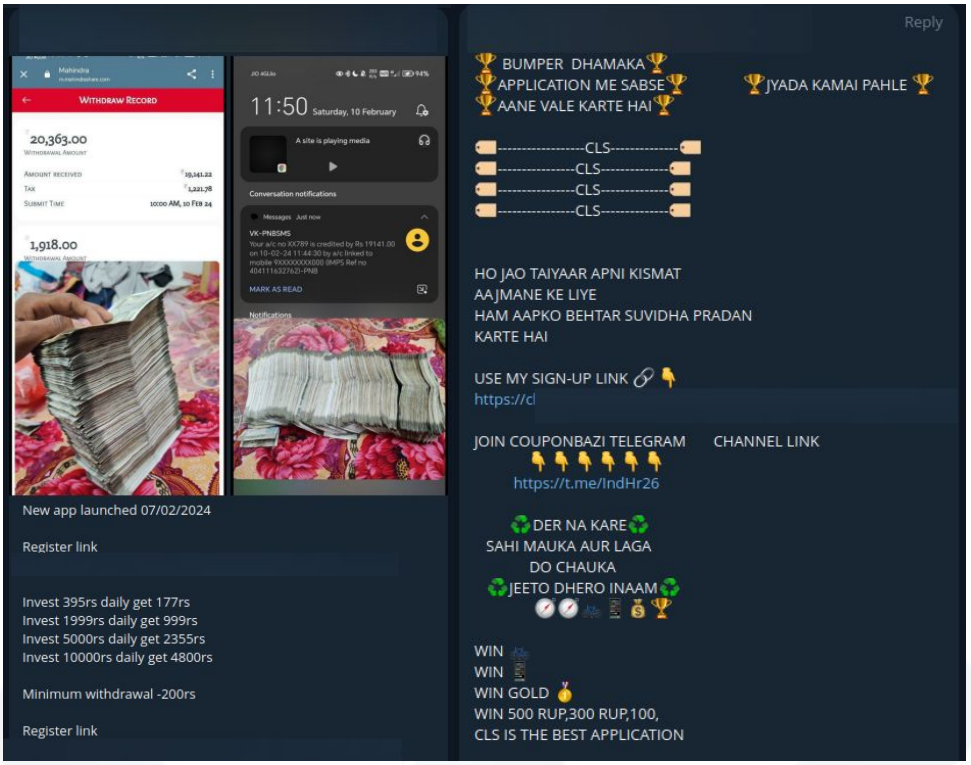
I am filing complaint against these fraudsters for losing my Amount and also providing their Phone numbers please kindly help to get our amount

I have attached images of app, Payment done while investing from Paytm

Figure 5 - Example of a complaint raised on an online Consumer Complaint Forum, by a disgruntled individual, after losing their hard earned money, to a similar scam scenario

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved



Figures 6 & 7 - Telegram Messages following a standard template of promoting similar investment schemes. Information such as Referral Link, Deposit vs Return Figures and successful withdrawal screenshots are included

Investment in Bogus Offerings from the Impersonating Company

In the guise of investment, investors are asked to invest in offerings provided by the company endorsing the investment scheme. In many of the scams that we have tracked, the offerings will vary according to the industry to which the company belongs to.

Case 1 - Impersonation of Global Agricultural Company [Annual Revenue > $ 1 Billion]

The impersonator company spread word about an investment scheme in the agricultural company directly targeted by the impersonation scam, who primarily produces goods such as spices, vegetables and fruits in which investments could be made. Telegram was used as a medium to promote the scheme. Associated with each product are it's income, revenue and period of profit - according to which investors can purchase products and assume that they have "invested" in the product. The investment company promises to use the invested money to produce the products. Over time, the offerings changed to investment in **cakes and musical instruments**.

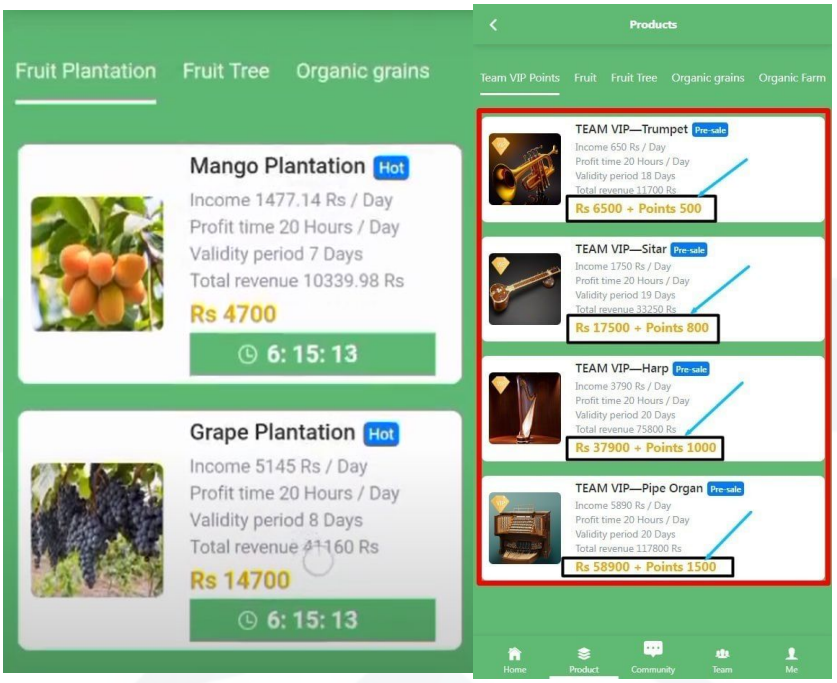
This will potentially set off red flags, as promised profits for these are too good to be true in most instances. When conducting an investigation on the same scam campaign, researchers were able to understand that the new wave of products were not part of the impersonating company's portfolio. It is understood that the general shift in offerings led to the scammers realizing that more money could be swindled in this manner, by observing the ever increasing count of investors.

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

Over time, the offerings changed and were made available to exclusive members - which may drive fear in the investor circle to invest more. Exclusive offerings are promised to provide more profits.

The investment cycle winds up after a period of 3-6 months (which may differ across similar schemes), where the investors (now victims at this point) become embroiled in significant losses.



Figures 8 & 9 - Eventual change of offerings from the fake investment company (agricultural produce to musical instruments)

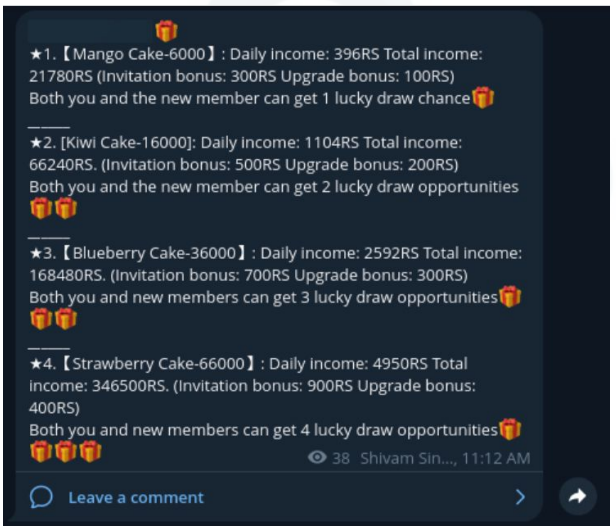


Figure 10 - A Telegram Group promoting these scams, offers investment opportunities in cakes produced by an impersonator company, with lucrative profits being promised, in exchange for investment

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

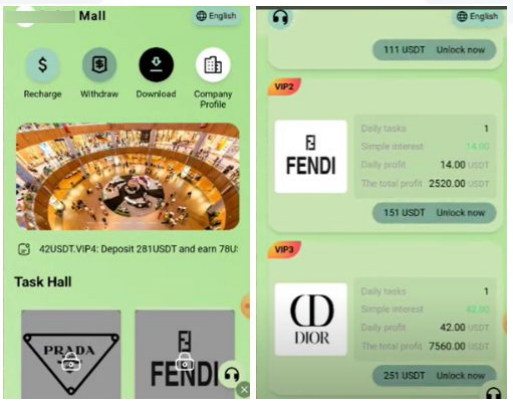
Additional Pointers indicating to a scam in the making:-

- The address of the Indian Office of the Impersonator Company was found to be rented out by a car rental company with a solid presence in the rental industry. This claim was verified with the help of Business Profile Information from Google.
- Shoddy and Unprofessional Videos shot by “employees” of the Impersonator Company to spread word about the Company’s objectives, vision and the need to raise investments. These were posted to a website acting as a front for the scam and on YouTube.
- Offline Meetings and Group Photos - As discussed previously, the scheme over time develops into an MLM model, where for every upline (person who refers), there will be a set of 10-20 individuals as downlines (people who get referred to the scheme) and they get classified into a team. When the profit is withdrawn, these members assemble and go for outings and take group photos displaying the logo of the impersonating company on their phones. These photos are then sent to the common Telegram Group to spread a false sense of security and assurance that the scheme is indeed legit and that more people can indeed invest without fearing losses.

Case 2 - Impersonation of Real Estate Development Company [Annual Revenue > $ 1 Billion]

- In a scam scenario that was tracked by CloudSEK’s Threat Intelligence Team concerning a major real estate development entity that develops malls among other commercial properties in the Middle East, scammers were inviting individuals to invest in brands that had leased space within the mall.

- These major brands included Burberry, Louis Vuitton and Dior, who operate in the luxury retail sector. This was done as a tactic to further induce authenticity of the scheme, to unsuspecting victims and in the process, and possibly dragging the reliability of these globally renowned brands into question.



Figures 11 & 12 - Names and logos of major retail brands, that had rented space within the mall, were misused in this campaign of the pig butchering scam, that CloudSEK had tracked

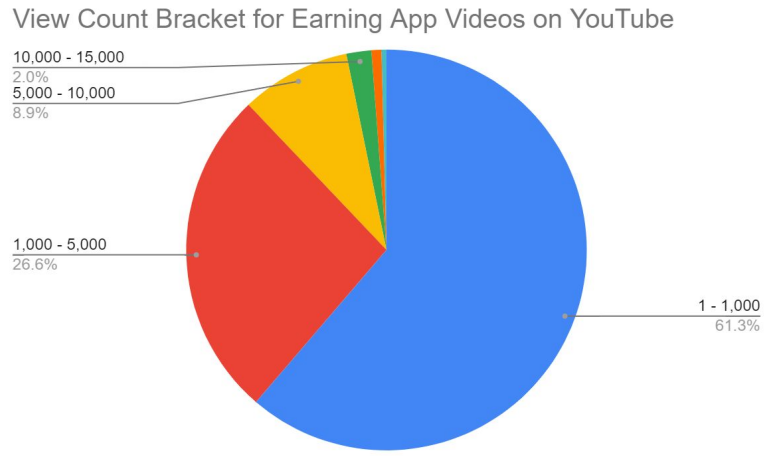
Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

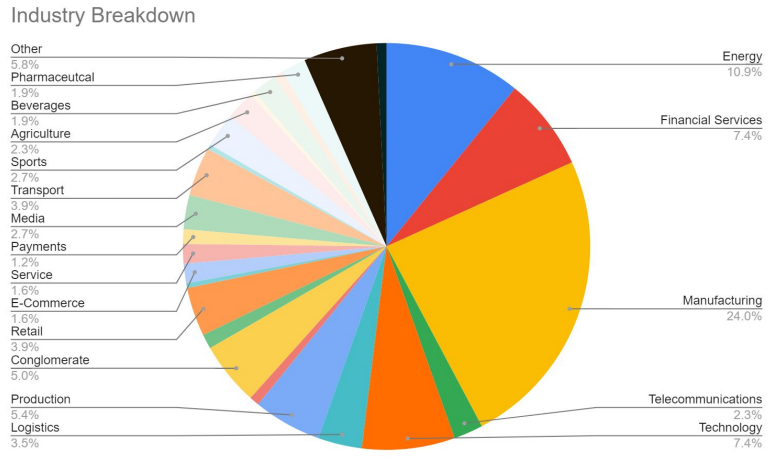
Other brand ventures of the same Development Company were similarly targeted, including one of the leading independent cinema theater chains in the region. Similarly, through our investigation, at least 2 other mall outlets in the region were being targeted in the guise of seeking investments. These were discovered from YouTube, with videos titled as “earning apps” with the targeted brand’s name being name-dropped to obtain views and lend authenticity.

Observations from Youtube: Rapid Spread of Content focused on Fraudulent Investment Ventures

For a sample data set of nearly 260 videos found to be discussing similar earning methods on YouTube since 2023, the average view count is nearly 2,263. The view count and industry breakdown (industries affected by similar impersonation scam campaigns) are provided below:-



Infographic 1 - Video Viewership classified into view brackets



Infographic 2 - Classification of Industries being affected by the active threat

To NOTE: It should be reiterated that multiple videos targeting one brand can be found, as many YouTube Channels have the tendency to cover the same class of fraudulent schemes that affects many global brands that are currently at the risk of being impersonated by scammers, and go on promoting them, one after the other in unwavering frequency.

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

Malicious Infrastructure Utilized in Scam Operations

During our research on valid use cases of similar scams affecting organizations, an observation made was the abuse of TLDs such as .cc, .top and .vip for registering fake domains to populate the scam. Another indicator of using .vip TLD is that it correlates with the concept that the similar class of schemes are grouped in terms of levels - named “VIP Levels”. Higher the invested amount, higher the VIP level you are classified under.

Infrastructure Overview

Domains/Web Infrastructure are repeatedly preferred and abused by scammers owing to privacy being maintained by the domain registrar in withholding the domain registrant’s name, details and cryptocurrency being accepted as a form of payment - to prevent payments from being traced back to an individual(s) operating as a group of scammers with similar motives.

Domain Names provided to these sneaky websites have ensured over time that it does not contain the company name that will be detected / matched with the company that it is trying to impersonate,throwing a spanner in the works of affected companies who are actively attempting to track such scams and reduce complaints of discontent from the scammed audience.

These scammers ensure that these websites are assigned domain names consisting of alphanumeric text / other benign keywords, which can be difficult to detect, unless the websites share similar DNS Record Patterns, share common phishing kits or domain registrant information, utilized by threat actors to set up similar websites. After the advent of an exit scam, these websites get taken down.

This raises the need for Fake Domain Classifiers to use OCR / Logo Matching Capabilities to detect and takedown such websites in time. The screenshot below shows a recent example of a website aiding in a targeted pig butchering scam against a leading IT Consulting MNC,based in India

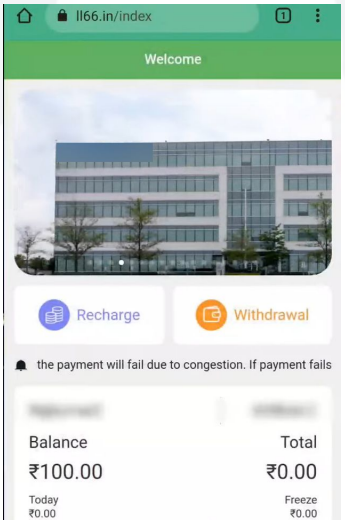


Figure 13 - Mobile screenshot of the scam website, pushing an investment scheme, associated with an MNC Brand

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

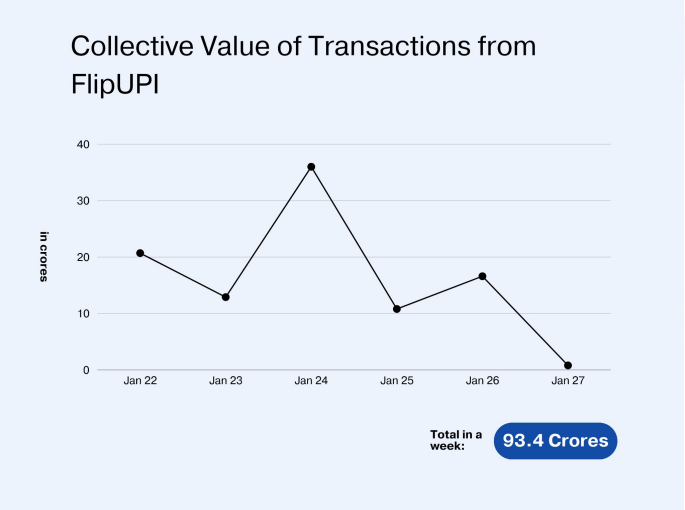
Transaction Analysis - Breaking into a Fraudulent UPI Payment Gateway

From our analysis of similar scam campaigns that's prevalent in the Indian region, the dependance on UPI, the real-time payment system is notable. QR Codes generated by scammers from digital wallet solutions are used as a single-stop method to conduct transactions in a bidirectional manner (investment into the scheme - withdrawal of profit). Since bank accounts are tied to UPI IDs, and by observing the,scale of scams running on the same modus operandi in India it can be a distinct possibility that falsified
documents are being used to create bank accounts at bulk to park these funds. **This potentially introduces the concept of money mules into the investment fraud ecosystem.**

The impending threat of fraudulent UPI Payment Gateways being utilized to route payments, in this class of scams cannot be understated and it should be considered, during similar brand threat investigations. Examples of such Payment Gateways include - FlipUPI, Upi-Cashier, UPIPaid, WowPayGLB etc

To observe the scale and involvement of payment gateway applications in this scam scenario, we tried to analyze the transaction history being routed through FlipUPI, one such UPI Gateway that was discovered to be used for fraud payments.Our analysis is as follows:-

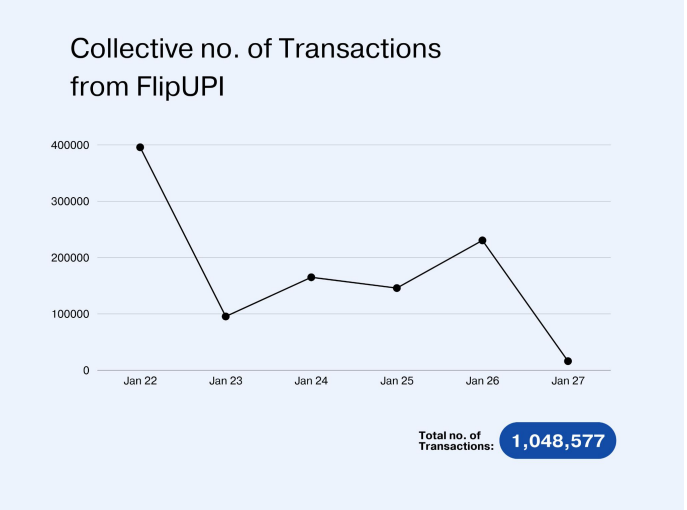
- The payments were being received by 36 unique VPA Addresses.
- A total of more than 15.5 lakh transactions transaction requests were made on flipupi.com on the UPI addresses, within a duration of 8 days



Infographic 3 - Magnitude of Transactional Amounts being routed through the Fraudulent UPI Payment Gateway 'FlipUPI'

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved



Infographic 4 - Magnitude of Transactions being routed through the Fraudulent UPI Payment Gateway 'FlipUPI'

The total amount of transaction requests made through the payment gateway crosses INR 100cr. Now, it is evident that not all the users who were redirected to the payment gateway made the complete transaction. Hence the website has three codes 0,1,2

- These are possibly the 3 categories in which the transaction are divided:

Status	Possible Definition	Amount
0	Successful Transaction	**INR 3.47 cr**
1	Transactions which are stuck or did not go through	**INR 14.59 cr**
2	Unsuccessful transactions	**INR 85.89 cr**

Please note that - The above classification is a hypothesis based on the transaction division which was found in the dumped transaction, we are taking the conservative approach by classifying successful transactions as the status which has least sum.

Investors are asked to submit information such as Bank Account Number, IFSC Code and Bank Name, in an attempt to streamline the convenience of payments. This in turn is harvested as PII by the scammers, which can be used for malicious purposes, after exit scamming.

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

Usage of Telegram to Relay Updates during the Scam Lifecycle

Telegram and Whatsapp groups have been commonly used by the scam operators to relay updates about the investment scheme. Users are added to the group, after making an initial deposit or after expressing an interest in the same. For some users, the initial withdrawal transaction is successful from the investment project, further heightening their trust in the investment project - leading them to invest more. Screenshots of withdrawal transactions from investors are asked to be shared, in a method to lend authenticity of the project and testimonies are shared on the groups

This investment project, with increasing rate of activity, progresses into an MLM Scheme where existing investors are asked to refer people and in the process are promised good referral bonuses. This not only extends the web of victims that the scammers can cheat, but goodwill is given a tradeoff here, as existing investors are convinced that the project is genuine, with initial withdrawals and bonuses given on time and would like to extend the benefits of the scheme to relatives and friends, with recommendations.

Eventually, the attempts to withdraw the profits become unsuccessful, eventual ghosting and lack of communication from the scam operators provide indiators to the now-victims that this was a fraudulent investment operation all along. This results in impersonated brands being unable to resolve complaints of victims on social media and consumer forum boards - with losses indirectly incurred due to their brand.

Figure 14 - Higher the VIP Level that a user is classified in after investment, higher is the risk of being embroiled in financial losses

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

Fraudulent websites

It has been brough to our attention that apm-india.com (and similar investment or earning apps) is a fraudulent pyramid investment scheme that is not affiliated with APM Terminals in any way. Our team has reported this site and it has been taken off line.

- If you have been a victim of fraud, we advise you to report it to your local police authorities.

The safety of our customers' data is paramount for us at APM Terminals. We attend to the highest standards in handling your data to ensure a safe and secure operation. APM Terminals will never ask you to pay money through any social media or 3rd party communication platform. Please only trust content from our official site, APMTerminals.com. If you are unsure about the legitimacy of a site, please **contact your local APM Terminals facility**.

Figure 15 - Public Advisory issued by a Shipping Company, in response to investment schemes falsely endorsed using their brand name, logo and products

Figure 16 - Earning Apps thrive on referral, which promises good incentives. This in turn increases the number of victims that get scammed

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

Figures 17 & 18 - Announcement regarding the abrupt ending of an investment scam operation on Telegram

Observations from Telegram Groups used to propagate these investment schemes

- Supply shortage - Investing members tend to buy (invest) in high value products offered by the company, which they believe will earn them significant profits. As the demand for these products surge, their availability will reduce, leading to scam operators to force investors to invest in other products.

- Eventual change in offerings - From items initially offered for investment, it will vary over time. For example investment in musical instruments and cakes by a fake company that initially started off with agricultural produce that it was inviting investments for.

- Positions within the company - Investors are offered fictional positions within the company, to establish an air of trustworthiness and transparency between the fraudulent company and investors.

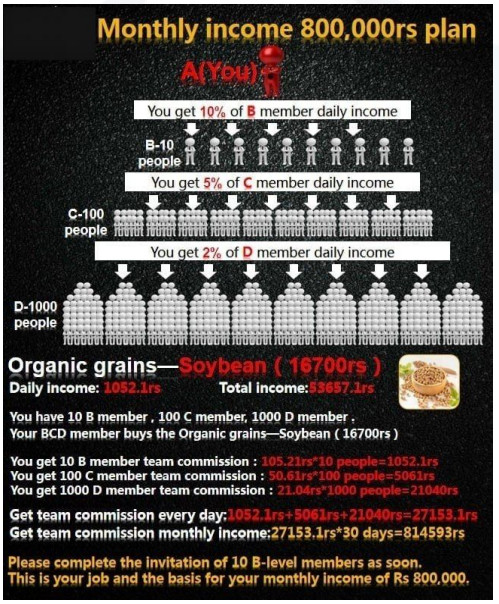


Figure 19 - Poster depicting the entire structure of the investment scheme as an MLM

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

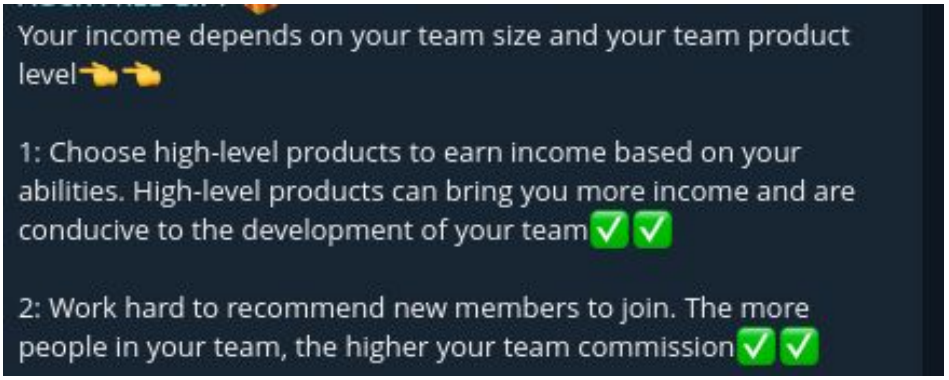
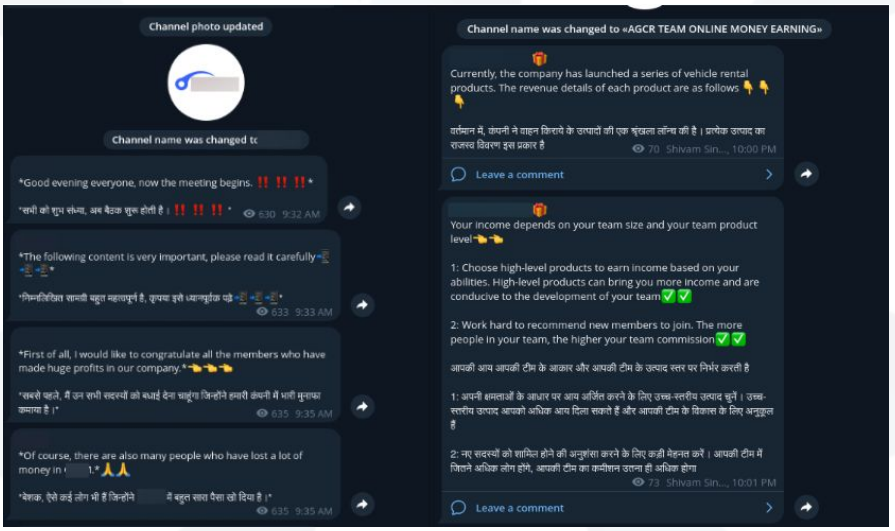
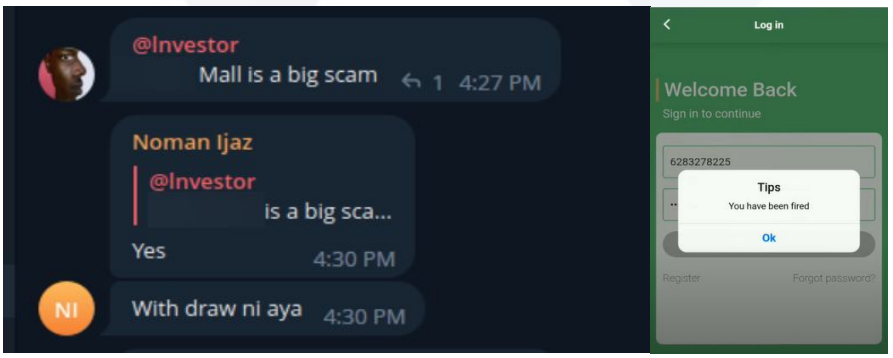


Figure 18 - Guidelines provided to investors - in order to net more profits

Eventually as the scammers begin to ghost the investors, the existing content of the investment scheme on the Telegram group - including messages, posters etc are removed. The scammers then begin to add new people to the group and start sending messages regarding a new investment scheme - **that is very likely to be impersonating another global brand** and the cycle recurs again. Due to scammers reusing the same Telegram Group to spread multiple investment offers, the count of subscribers stays inflated to the tune of several thousands



Figures 20 & 21 - Initiation of a new scam campaign on the same Telegram Group, where records of a previously-run investment scheme were scrubbed



Figures 22 & 23 - Messages observed in the Telegram Groups indicating that promised payments are not being credited on time to the investor's wallet and eventually it dawns on the investor that that the entire investment operation is a scam

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

Recurring Similarities with Color Prediction Scams observed in India

Color Prediction Games promise quick money by allowing users to place bets and win good returns for predicting the right color. In a blog covered by CloudSEK's Threat Research Team in July 2022, numerous fake domains were uncovered, wherein the logos and brand names of known retail brands were used to propagate such games on Telegram and Youtube.

The motive of the scam operators was to get more attention from the average social media user and exploit their trust on renowned brands, ultimately participating in these games. The catch with these games is that participants lose out on winnings after a certain time or are unable to access topped up money on wallets provided by these games.

It is no surprise that these websites and scams get promoted to this day on YouTube, in the guise of "Mall Earning Apps" and "Color Prediction Games", and minting money in the process

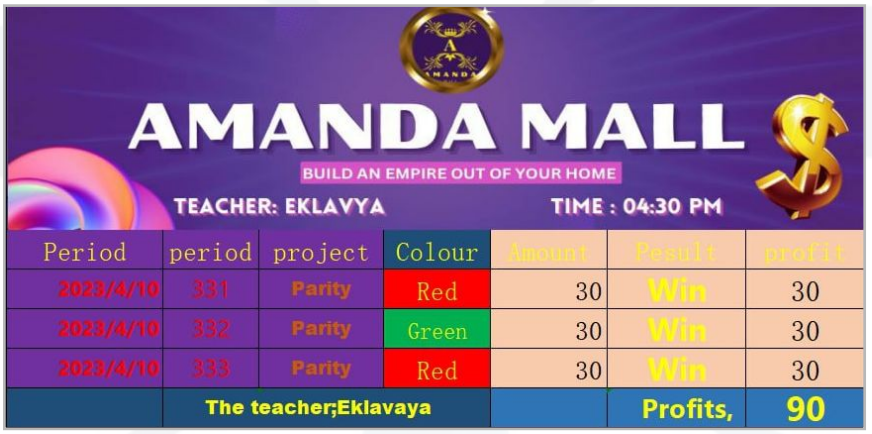
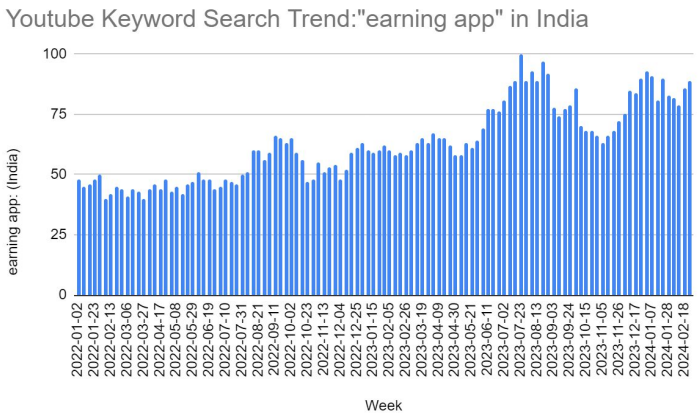


Figure 24 - Color Chart and investment vs Profit Rates for a Color Prediction Game

Infographics depicting the extent of the reach of Earning Apps in India



Infographic 5 - Magnitude of the usage of the search term "earning app" on YouTube since 2022

From the above trend we can see a drastic spike in the number of search queries related to the term "earning app" on Youtube from mid 2022, which is estimated to be the time period when videos were started to be used to promote investment schemes.

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

It is important that we understand the impact that similar phony investment scheme campaigns can have on the region economically or otherwise:-

- This scam provides a gateway for Threat Actors to lure people, who are genuinely interested in improving personal finances and then scam them, by luring them with names of major brands into disrepute.
- This reduces the brand reputation of globally established organizations from multiple industries, leading to decrement in trust from the general public.
- There could be direct financial losses stemming from fraudulent transactions carried out through the compromised accounts.

We at CloudSEK have been actively reporting incidents of similar impersonation scams to our clients, since 2022 and have been helping them responsibly, with takedowns to prevent scammers from luring a larger count of audience into their trap.

There are some proactive methods that can be used to monitor and mitigate these threats:

- Monitor newly created domains
- Invest in better SEO techniques so that the scam domains do not pop up above the original domains
- Proactively takedown videos that contain content infringing brand or associated trademarks from YouTube, due to the amount of misinformation being spread, about investment schemes that are not endorsed by your brand.

Conclusion

This whitepaper aims to spread awareness to underline the fact that any company having a significant internet and brand presence should be wary of similar impersonation scams. At a day and age, when the concept of trademark infringement has received recognition and and budgets are allocated by organizations to combat fraud with the help of specialized teams, appropriate measures to nullify the threat at it's infancy can be embraced, through social media content monitoring and takedown services, which CloudSEK offers.

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

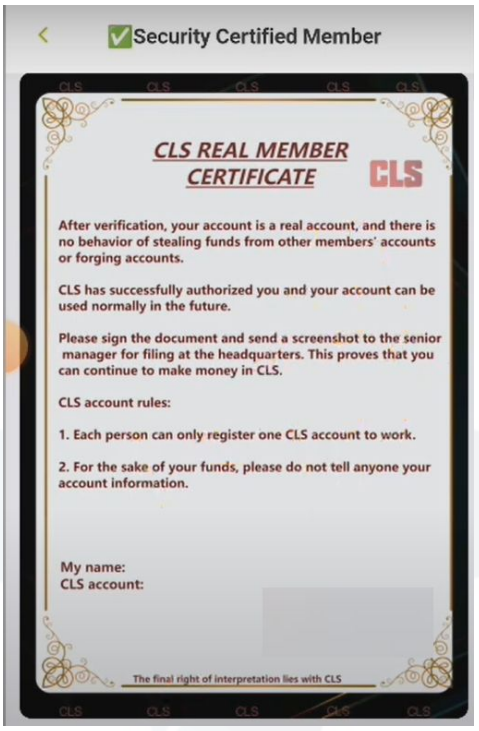


Figure 25 - Digital Certificate issued to CLS Earning App member, upon signing up to the scheme

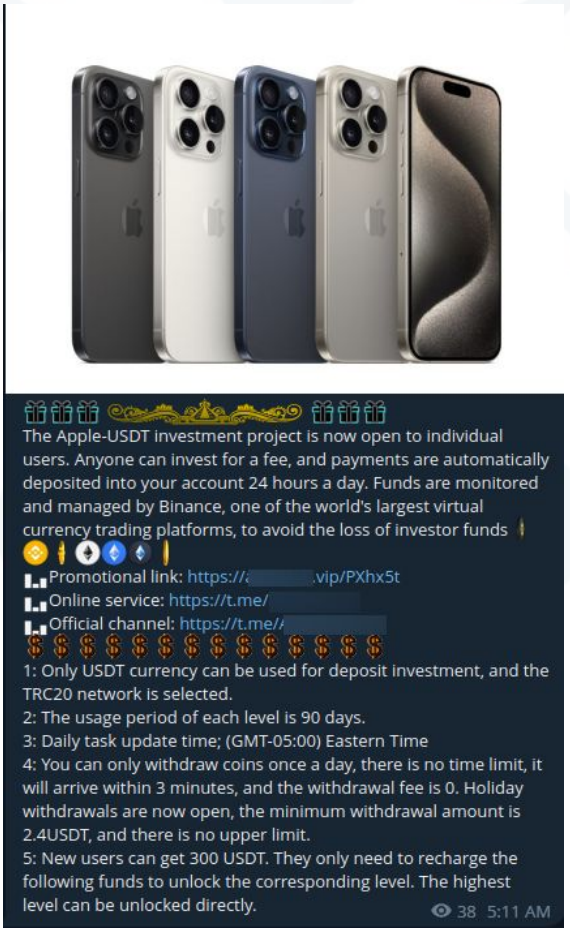


Figure 26 - Investment Scam targeting Apple's 'IPhone' Product Offering

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

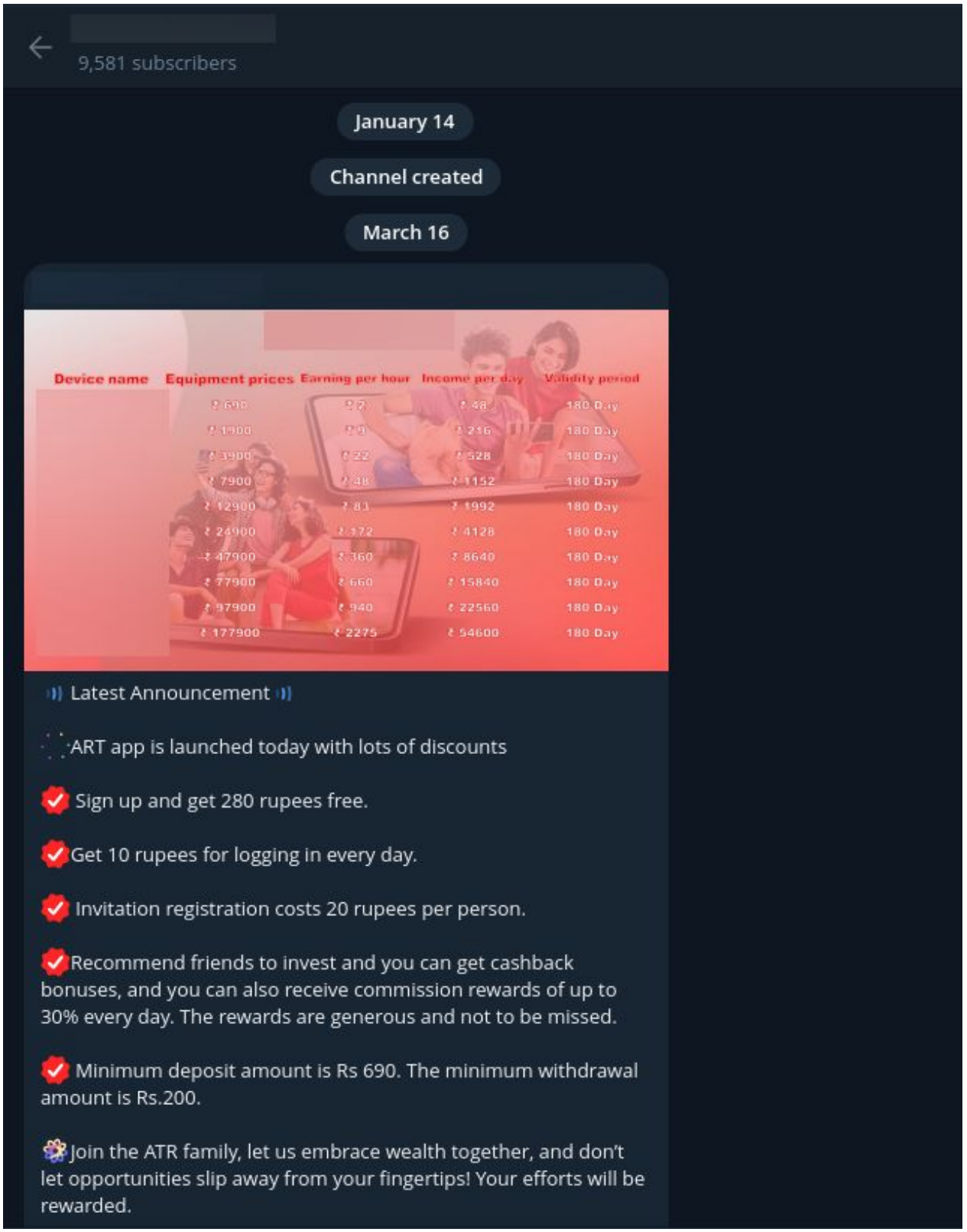


Figure 27 - A Telegram Group found to be promoting a fraudulent investment scheme that targeted one of India's top Telecom Companies. Notice the contrast between the inflated number of subscribers and the channel start date

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.

© 2024 CloudSEK Information Security Pvt. Ltd. All rights reserved

CloudSEK

We Predict Cyber Threats

Monitor. Analyse. Predict.

Secure your Tomorrow,Today!

Request for a Free Demo of our platform:

SCAN ME

OR

Mail us at **info@cloudsek.com**
or visit **https://cloudsek.com**

Gain access to a free trial and Detailed POC on CloudSEK Platform

Registered Office:

CloudSEK Research Pte Ltd.
51 Chin Swee Rd. #07-12 Manhattan House,
Singapore 169876

Regional Office: United States

CloudSEK Inc.
8 The Green, Ste A, Dover, DE - 19901
United States

Regional Office: India

CloudSEK Information Security Pvt Ltd
16/1, WINGS, Cambridge Rd, Halasuru,
Cambridge Layout, Jogupalya,
Bengaluru, Karnataka, India - 560008

Regional Office: United Kingdom

CloudSEK, 4th floor, Rex House,
4, 12 Regent Street, London,
SW1Y 4PE - United Kingdom