Cyberint
A Check Point Company

The Rise of **Pig Butchering Scams**

December 2024

TABLE OF CONTENTS

THE RISE OF PIG BUTCHERING SCAMS

BACKGROUND

In recent years, "Pig Butchering" (also referred to as "杀猪盘 shāzhūpán") scams have rapidly emerged as a significant global threat, primarily targeting individuals with fraudulent investment schemes. This type of scam, originally known for its roots in China, has transformed into a global phenomenon, where victims are led to believe they are making lucrative investments, often in cryptocurrency. The name "pig butchering" comes from scammers "fattening up" their victims by gaining their trust before seizing their funds, leaving the victims with significant losses.

The scam involves criminals engaging with targets through social media, direct messaging apps, and dating apps, sometimes for months, to build a sense of trust and familiarity.

Eventually, the victims are convinced to invest in what appears to be a legitimate venture, only to realize later that their money has been stolen. This scam is now global, with operations frequently run by groups in Southeast Asia.

According to the FBI[1], cryptocurrency-related scams, including pig butchering scams, accounted for a staggering $5.6 billion in reported losses in 2023, a sharp increase from previous years.

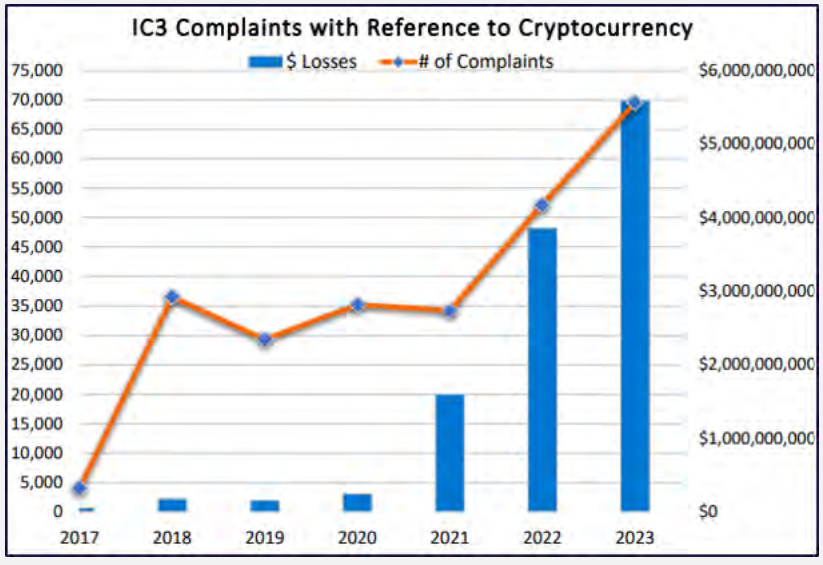


Figure 1: FBI report highlights a significant rise in both the number of complaints and financial losses related to cryptocurrency investment fraud, reflecting a growing trend over the past few years.

On a global scale, losses attributed to **pig butchering and similar schemes were conservatively estimated at around $64 billion annually.**[2]

---

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3CryptocurrencyReport.pdf

[2] https://archive.md/20240923175547/https://www.americanbanker.com/news/house-lawmakers-pitch-proposals-to-address-pig-butchering-scams

INTRODUCTION

To demonstrate the dangers of and investment scams, we have focused on analyzing and exploring domains that are known to be associated with these scams based on their website structure. These fraudulent websites often follow a similar template, aimed at deceiving potential victims into thinking they are engaging with a legitimate investment platform.

While most pig butchering scams are associated with Chinese-speaking threat actor groups, our investigation suggests that this specific scam appears to be linked mainly to threat actors originating in Africa, indicating the global expansion and diversification of such operations.

Scam websites typically feature a professional-looking home page promising high returns, a fabricated "About Us" section to establish credibility, and an "Investments" page promoting quick profits, often through cryptocurrency. Additional pages, such as Statistics, Registration, Login, and Cryptocurrency Prices, further enhance the illusion of legitimacy.
A key feature across these sites is a chatbot, used to direct victims to messaging platforms like WhatsApp or Telegram for more personal interaction with scammers.

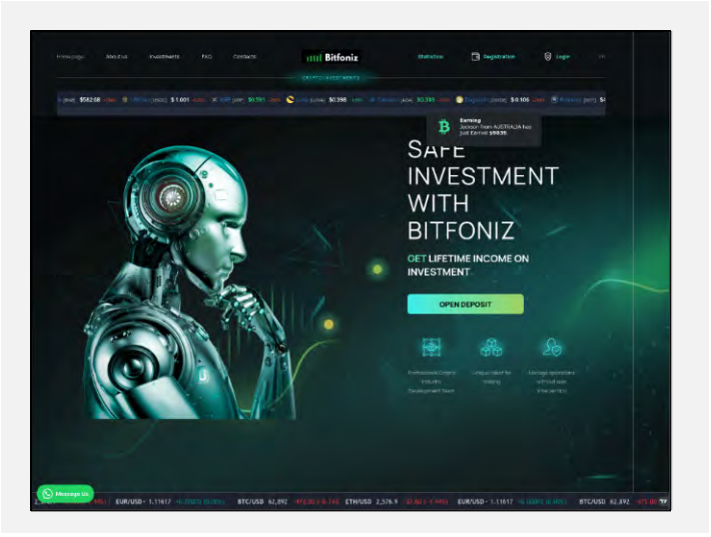


Figure 2: Screenshot of a typical website layout used in pig butchering scams.

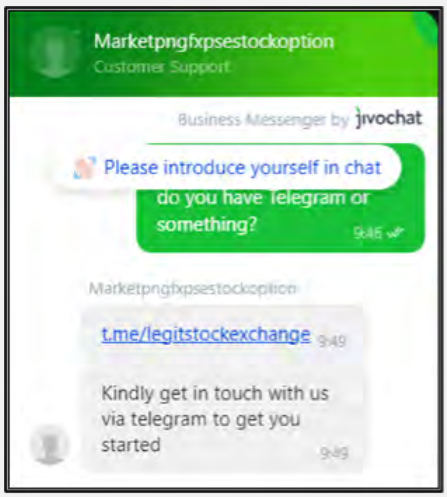


Figure 3: Interaction with the scammers via the website's chatbot reveals they redirect victims to Telegram.

The combination of easily replicated website templates, the use of social engineering through chatbots, and the promise of high investment returns makes this scam highly effective in targeting all kinds of victims worldwide.

EXECUTIVE SUMMARY

BACKGROUND

- This report investigates the rise of "Pig Butchering" scams, also known as "杀猪盘 shāzhūpán," a global fraud phenomenon targeting individuals through fake investment schemes, primarily in cryptocurrency.
- Originating in China, these scams have expanded globally, with scammers using social media, dating apps, and direct messaging platforms to build trust over time before defrauding victims.
- These scams often employ professional-looking websites, using fabricated success stories, high-return promises, and fake documents to create an illusion of legitimacy and lure unsuspecting victims.
- The rise of AI has simplified the creation of convincing fraudulent platforms, enabling more threat actors to join and scale these operations.

FINDINGS

- **Our investigation uncovered over 1,000 domains** with similar fraudulent templates, pointing to a large-scale scam linked to threat actor groups in Africa.
  - Although the threat actors used relatively simple methods to deceive victims, these scams have still resulted in significant financial losses, with estimated annual losses reaching tens or even hundreds of thousands of dollars.

- Our investigation exposed poor security practices across six fraudulent websites, allowing access to sensitive internal files, including ".env" configuration files, database credentials, and logs, linked to the Laravel framework.

- We identified accessible directories containing uploaded images, personal identification documents, and transaction confirmations, which could be exploited for blackmail or sold as personal data.
  - **The impact spans 27 countries across multiple continents, affecting victims from diverse backgrounds with no specific demographic profile.**

- Scammers promote their schemes on social media, especially Facebook, by impersonating "successful" and "attractive" individuals to lure victims into fake investment opportunities.
  - They use fabricated success stories and motivational posts to create an illusion of financial gain, often including step-by-step instructions to deposit funds.

- Our controlled engagement exposed scammers' tactics, including impersonating industry figures, using inconsistent cover stories, and displaying limited knowledge of claimed origins.

RECOMMENDATIONS

- Be skeptical of high-return investment offers, verify platform legitimacy, and avoid sharing sensitive personal information.

- Stay cautious of social media profiles impersonating successful individuals and report suspicious platforms or profiles to authorities.

FINDINGS

Origins and Components of Websites

We have identified that the first indications of threat actors using these website templates appeared in March 2022. In total, Cyberint identified over 1,000 domains that used this website template. The earliest YouTube instructional[3] video we discovered was uploaded in September 2022 on a channel named "blex ony." The video, narrated by a Nigerian individual, provides step-by-step instructions on setting up such a website. The video's description includes a phone number, +2348088522446, for those interested in purchasing this template. It appears the channel features additional scam website templates for sale, which might indicate the involvement of a larger threat actor group.

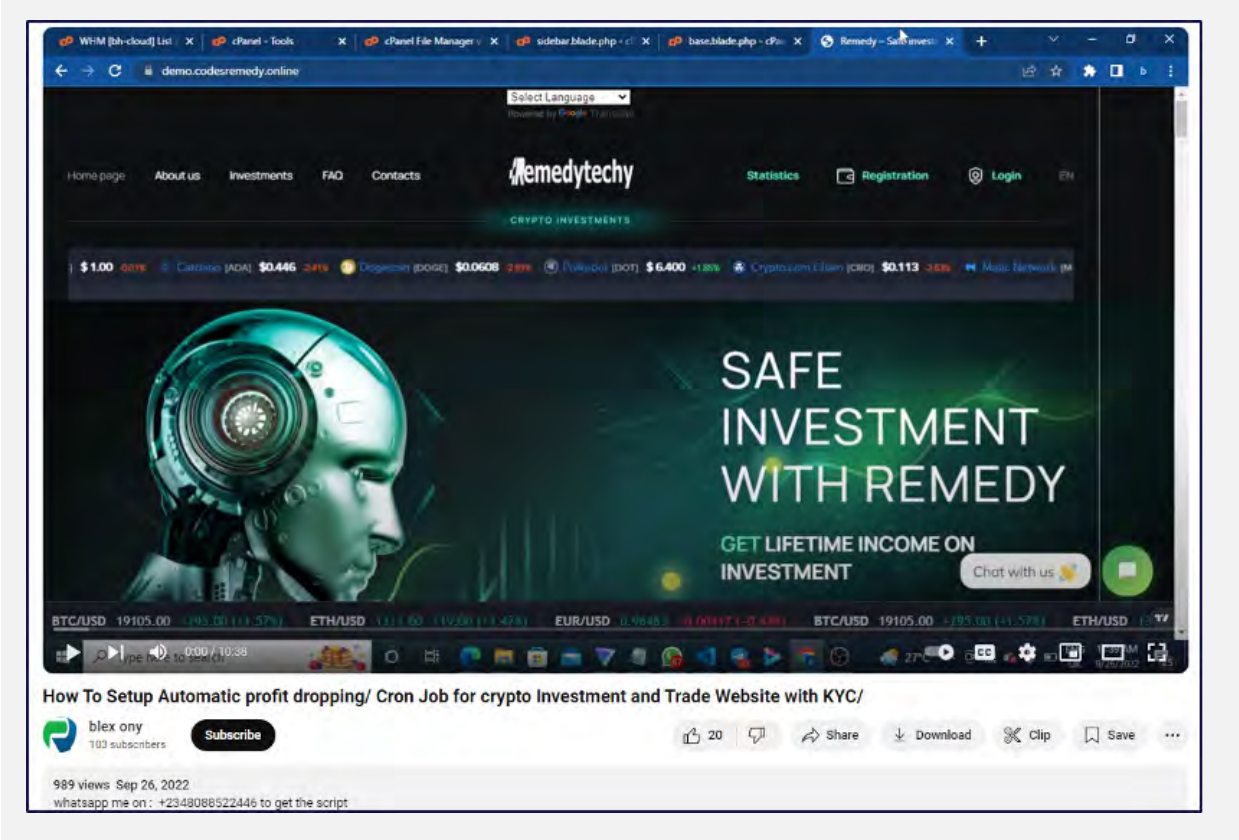


Figure 4: The first YouTube instructional video identified, showcasing these website templates, September 2022

Furthermore, we identified another YouTube video offering the script for free, published by a channel named "Codexoo."[4] Upon accessing the link in the description, we were able to download the template script.

[3] https://www.youtube.com/watch?v=QmP-XXGBxXg

[4] https://www.youtube.com/watch?v=4UFRb6GPPV4

We identified that the scammers are using the Laravel framework based on the presence of certain files. The script folder includes files such as "composer.json" and other default files that are typically generated automatically when creating web applications with Laravel.[5]

Figure 5: Screenshot of the script folder displaying Laravel's default directories.

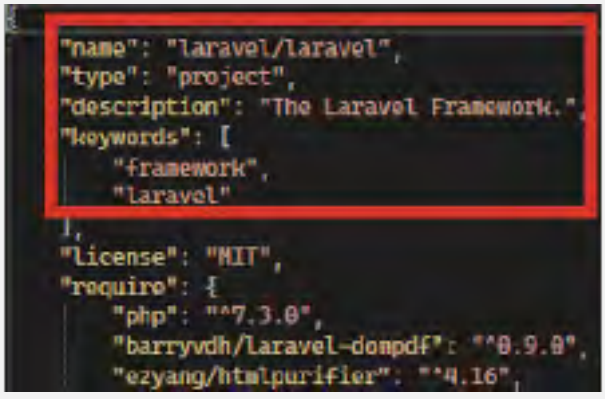


Figure 6: Screenshot of the "composer.json" file, indicating that the web application is built using Laravel.

[5] https://www.geeksforgeeks.org/laravel-directory-structure/

Scam Impact

Our investigation actively leveraged poor security practices on six of the fraudulent platforms, enabling us to access internal directories and various sensitive files which were stored on these sites' backends, including .env configuration files, logs files, and more. These types of files and directories are known to be associated with Laravel framework.

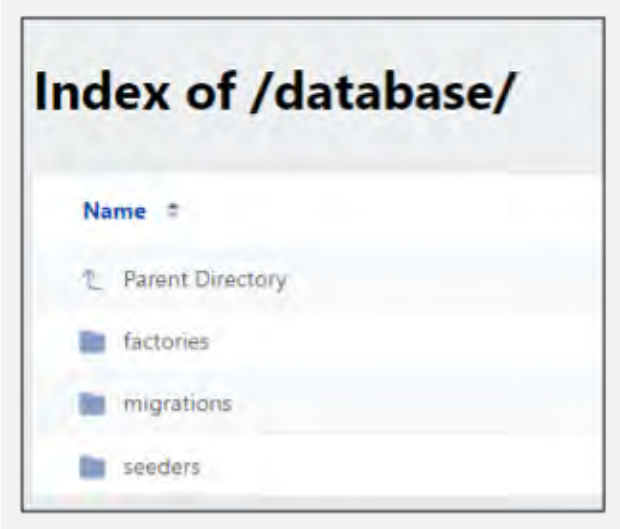


Figure 7: An example of a publicly accessible internal directory named "database."

Figure 8: An Example of a sensitive internal .env configuration file uncovered, revealing database credentials, application keys, and server settings on the fraudulent platform.

Additionally, we located directories where uploaded images are stored.

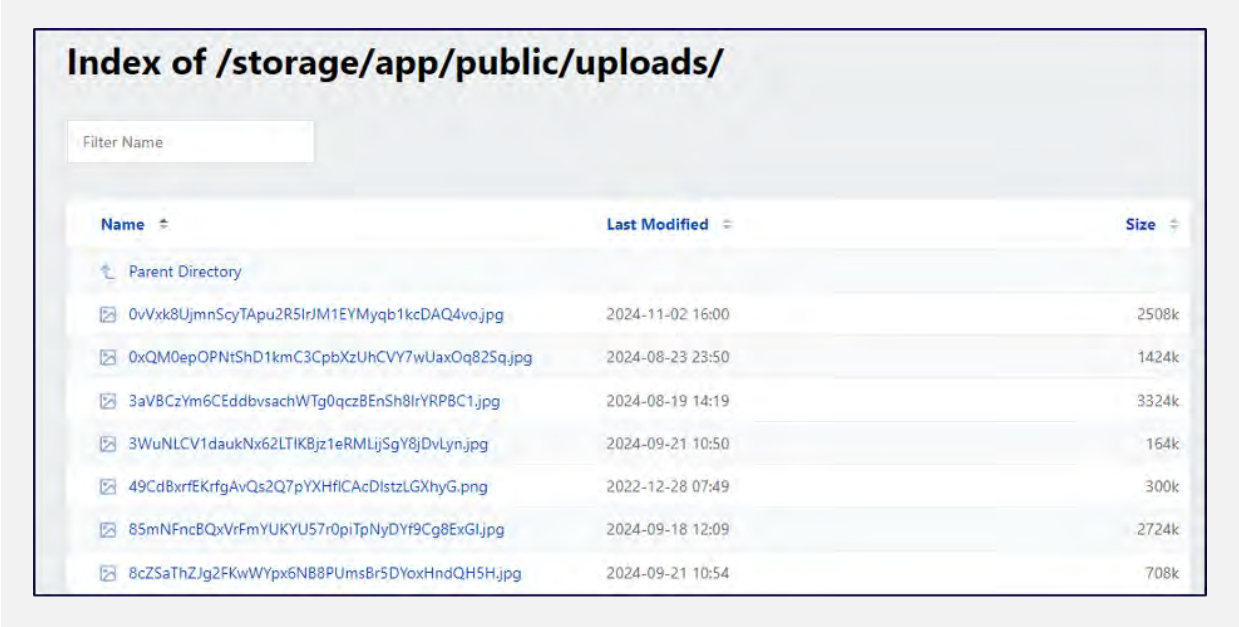
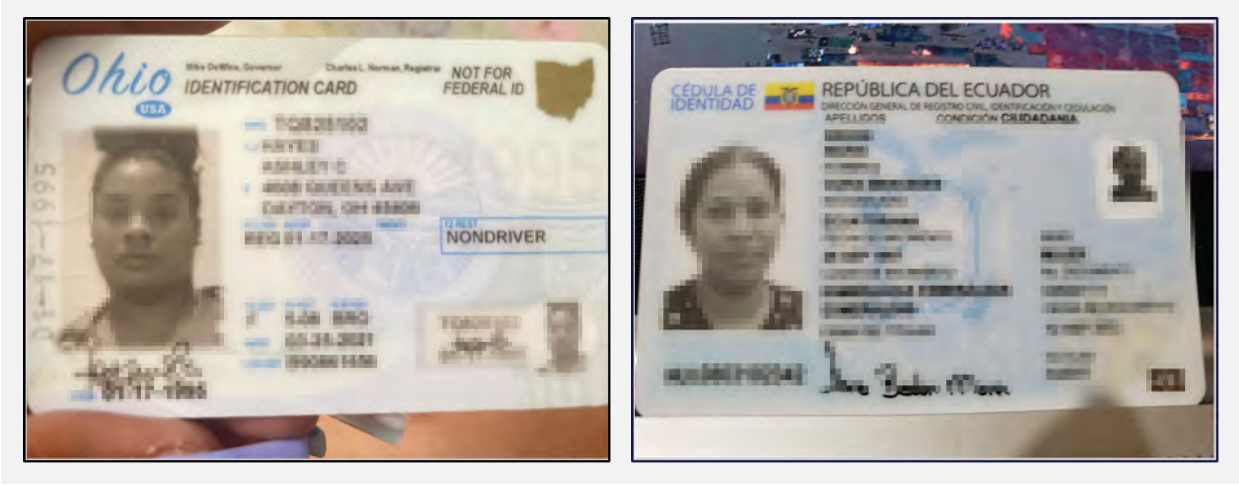


Figure 9: Uploaded images located in the "storage/app/public/uploads" directory

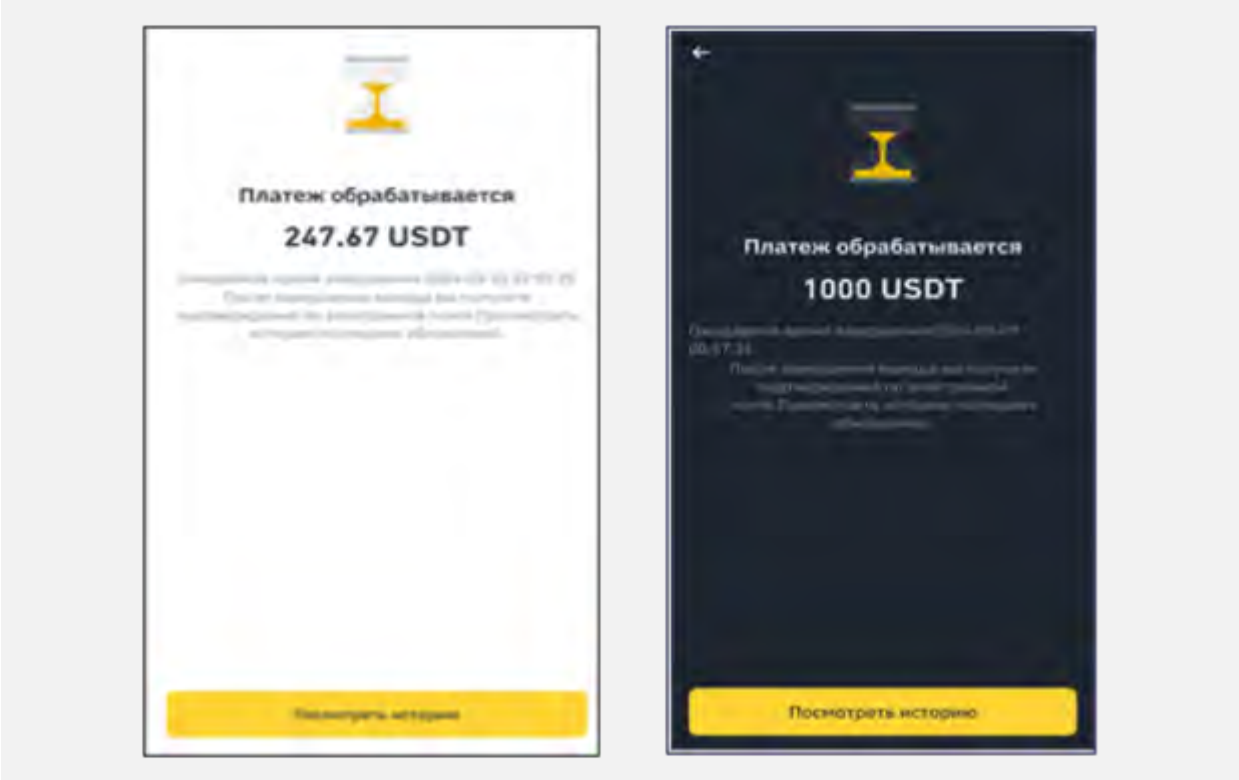
These platforms require victims to submit personal identification, such as ID cards, driver's licenses, or passports, during registration, which can later be used for blackmail or sold as personal data.



Figures 10-11: Examples of identification cards uploaded by the victims to the platforms.

We also discovered images related to transaction confirmations, which reveal victims' attempts to transfer funds to these fraudulent schemes.

The total estimated losses for victims impacted by these six platforms amount to several thousand dollars. However, since Cyberint has identified over 1,000 domains using this specific scam template, victim losses are likely in the tens or even hundreds of thousands of dollars.



Figures 12-13: Examples of payment receipts uploaded by Russian-speaking victims to the platforms.

The impact of these 6 scam websites is worldwide, affecting a broad range of 27 countries, including: Algeria, Argentina, Brasil, Canada, Colombia, Dubai, Ecuador, Egypt, Iran, Jordan, Mauritania, Mexico, Morocco, Nicaragua, Philippines, Russia, South Africa, Spain, Sudan, Suriname, Tajikistan, Turkey, United Arab Emirates, United Kingdom, United States, Uzbekistan, and Yemen.

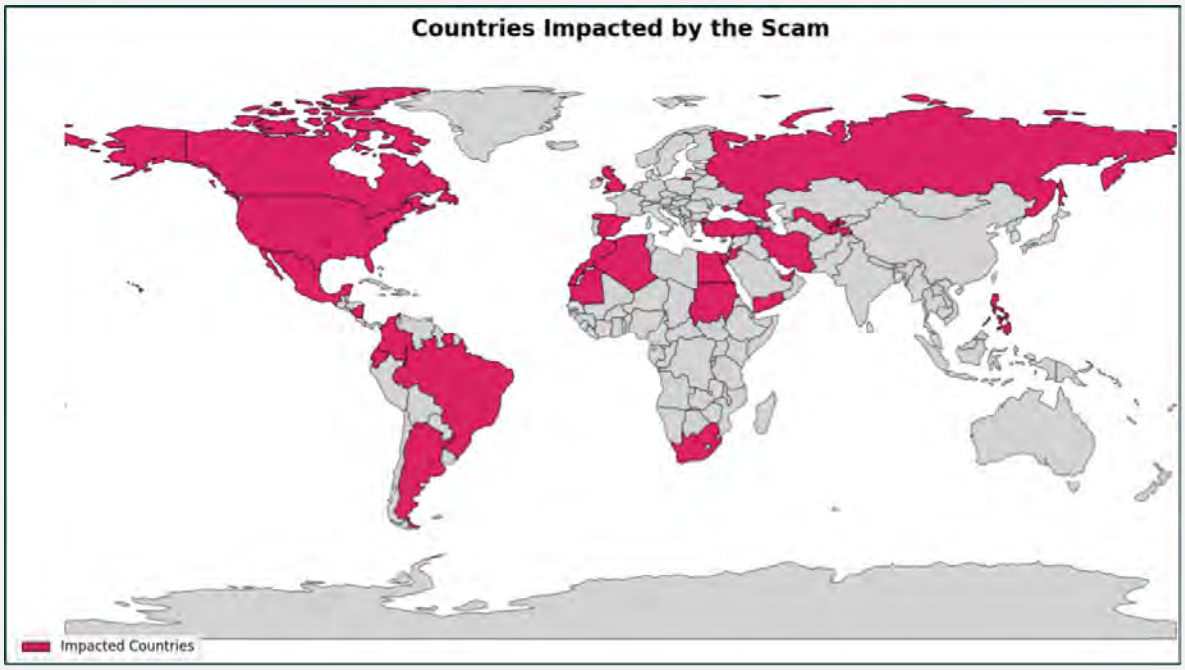
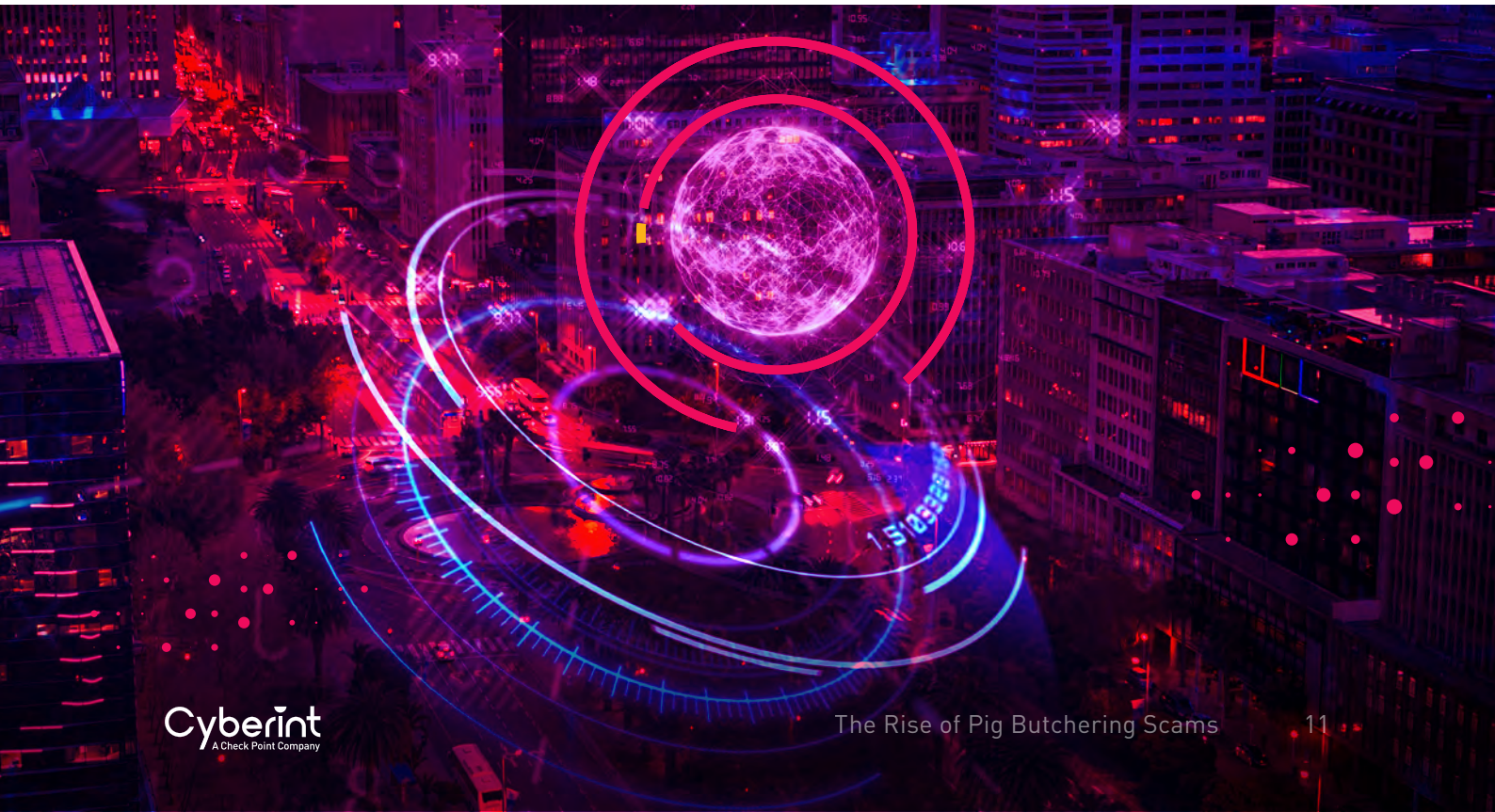


Figure 14: Map highlighting countries impacted by the six fraudulent platforms we investigated. The highlighted regions indicate the global reach of these scams, spanning multiple continents and affecting diverse populations across North America, South America, Europe, Africa, and Asia.

Based on the images, the victims come from diverse backgrounds, with no specific gender, age, or other demographic making an "ideal" target.



Scam Promotion

Our investigation has revealed that scam operations are primarily promoted via social media, with Facebook being a key platform. Scammers often impersonate "attractive" and "successful" men and women to lure potential victims into investing in fraudulent forex schemes. This tactic was first used by Chinese threat actors when pig butchering began in 2016, with romance scams being the primary method to lure victims. Scammers built fake relationships to gain trust before introducing fraudulent investments, similar to today's approach of impersonating attractive, successful individuals on social media.

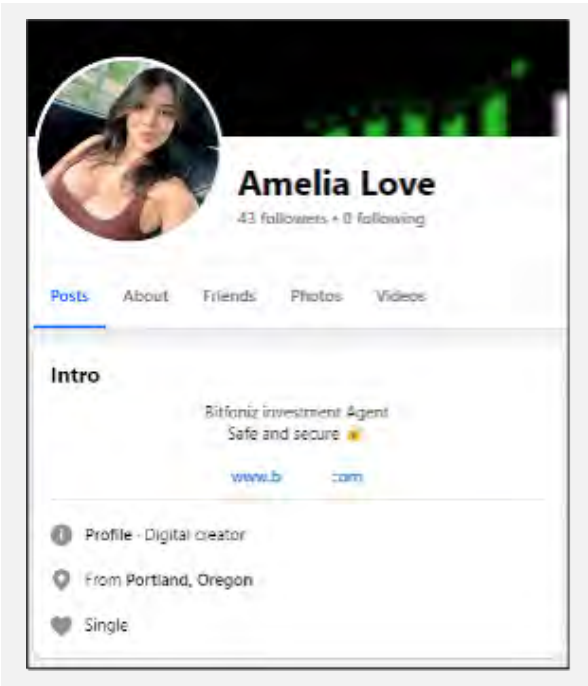


Figure 15: A Facebook profile of an "attractive woman" actively promoting the scam.[7]

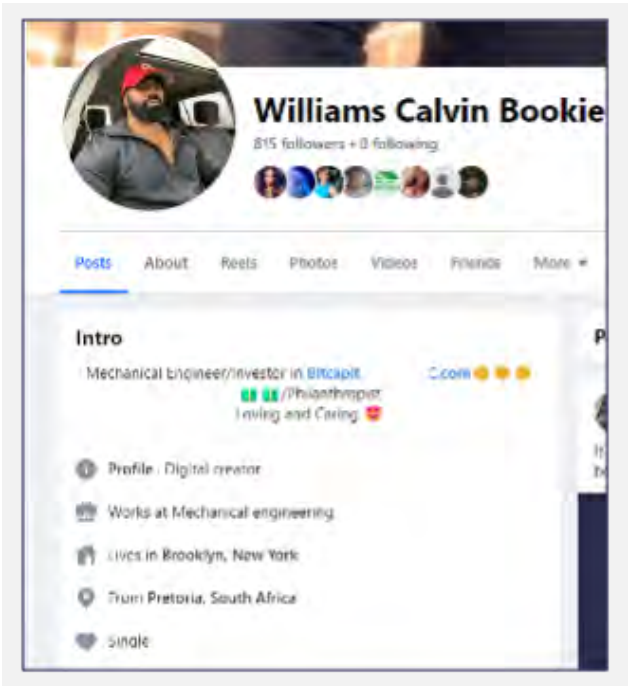


Figure 16: A Facebook profile of a successful and attractive man actively promoting the scam.[6]

[6] https://www.facebook.com/profile.php?id=61556731795226 - link taken down by Facebook at time of print

[7] https://www.facebook.com/profile.php?id=61556299145340 - link live at time of print, but likely to be taken down

Examples of Promotional Content

Scammers post about financial success and the ease of investment, often sharing fabricated success stories and providing step-by-step instructions for depositing funds. Some examples include:

1. Fabricated Success Stories:

Posts congratulating individuals on large "profits" from fraudulent platforms. to make victims think trading is easy and profitable.

Figure 17: A fabricated success story promoting crypto investment, urging readers to reach out for details.[9]

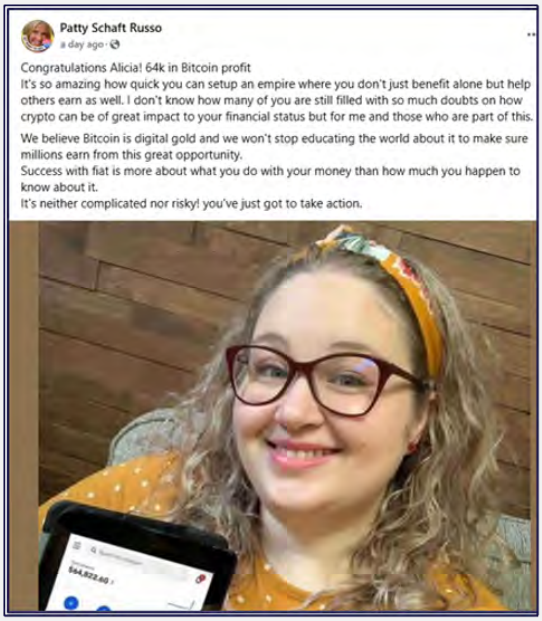


Figure 18: Fabricated story of a $64k Bitcoin profit, promoting crypto as an easy wealth opportunity.[8]

2. Motivational Posts:

Inspirational quotes paired with links to fraudulent sites, appealing to users' desire for financial success.

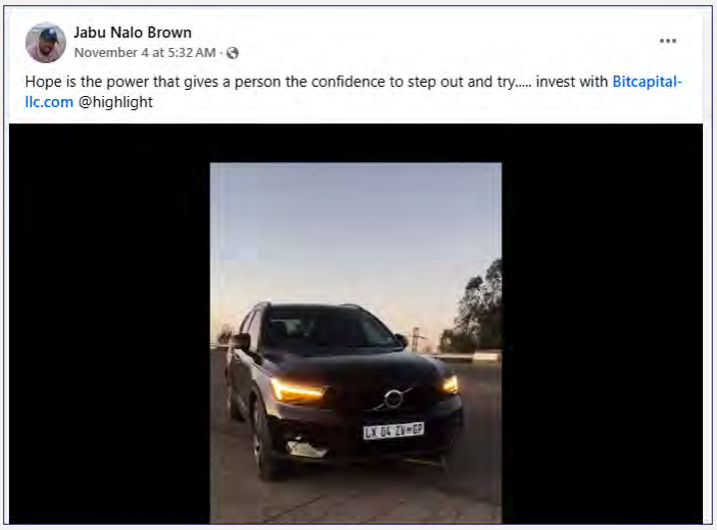


Figure 19: The threat actor uses motivational posts with luxurious cars like this, to lure victims into investing in fraudulent platforms [10]

---

[8] https://www.facebook.com/russopl/posts/pfbid02JmrNg8MZXhi2bvsb2zxENDsub3SihUmqR7yURTt3beNTUF6hKNiJ46Fwmunrx4s5l - link taken down by Facebook at time of print

[9] https://www.facebook.com/russopl/posts/pfbid09MNDTfqh5Trym4FQAoiG5Amp2jnpv996csFjnvCzgJUCBGc8H2CxAXQ33tJEaTfsl - link taken down by Facebook at time of print

[10] https://www.facebook.com/100082268303158/videos/1196223238104890 - link live at time of print, but likely to be taken down

Engaging With the Scammers

Our proactive controlled engagement revealed several key characteristics of this scam:

1. Impersonation of Industry Figures:

- The scammers exploited the identity of Larry Collin by using his profile picture and name on their Telegram account. The usage of Larry's identity - a well-known figure in the crypto industry, originated in the Philippines, likely helped lend credibility to their scam.

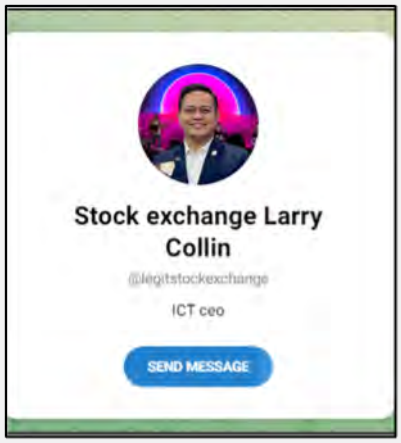
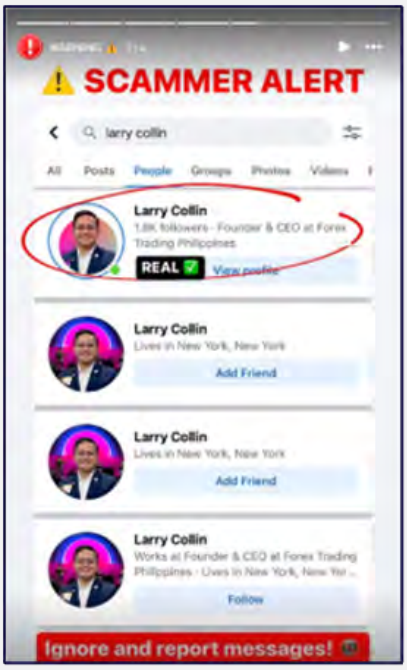


Figure 20: The threat actors used Larry Collin's identity to boost their credibility.

- The original social media profiles of Larry Collin have issued warnings about impersonation and scams.[11]



Figures 21-22: Larry's official profiles issued warnings about impersonation scams.

[11] https://www.instagram.com/stories/highlights/17895469544801907/

2. Inconsistent Cover Story

- When further communication took place, the scammers then claimed to be Ramon S. Monzon, the President and CEO of the Philippine Stock Exchange, and not Larry.[12]

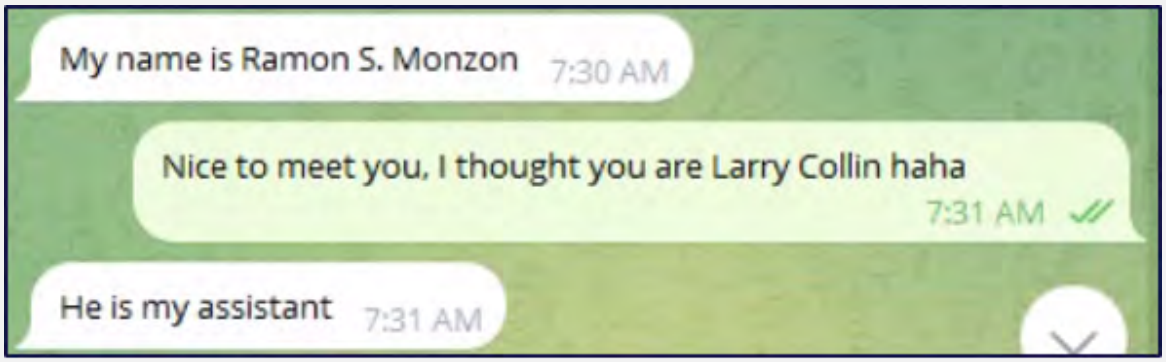


Figure 23: The threat actor posed as another individual, weakening the credibility of their cover story.

- They claimed to be from the Philippines, but when asked if they spoke Tagalog, a popular language of the Philippines, they responded that they understood it but preferred to communicate in English, which made it less likely that they were actually from the Philippines.

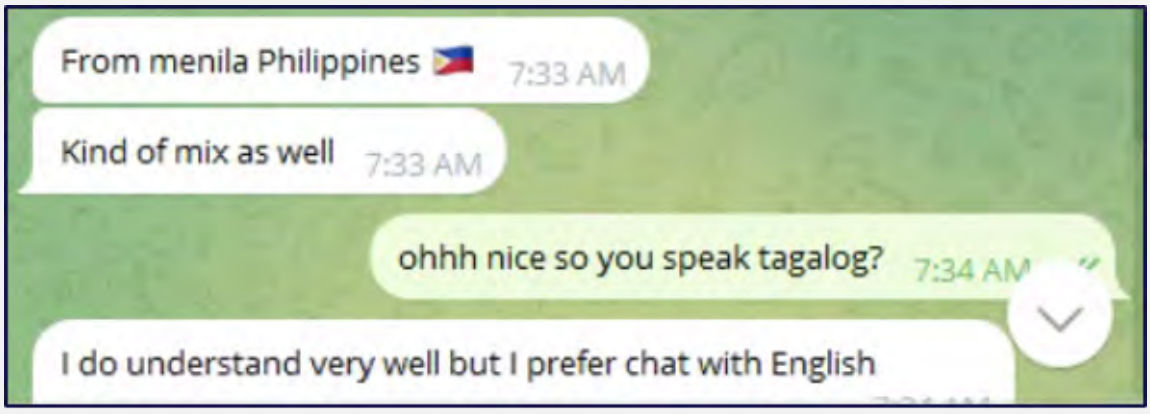


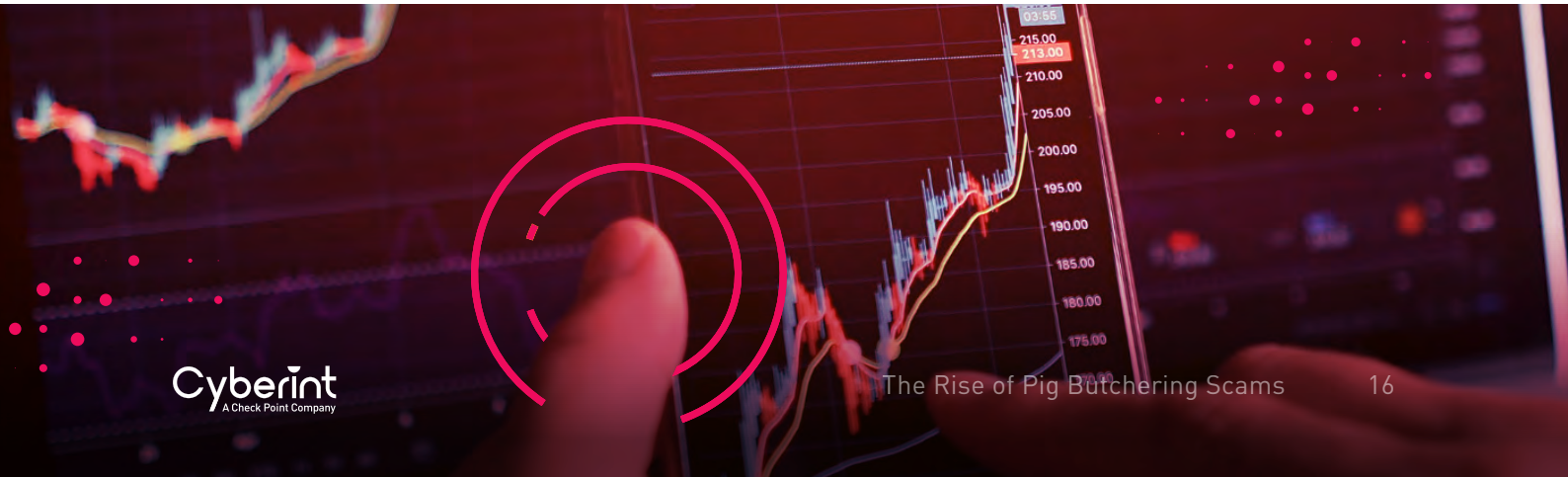
Figure 24: The threat actor claimed to be from the Philippines but avoided speaking Tagalog, making their origin doubtful.

[12] https://www.bloomberg.com/profile/person/20129791

3. Promising Exorbitant Returns:

- The threat actors offered victims a ten-time return on their investment, a highly unrealistic and unsustainable promise.

Figure 23: The threat actor posed as another individual, weakening the credibility of their cover story.



4. Social Engineering Tactics:

- The scammers shared fake screenshots of satisfied customers to build trust and credibility.

- They provided a fraudulent certificate of incorporation to further legitimize their operations.

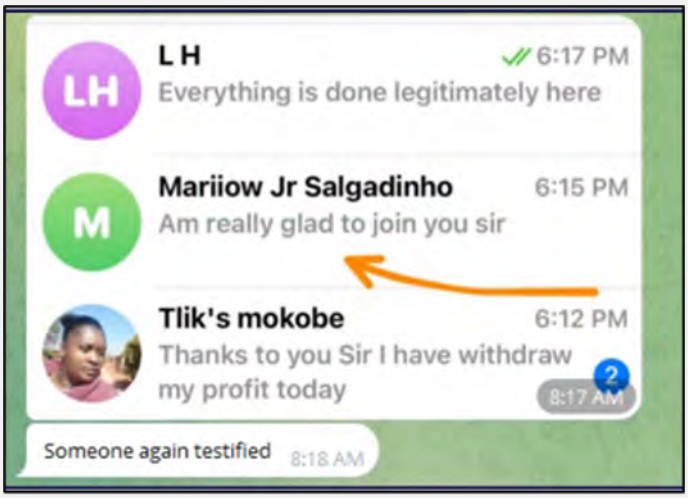


Figure 26: Fake screenshots of supposed satisfied customers used to build trust and credibility.

Figure 27: Fraudulent certificate of incorporation presented to make the operation appear legitimate.

5. Geographic Red Flags:

- Invoices sent by the threat actors were denominated in Papua New Guinean Kina (PGK), suggesting potential origins in that region.

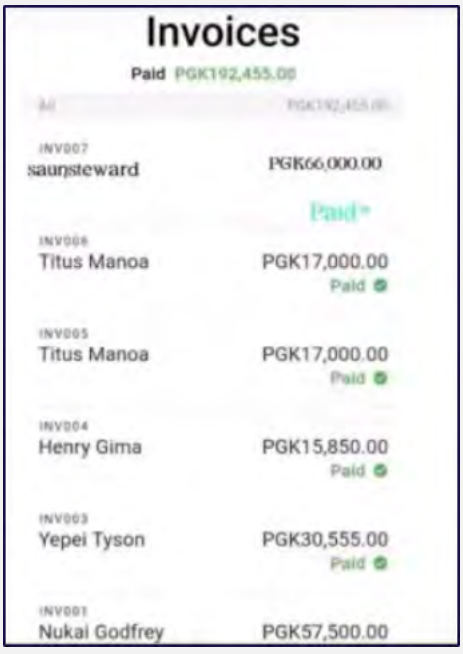


Figure 28: The threat actor provided invoices implying a connection to Papua New Guinea.

CONCLUSIONS

Pig butchering scams have grown from their origins in China to become a global threat, with some operations led by groups in Africa. Using social media, especially Facebook, scammers impersonate successful individuals to lure victims into fake investment schemes.

Threat actors exploit the general public's limited knowledge of cryptocurrency, and combined with pig butchering techniques, this makes these types of scams increasingly prevalent and efficient.

Our investigation uncovered over 1,000 domains promoting these scams, relying on low-sophistication tactics to interact with victims. Despite this simplicity, these scams are estimated to cause significant financial losses across 27 countries, impacting diverse demographics with no specific "ideal victim" profile.

With the rise of AI, creating convincing and functional fraudulent platforms has become easier, likely fueling the continued growth of these scams as more types of threat actors get involved, attracted by high success rates.

RECOMMENDATIONS

1

Be Skeptical of High-Return Investment Offers:
If an investment opportunity promises unusually high returns with little risk, it's likely a scam. Genuine investments rarely guarantee high returns, especially within short timeframes.

2

Verify Platform Legitimacy:
Before investing, research the platform thoroughly. Check for verifiable registration details, official business licenses, and reviews from trusted sources. Be cautious of websites that lack transparency or only provide limited contact information.

3

Avoid Sharing Personal Information:
Scammers often request personal identification information during "registration." Avoid sharing sensitive data like ID cards, passports, or driver's licenses, especially on unfamiliar platforms, as these can be used for identity theft or blackmail.information.

4

Be Skeptical of Social Media Profiles Claiming Success:
Scammers use social media to impersonate attractive, successful individuals to build a sense of trust and legitimacy.

5

Report Suspicious Platforms and Profiles:
If you suspect a platform or individual is attempting to scam you, report it to relevant authorities or the social media platform. Reporting helps prevent others from falling victim to similar schemes.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-37-286-777
17 Ha-Mefalsim St Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House,
14-18 Great Titchfield Street,
London, W1W 8BD

USA - TX

Tel: +1-646-568-7813
7250 Dallas Parkway STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
Level 42, Suntec Tower 3,
8 Temasek Boulevard. Singapore 038988

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road
Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm