CYBERCRIME AND THE ASIA-PACIFIC REGION

Meghan Edwards

The Aracari Project

WWW.ARACARIPROJECT.IO

Abstract

In an increasingly digital world cybercrime continues to rise. Cybercrime continues to represent an increasing threat to Asian countries. This study analyzes the different forms of cybercrime and the associated scams linked to it along with analyzing why these crimes are occurring at an increased rate. This study's ultimate goal is to increase understanding of cybercrime in the Asia-Pacific region, discuss why cybercrime is so high there, and offer a comprehensive view of the leading groups carrying out these attacks. This study will be conducted using content analysis using publications on cybercrime, cybercrime, and scams in the Asia-Pacific region, and publication and data on the various groups carrying out these scams and attacks.

Keywords: Cybercrime; Asia-Pacific; DDoS; Ransomware; Hack

Introduction

Cybercrime is widely prevalent and increasing as the world continues to modernize, it has increased at a high rate in the Asia-Pacific region for a multitude of reasons. Three major reasons include a lack of cyber security and awareness, quicker transactions, and an increase in internet connectivity (Harby, 2019). The major forms of cyber-attacks that are prevalent in the Asia-Pacific region include "ransomware, scams, crime as a service attack (the practice of cybercriminals selling access to the

tools and knowledge needed to execute cybercrime), hacking and Denial of Service (DDoS) Attacks (attacks designed to crash IT systems)" (Williams, 2022).

This research aims to analyze the current literature surrounding cybercrime and scams in the Asia-Pacific region and offer a comprehensive review of why these crimes are occurring at an increasingly heightened rate as well as offering a detail explain of who these actors are and where they are located. This research will further analyze what the crimes are and how they are being conducted. The hope is that this research will offer a more concise and comprehensive look into the current data out there.

Literature Review

The rapid growth in internet use in the Asia-Pacific region (especially in China, Indonesia, and India) since 2002, has contributed to the significant increase in cybercrime in the region (Broadhurst & Chang, 2013). The top countries to experience the largest increase in cyberattacks in the Asia-Pacific region were Japan, Singapore, Indonesia, and Malaysia. The increase in occurrence of these crimes continues to rise, for example, the Check Point Research report stated, the Asian Pacific region experienced a 168% year-on-year increase in cyberattacks in May 2021 compared to May 2020 (Williams, 2022).

China

The Chinese Judicial Big Data Research Institute conducted an analysis of cybercrime in China and discovered that between 2017-2021 40% of their cybercrimes involved some form of fraud. Most of these fraud cases focused on fake loans, impersonation, and false recruitment (Wyk, 2022). A recent case involving false recruitment and a "Pig Butchering" scam (gaining someone's trust under false pretenses to get them to invest in phony investments and taking all of their money) (Olcott, 2022) involved the Chinese Mafia who falsely recruited individuals from the Philippines under the guise of employment with call centers and offshore gaming operator jobs in Thailand. However, these individuals would end up becoming victims of Human Trafficking as they were brought to Myanmar where the victims are then taught how to scam people around the world by establishing relationships through social media apps like Facebook, WhatsApp, and the dating platform Tinder (Butts, 2022). They were instructed to target professionals and get them to invest in cryptocurrency apps that would take their money and give it to the Chinese Mafia. Failure to comply with this would result in a lack of food, being sold to another company, and threats to their lives (Butts, 2022). However, many more groups within China are a lot more active, many of whom target high-profile companies.

One of the most active Chinese Hacking groups that were named by the U.S Department of Justice in 2020, is the Double Dragon (also known as ATP41, Barium, Winnti, Wicked Panda, Wicked Spider, TG-2633, Bronze Atlas, Red Kelpie, and Blackfly). They are believed to be sponsored by the Chinese Communist Party (CCP) for espionage purposes while also moonlighting for their financial gain. One such operation they conducted compromised over 100 different companies (Carrega & Perez, 2020). Double Dragon has targeted over 14 countries, most notably the United States. Some of their activities include incidents of tracking, the compromising of business supply chains, and collecting surveillance data. One of their most recent operations occurred in 2022 where they stole at least $20 million in COVID-19 relief aid for the United States (Carrega & Perez, 2020; Fitzpatrick & Ramgopal, 2022). Double Dragon uses a variety of techniques including passive backdoors to access files (which is harder to detect than the traditional backdoor access) and supply-chain compromises where they inject code into legitimate files to compromise the system and gain access. Finally, they will often use a malware program known as Bootkit (a variation of rootkit that replaces the original program with a compromised one to gain access, it is incredibly difficult to detect). These tools are utilized most often through false video games that will give them total access to a system (Fraser et al., 2019).

Hong Kong

Hong Kong specifically has seen a significant increase in cryptocurrency scams, as of 2022, Hong Kong saw a 105% increase in these scams since 2021. They have seen HK$1.5 billion (US$ 201 million) in crypto scams alone between January and June of 2022, a 41% increase compared to the same time frame in 2021 (Liu, 2022). A major component of these scams comes from romance and investment scams. Individuals will meet their victims online, posing as attractive young men and women and they will eventually convince the individual to invest in cryptocurrency. One such scam would target people on various dating sites like Tinder. Once a foundation of trust was built they would then be convinced to buy legitimate cryptocurrency through WhatsApp and then trade it into OEN (Crypto Coin) . These scammers would use two different sites to make the trade into OEN, Bitfex. pro and Bitfex.vip (Chan, 2021). The investors would then proceed to go and pull out the expected profits from the investment but instead would be asked to put more money in, eventually leaving them with very little cash and the scammer would proceed to disappear. Bitfex.pro is suspected to be a sister website to the Hong Kong-based site oen.asia, both of which are run by Wu Weidong, who is suspected of running five other similar sites (Chan, 2021).

Many similar scams will use fake crypto websites that will create a fake chart that will showcase one's deposited funds growing. Many will even allow an individual to withdraw a small number of their funds in an attempt to build trust, however any attempt to withdraw all of one's funds will show that they have no money in their account (Tse, 2023).

Hong Kong has begun to take steps in combating crypto-based scams, such as drafting regulatory requirements for licensed crypto exchanges and working on amendments to their licensing regime for virtual asset service providers. This will require a license to conduct crypto business in Hong Kong and will take effect in June of 2023 (Qin, 2022). In September 2022, the Hong Kong police also launched a service called Scameter. A service that will allow users to search phone numbers, and names to see if they have been flagged as being related to a scam. They will be color coordinated to indicate the risk level or indicate if they have not been linked to any scam services. Finally, the site will also provide fraud prevention tips (Zou, 2023).

Indonesia

The Financial Transaction Reports and Analysis Centre of Indonesia (PPATK) has reported a significate increase in cybercrime between 2019-2021, there was a reported 9,801 reported cases in 2019 whereas there were 23,000 reported in 2021

(UNDOC, 2022) One common scam is the Pig Butchering method, rather then a typical romance scam, the individual will text a number acting as if they know them, should the victim reply saying they have the wrong number the scammer will then attempt to strike up a conversation to get them to become friendly with one another (Newman, 2023). If the victim takes the bait, the scammer will eventually suggest that they invest in cryptocurrency, should they agree, they will suggest a malicious app or website to utilize, many of which mimic legitimate services. They will be able to draw out a small amount to make it appear legitimate, however, once they invest all that they can the scammer will stop correspondence, take the money, and disappear (Newman, 2023).

Malaysia

Between 2017-2021 Malaysia reported 98,607 online fraud cases, one major scam was romance scamming. (Hazim, 2022) One such cryptocurrency scam associated with this is what is known as the CryptoRom (utilizing apps that give full access to one's information and data), which targets Android and iPhone users through the popular dating apps Bumble and Tinder. Once the scammer has gained the victims' trust, they will convince them to invest in cryptocurrency on fake websites. When the victims would try to withdraw their invested money, they would find that

their accounts had been frozen, and they must pay hundreds of thousands of dollars in fake profit taxes to regain access (Wong, 2022). Along with that, some of the practitioners of the CryptoRom scam, have learned how to bypass much of Apple's software that prevents scams by using Apple's TestFlight programs to test beta apps. Some individuals who test the beta apps had been instructed via email to test an app called BTCBOX, a Japanese Cryptocurrency exchange. Many of which utilize minimal coding to gain access (Wong, 2022).

Singapore

The Singapore police force reported in 2021, that cybercrime, more specifically scams, increased by 36% from the 2020 reports. Like the scams in Hong Kong, many Singaporeans have fallen victim to romance scams that follow the Pig Butchering scam. Many victims would be lured into investing in some form, where they would have to pay administrative fees, security fees, or taxes to reap their profits. Many earned a small profit in the initial stages, leading them to believe that the investments were real, the money would usually be transferred to a bank located in China and Hong Kong (Tan, 2022).

Another major cybercrime in Singapore utilizes deep fake accounts of high-profile individuals (such as Elon Musk) to enter into cryptocurrency giveaways in

exchange for their crypto wallet details and personal information (Sum, 2022). A Singapore cyber security group known as Group IB found that this scam alone garnered S$2.4 million (USD$1.68 million) between February 16th-18th 2022. These scams involved a total of 281 transactions all linked to a deep fake account promoting a cryptocurrency giveaway (Sum, 2022). A main issue that Singapore has found is the difficulty in solving these types of cases as many of these crimes are being committed by people outside of Singapore. Most of the money transactions are to accounts outside of Singapore as well, making it difficult for the individuals to get their money back and difficult to solve unless they have the cooperation of law enforcement agencies outside of Singapore (Sum, 2022).

Method

This research is a nonreactive study employing content analysis as it utilized data and research that had already been published. A content analysis analyzes certain words, ideas, and phrases to understand better the topic and research focus area (Pedhazur & Schmelkin, 1991). Content analysis can take one of two approaches latent (interpret the meaning) or manifest content (evidence that is directly seen, such as words or phrases). This study utilizes the latent content method (Holsti, 1969). The research study design used content analysis to explore various works, including

reports and literature reviews, on cybercrime with a focus on crypto-based internet crime. These sources were chosen due to their in-depth analysis of cybercrime in the Asia-Pacific region and their focus on cryptocurrency scams.

Sample Design

This analysis employed a purposive sample as the topic area was very specific. A purposive sampling method is a nonprobability sampling method that involves the researcher using their expertise to select a sample that is most useful to the purposes of the research. Which relies on qualitative data rather than statistical data (Lavrakas, 2008). This research focused solely on cybercrime that involved any sort of money exchange with an emphasis on cryptocurrency-related crimes and it excluded any data involving cybercrime outside of these set focal points. This research focused on different elements of the crime such as how they were being committed, what areas or regions these crimes were found in, why they were occurring at higher rates, and what groups may be responsible for the crime. The sources used allowed for a better understanding of the different countries of focus along with a better understanding of why these cybercrimes were occurring at a higher rate.

Key Variables

This research included independent and dependent variables. The independent variable of increased internet usage and cryptocurrency popularity affects the dependent variable of cybercrime and cryptocurrency scams. The increase in internet usage and the popularity of cryptocurrency allowed cybercrime to rise at a much faster rate. These variables seem to support the ideology that as internet use increases so too will internet crime.

Results

An extensive search was conducted on the various cyber crimes affecting the Asia-Pacific region with an emphasis on cryptocurrency-based crime. In looking at all the published work relevant to this research, it had to meet specific criteria, as noted in the methods section. The following table from Statista will showcase the highest internet usage by country in Asia. Table 1: Internet usage by country, specifically looking at the highest internet usage. This table helps to show a correlation between the aforementioned evidence of increased cybercrime in the specific countries listed out as it correlates with the increased use of the internet. It should note that this graph does exclude Hong Kong in this graph.

Table 1: Highest-rated internet usage by country in Asia

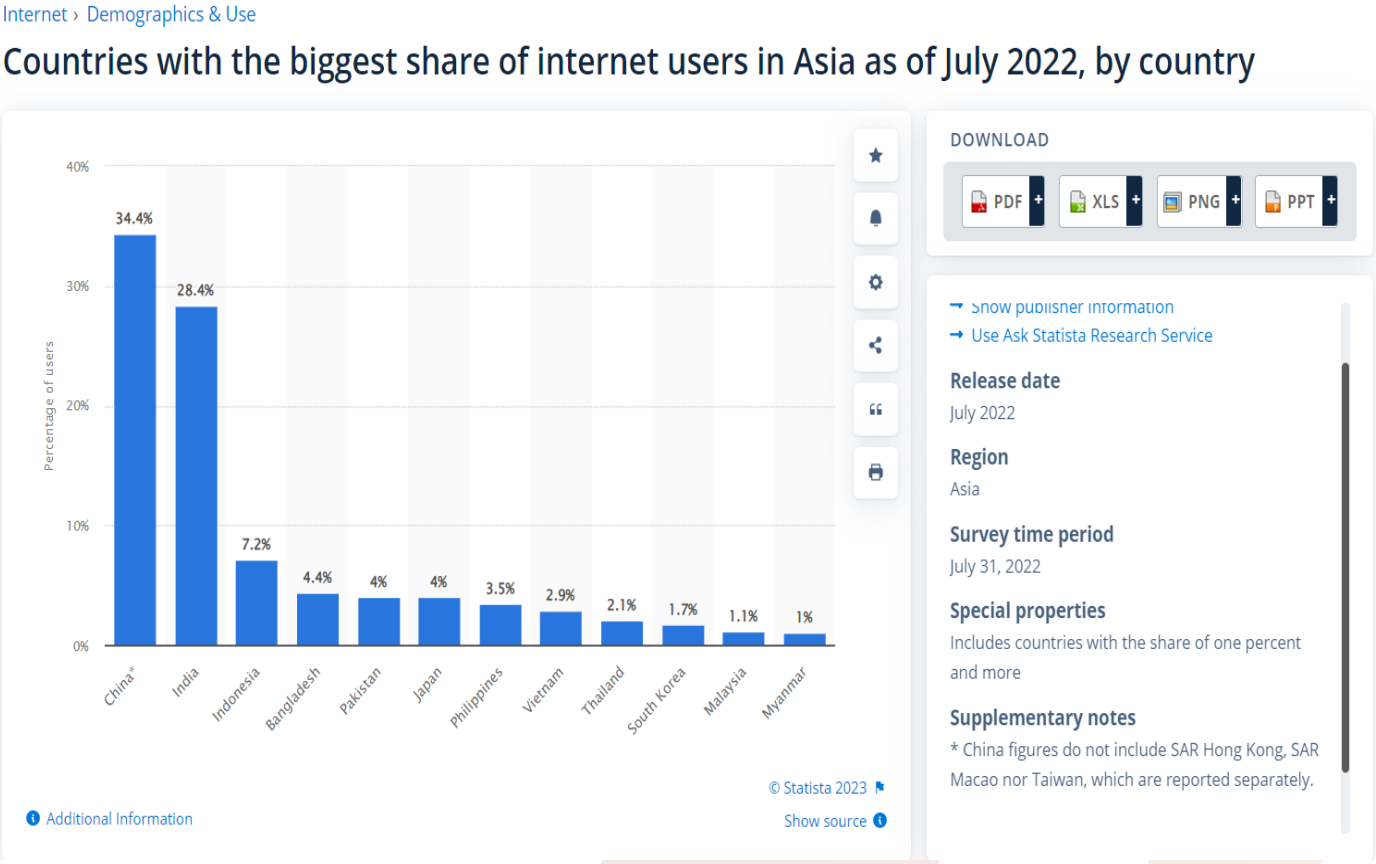


Table 1

The above table represents the highest-rated internet users in Asia with the corresponding rates throughout 2022.

Figure 1 provides an example of a romance scam that is prevalent in Indonesia where they will purposely text a wrong number.

Figure 1: Example texts of romance scams in Indonesia (Genc, 2022)

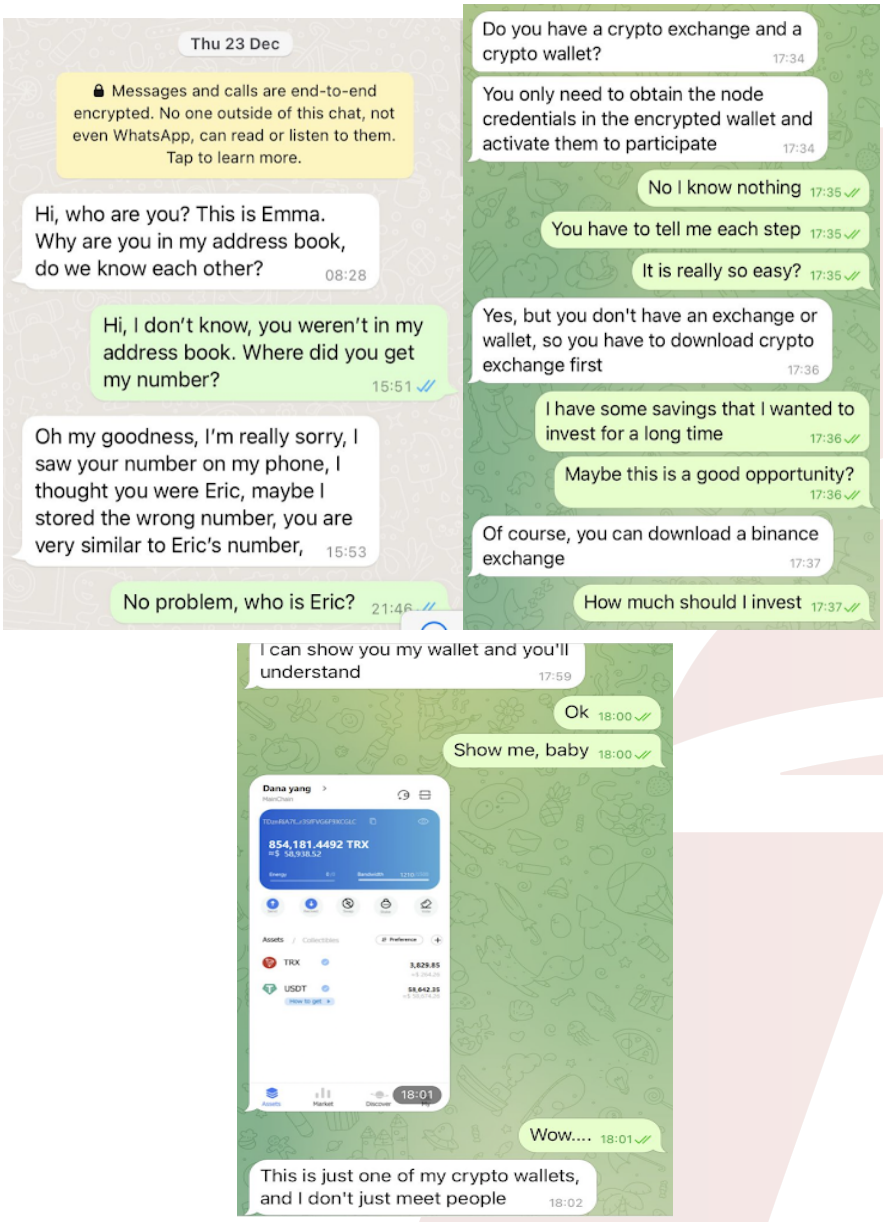
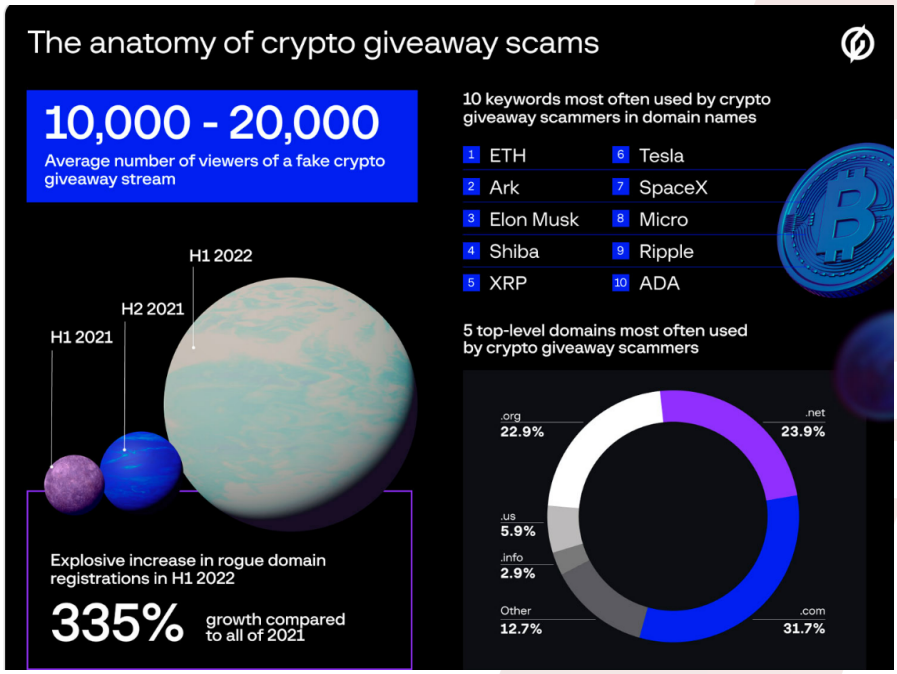


Figure 1

The above figure offers an example of how a scammer may reach out and hook someone in through conversation to invest in cryptocurrency where they hold total

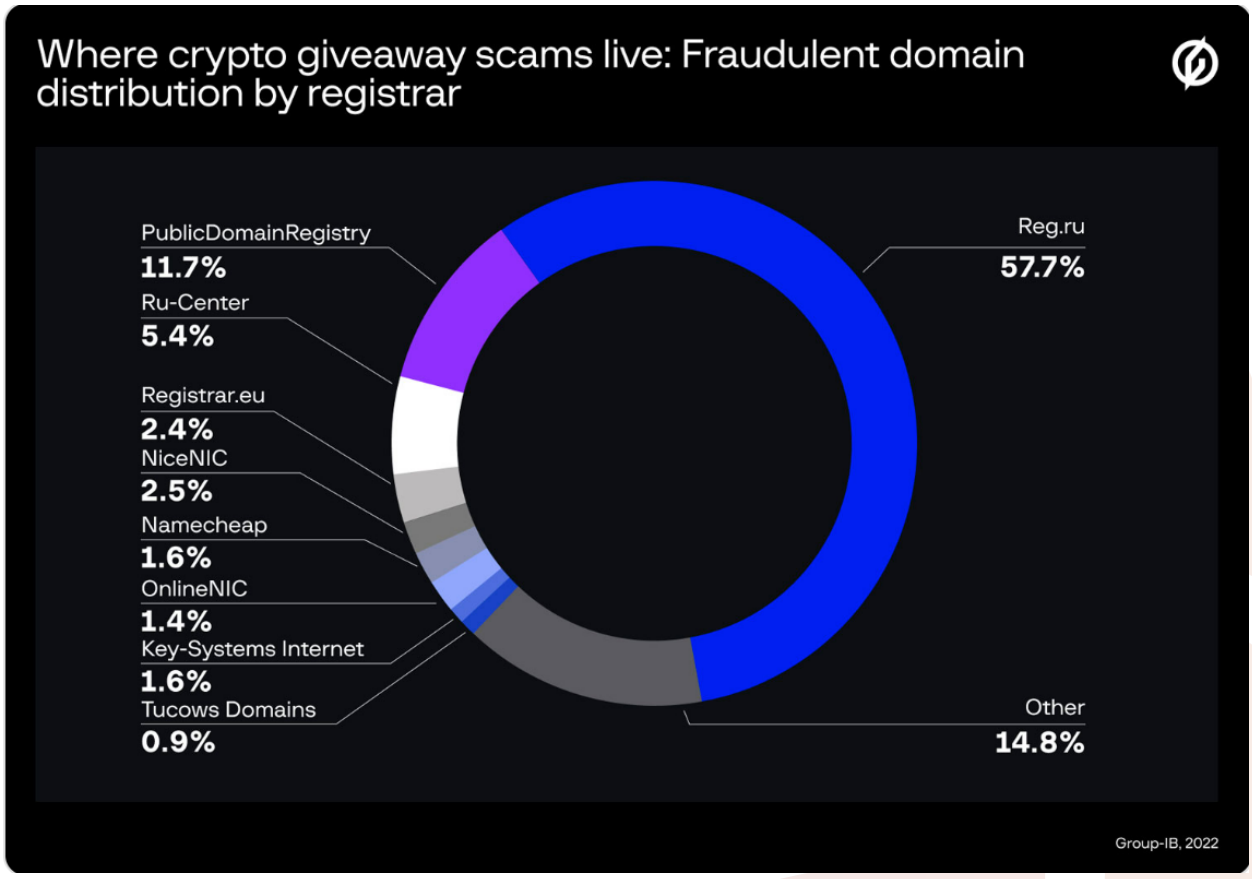
control over the victim's account and information. Figure 2 shows the average statistics of cryptocurrency giveaway scams, along with popular verbiage associated with this type of scam.

Figure 2: Anatomy of cryptocurrency giveaway scams (Group-IB, 2022)



The above figure breaks down crypto giveaway scams based on keywords and how the prevalence of these scams has increased between 2021-2022. Figure 3 will show a further breakdown of this data by breaking down the most used domains in this form of scam.

Figure 2: Crypto giveaway scams domain distribution by registrar (Group-IB, 2022)



The results of this study have found that the most prevalent scams related to cryptocurrency in the Asia-Pacific region appear most often to be romance scams and scams involving fake websites, apps, and giveaways. The prevalence of these scams has increased immensely as internet usage within this area increases. More specifically, crypto-based crime has increased due to its rising popularity and the promise that an individual could get a lot of profit quickly.

Conclusion

This research aimed to offer a more comprehensive view into the current data that is out there regarding cybercrime in the Asia-Pacific region and offer a potential explanation as to why these crimes occur at such a high rate within the region. This study showed that a major contributing factor to this is the increased internet usage and the global popularity of cryptocurrency. However, as previous literature has shown there are other mitigating factors as to why this crime has such a high rate in the region, and that may be due to a lack of knowledge and how to identify these scams before one will commit to these investments.

One limitation of this study was not having access to the social concepts and understanding of the region surrounding cryptocurrency and whether it is a common topic of discussion to discuss with one's cohorts the risk of being scammed.

Further analysis should include a social aspect to understanding why crypto-based scams are occurring at such a high rate in the Asia-Pacific region as cultural aspects may help to better understand why this crime is occurring at such a significant rate. Further analysis should also include a deep look into what, if any, training or public service announcements are offered in these regions that are easily accessible for all on what to look out for before one will invest in any form of crypto. This analysis supported the hypothesis as it found that the increased usage of the internet,

more transactions, and lack of training and knowledge create the perfect trifecta for cybercrime like cryptocurrency scams to occur. The importance of analyzing the methodology utilized by scammers and where these particular methods are seen most often are both areas underscored through this research project. Future research should aim to use this data and relate it to social factors within the Asia-Pacific region.

References

Broadhurst, R., & Chang, Y.-C. (2013). Cybercrime in asia: Trends and challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2118322

Butts, D. (2022, November 24). *Chinese mafia forcing Filipinos to work for crypto scams, says Philippine senator*. Forkast. Retrieved January 17, 2023, from https://forkast.news/chinese-mafia-forcing-filipinos-to-work-for-crypto-scams-says-philippine-senator/

Carrega, C., & Perez, E. (2020, September 16). *5 Chinese nationals among those charged with cyberhacking that victimized over 100 people and companies worldwide | CNN politics*. CNN. Retrieved January 18, 2023, from https://www.cnn.com/2020/09/16/politics/chinese-nationals-cyberhacking/index.html

Chan, E. (2021, July 19). *Sexy fraudsters scam $546m from crypto punters*. The Standard. Retrieved January 18, 2023, from https://www.thestandard.com.hk/section-news/section/11/232236/Sexy-fraudsters-scam-$546m-from-crypto-punters

Fitzpatrick, S., & Ramgopal, K. (2022, December 5). *Hackers linked to Chinese government stole millions in Covid Benefits*. NBC News. Retrieved January 18, 2023, from https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636

Genç, E. (2022, December 10). *Crypto romance scams: Don't fall for these dating App Swindlers*. CoinDesk Latest Headlines RSS. Retrieved January 23, 2023, from https://www.coindesk.com/learn/crypto-romance-scams-dont-fall-for-these-dating-app-swindlers/

Group-IB. (2022, September 16). *Scammers made $1.6 million in yet another fake crypto giveaway - group-IB*. Group-IB. Retrieved January 23, 2023, from https://www.group-ib.com/media-center/press-releases/crypto-trap/

Harby, D. (2019, August). *The rise of cybercrime in Asia Pacific and considerations for organisations operating in the region*. Holman Fenwick Willan Law Firm. Retrieved January 17, 2023, from https://www.hfw.com/The-rise-of-cybercrime-in-Asia-Pacific-and-Considerations-for-organisations-operating-in-the-region-August-2019#:~:text=1.,investment%20and%20low%20awareness2.

Hazim, A. (2022, May 24). *Malaysia's crypto scene a goldmine for scammers - the Malaysian Reserve*. The Malaysian Reserve. Retrieved January 18, 2023, from

https://themalaysianreserve.com/2022/05/24/malaysias-crypto-scene-a-goldmine-for-scammers/

Holsti, O. R. (1969). Content analysis for the social sciences and humanities. Reading, MA: Addison-Wesley.

Lavrakas, P. J. (2008). *Encyclopedia of survey research methods* (Vols. 1-0). Thousand Oaks, CA: Sage Publications, Inc. doi: 10.4135/9781412963947

Liu, O. (2022, August 4). *HK$387.9 million in cryptocurrency scammed in first half of 2022 in Hong Kong*. South China Morning Post. Retrieved January 18, 2023, from https://www.scmp.com/news/hong-kong/law-and-crime/article/3187760/cryptocurrency-scams-made-most-money-conned-through

Newman, L. H. (2023, January 2). *What is a pig butchering scam?* Wired. Retrieved January 18, 2023, from https://www.wired.com/story/what-is-pig-butchering-scam/

Olcott, E. (2022, June 27). *Crypto swindlers prey on ethnic Chinese women looking for Love*. Financial Times. Retrieved January 17, 2023, from https://www.ft.com/content/b325b37a-ae62-4af1-ba56-568598d2dbe7

Pedhazur, E. J., & Schmelkin, L. P. (1991). Measurement, design, and analysis: An integrated approach. Hillsdale, NJ: Lawrence Erlbaum.

Qin, N. (2022, December 13). *Hong Kong mulls regulatory requirements for local licensed crypto exchanges: Report*. Forkast. Retrieved January 18, 2023, from https://forkast.news/headlines/hong-kong-mulls-regulatory-requirements-for-local-licensed-crypto-exchanges-report/

Statista. (2023, January 3). *Asia: Distribution of internet users by country 2022*. Statista. Retrieved January 23, 2023, from https://www.statista.com/statistics/272358/distribution-of-internet-users-in-asia-pacific-by-country/

Sum, D. (2022, November 15). *Crypto scams tripling every year globally, victims lured by Deepfakes and giveaways: Experts*. The Straits Times. Retrieved January 23, 2023, from https://www.straitstimes.com/singapore/crypto-scams-tripling-every-year-globally-victims-lured-by-deepfakes-and-giveaways-experts

Tan, C. (2022, February 21). *Everything about pig-butchering scams, a scam variant that's in s'pore now*. Goody Feed. Retrieved January 18, 2023, from https://goodyfeed.com/pig-butchering-scams/

Tse, N. (2023, January 5). *Crypto scams in Hong Kong and points to note*. Oldham, Li & Nie. Retrieved January 18, 2023, from https://oln-law.com/crypto-scams-in-hong-kong-and-points-to-note/

UNDOC. (2022, April). *Assessing the digital financial threat landscape in Indonesia*. United Nations : UNODC Regional Office for Southeast Asia and the Pacific. Retrieved January 18, 2023, from https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2022/03-assessing-digital-financial-threat-landscape-indonesia.html#:~:text=PPATK%20analysis%20shows%20that%20fraud,to%20approximately%2023%2C000%20in%202021.

Williams, S. (2022, December 17). *Commonwealth tackling rising cybercrime threat in Asia*. TechDay. Retrieved January 17, 2023, from https://securitybrief.asia/story/commonwealth-tackling-rising-cybercrime-threat-in-asia#:~:text=Cybercrime%20represents%20an%20increasing%20threat,issues%20for%20governments%20and%20businesses.

Wong, J. H. (2022, July 6). *Love at the price of cryptocurrency scams*. The Edge Markets. Retrieved January 18, 2023, from https://www.theedgemarkets.com/content/advertise/love-price-cryptocurrency-scams

Wyk, B. van. (2022, August 23). *China's cyber crime problem is growing*. The China Project. Retrieved January 17, 2023, from https://thechinaproject.com/2022/08/23/chinas-cyber-crime-problem-is-growing/

Zou, T. (2023, January 4). *Crypto takes up 70% of online investment scams in Hong Kong*. Forkast. Retrieved January 18, 2023, from https://forkast.news/headlines/crypto-70-online-investment-scams-hong-kong/