Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams

Pengcheng Xia[1], Haoyu Wang[1], Xiapu Luo[2], Lei Wu[3], Yajin Zhou[3], Guangdong Bai[4], Guoai Xu[1], Gang Huang[5], Xuanzhe Liu[5]
[1] Beijing University of Posts and Telecommunications, Beijing, China
[2] The Hong Kong Polytechnic University [3] Zhejiang University
[4] The University of Queensland [5] Peking University

***Abstract*—As COVID-19 has been spreading across the world since early 2020, a growing number of malicious campaigns are capitalizing the topic of COVID-19. COVID-19 themed cryptocurrency scams are increasingly popular during the pandemic. However, these newly emerging scams are poorly understood by our community. In this paper, we present the first measurement study of COVID-19 themed cryptocurrency scams. We first create a comprehensive taxonomy of COVID-19 scams by manually analyzing the existing scams reported by users from online resources. Then, we propose a hybrid approach to perform the investigation by: 1) collecting reported scams in the wild; and 2) detecting undisclosed ones based on information collected from suspicious entities (e.g., domains, tweets, etc). We have collected 195 confirmed COVID-19 cryptocurrency scams in total, including 91 token scams, 19 giveaway scams, 9 blackmail scams, 14 crypto malware scams, 9 Ponzi scheme scams, and 53 donation scams. We then identified over 200 blockchain addresses associated with these scams, which lead to at least 330K US dollars in losses from 6,329 victims. For each type of scams, we further investigated the tricks and social engineering techniques they used. To facilitate future research, we have released all the well-labelled scams to the research community.**

I. Introduction

The coronavirus pandemic (COVID-19) has quickly become a world-wide crisis. Beyond the virus in the physical world, the cyber-space also suffers from the security threats relevant to COVID-19. Recent months have witnessed a surge of malicious campaigns that are exploiting the pandemic, such as email scams, ransomware, phishing domains and malicious apps [1]–[4], etc. According to the report from Federal Trade Commission (FTC), victims in the US have lost over $77 million to fraud during this crisis by the time of July 2020 [5], and the number is just the 'tip of the iceberg', as the fraud was typically under-reported by consumers.

Blockchain, as one of the most popular techniques in recent years, has attracted great attentions from attackers in this pandemic. As more and more businesses accept cryptocurrencies as payments and people have been drawn to cryptocurrencies, more scammers have appeared to take advantage of these eager new targets to steal money. According to an FBI press released on April 2020, the number of scams related to cryptocurrency has increased greatly during the COVID-19 pandemic [6]. For example, some scammers posing as World Health Organization (WHO) sent fake emails asking for Bitcoin donation [7]. They also used a forged email address, "donate@who.int", to defraud people. Also, it is reported that a malicious COVID-19 themed domain `coronavirusapp.site` claims to offer a real-time coronavirus tracking app [8]. However, the app is a new kind of ransomware called "CovidLock" that locks the victim's devices and requests for Bitcoins in 48 hours on the ransom note. Besides, a number of Initial Coin Offering (ICO) and other token scam projects are taking advantage of COVID-19 to release trashy cryptocurrency tokens (e.g., CoronaCoin, COVID19 Coin), to cheat inexperienced investigators [9]. For example, three consecutive *exit scams* happened for the CoronaCoin, which broke the project.

This Work. In this paper, we take the first step to characterize the coronavirus-themed cryptocurrency scams. Our goal is to systematically *summarize and investigate different types of cryptocurrency scams related to COVID-19*, *explain how they work*, *measure their prevalence* and *characterize their impacts*. To this end, we first make efforts to create a taxonomy of COVID-19 themed cryptocurrency scams (see **Section III**). By resorting to security reports of COVID-19 cybersecurity attacks and scam reports obtained from discussion forums, we have summarized a taxonomy of 6 types of scams that take advantage of both COVID-19 and cryptocurrency to infect unsuspecting users. These scams include: 1) COVID-19 token scam, 2) COVID-19 giveaway scam, 3) COVID-19 blackmail scam, 4) crypto malware scam, 5) COVID-19 themed Ponzi scheme, and 6) crypto donation scam. By demystifying these types of scams, we propose a hybrid approach to collect scams in the wild (see **Section IV**), and identify 195 COVID-19 themed cryptocurrency scams in total, which correlate with 201 scam blockchain addresses, 57 scam domains, 14 crypto malware, 47 social accounts and 91 coronavirus-related tokens. We further measure the characteristics and impacts of these scams (see **Section V**). Our investigation shows that at least 330K US dollars have been stolen by the attackers from $6,329$ victims, which is a lower bound estimate of the prevalence and criminal profits associated with these scams.

To the best of our knowledge, this paper takes the first step to reveal the COVID-19 themed cryptocurrency scams with some unexpected and interesting observations. We believe this work shall shed some light on identifying scams related to public events. To boost future research, we have released all the collected COVID-19 cryptocurrency scams to the community at: https://covid19scam.github.io.

II. Background and Related Work

A. Blockchain and Cryptocurrency

Blockchain was invented in 2008 to act as a public, decentralised ledger for Bitcoin. It stores transactions or related events among involved parties. Each transaction in a block is verified by consensus on most of the system's participants, and the data stored in the blockchain cannot be modified. Cryptocurrency is a kind of digital asset that uses cryptography to ensure the security of its creations and transactions. Since the debut of Bitcoin, thousands of cryptocurrencies are emerging [10]. Cryptocurrencies except Bitcoin can be classified into two types: *Altcoins*, which mean alternatives to Bitcoin, and *tokens*, which are unable to operate independently without existing blockchain platforms. Blockchains like Ethereum and EOSIO, have simplified the development of token smart contracts. One can create a token smart contract with just a few lines of code [11]. Recent work [12] suggested that there are over 160,000 tokens exist on Ethereum.

B. Cryptocurrency Scams

More and more attackers target on cryptocurrencies to make a profit. In 2019, cryptocurrency scams caused over $ 4.26 billion in losses [13]. Although users, wallets and exchanges are adopting new countermeasures to avoid being scammed, new scam techniques still emerge to defraud users' money. Vasek and Moore surveyed the presence of Bitcoin-based scams [14] in 2015. By gathering reports from voluntary vigilantes and reports tracked in online forums, they identified 192 scams and categorized them into four groups: *Ponzi schemes*, *mining scams*, *scam wallets* and *fraudulent exchanges*. Most of existing scam studies were focused on detecting the Ponzi schemes [15]–[21], fraudulent Initial Coin Offering (ICO) [22], [23], market manipulation of cryptocurrencies [19], [24]–[27], blockchain honeypots [28], and phishing scams [29], [30], etc. To the best of our knowledge, this paper is the first work to study COVID-19 themed cryptocurrency scams.

C. COVID-19 related Research

Since its outbreak, coronavirus has attracted great attentions from various research communities. A large number of studies were focused on the medical domain, including pathology study, epidemiology study, treatment study and so on [31]–[34]. There are also some sociology or psychological studies on COVID-19 like misinformation research or social impact analysis [35], [36]. Computer scientists have adopted computing techniques like machine learning to help medical practitioners deal with COVID-19. Zhang et al. [37] proposed the confidence-aware anomaly detection (CAAD) model to screen viral pneumonia on chest X-ray images. Wang et al. [38] proposed COVID-Net, a deep convolutional neural network design tailored for the detection of COVID-19 cases from chest X-ray (CXR) images.

At the same time, however, cyber attackers also exploit this situation to conduct criminal activities [3], [39]–[43]. Lallie et al. [39] analyzed the timeline of COVID-19 themedcyber-attacks. They utilised the UK as a case study to demonstrate how cyber-criminals leveraged key events and governmental announcements to carefully craft and design attacks. Ahmad et al. [43] analyzed the security challenges on the work-from-home model and proposed some recommendations on how to avoid being attacked by phishing websites or emails. He et al. [3] presented a systematic analysis of coronavirus-themed malware and found that over 53% of the malicious apps they collected were camouflaged as official apps. They also found that these apps aim to steal users' private information or to make profit by phishing and extortion. Sun et al. [44] analyzed the security and privacy issues of COVID-19 contact tracing apps. Although a few previous studies mentioned COVID-19 themed scams, there lacks a systematic study on COVID-19 themed cryptocurrency scams, such as the impact and popularity of these scams.

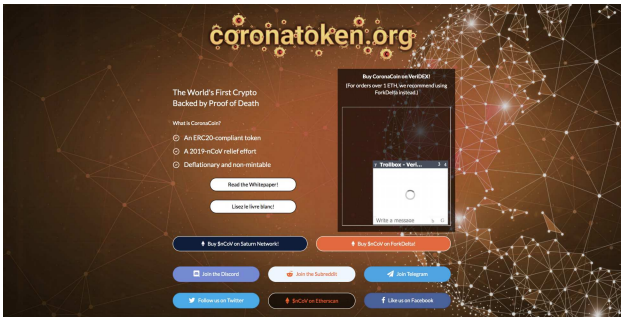


Fig. 1. Screenshot of *coronatoken.org* (the official website of CoronaCoin).

III. A Taxonomy of COVID-19 Crypto Scams

To understand the prevalence and characteristics of COVID-19 themed crypto scams in the wild, we first create a comprehensive taxonomy by manually analyzing the existing scam reports. We will explain how each kind of scams works in this section. Based on this taxonomy, we will further measure their popularity and impacts in Section IV and Section V.

Creating the Taxonomy. We resort to the following information to create the taxonomy: 1) security reports of COVID-19 cybersecurity attacks released by security companies (e.g., DomainTools [45] and McAfee [46]), 2) over 40 scam reports obtained from scam accusations on Bitcointalk [47] and BitcoinAbuse [48], 3) COVID-19 themed scams summarized by the Federal Trade Commission (FTC) [49], 4) COVID-19 scams reported in the threat intelligence platforms (e.g., AlienVault [50] and COVID-19 MISP [51]), and 5) the related information by searching keywords like 'COVID-19 attack' and 'COVID-19 scam' on Google. We summarize a taxonomy of 6 types of scams related to COVID-19, as shown in Table I. We will detail these scams in the following subsections.

A. COVID-19 Token Scam

A number of Initial Coin Offering (ICO) projects and scam token projects take advantage of COVID-19 to release trashy cryptocurrency tokens to cheat inexperienced investigators. In

TABLE I
A TAXONOMY OF 6 KINDS OF COVID-19 CRYPTOCURRENCY SCAMS.

Type of Scams	Tricks	Scam Entities	Example
COVID-19 token scam	Issuing new tokens that claim to be used for charity; "Pump-and-dump" schemes	Token	CoronaCoin (0x10Ef64cb79Fd4d75d4Aa7e8502d95C42124e434b)
COVID-19 giveaway scam	Promising to reward users based on the money they sent.	Social Network Domain	https://gatesbtc.live
COVID-19 themed Blackmail	Threatening to spread coronavirus if not receive cryptos, or selling products/cures for COVID-19.	Email	abtconsultnl@oceanenergy.ch
Crypto Malware	Locking victims' phones or computers and asking for cryptos	Software	https://coronavirusapp.site
Ponzi Schemes	Claiming to return high interest payback if someone invest with cryptos	Domain, Social Network	https://coronainvest.io
Donation Scams	Acting as public organizations and claiming to raise money for COVID-19	Domain, Social Network	https://covid-coin.com

addition to claiming to help people alleviate the pain of virus and lockdown, the founding teams of some tokens also indicate that they will participate in public welfare activities and donate part of the profit of the tokens to charitable organizations. Moreover, many tokens can be traded on some decentralized cryptocurrency exchanges (DEX) and their promotion tricks make investors believe these tokens are profitable. However, some tokens are totally scams since the very beginning, and the founders would just disappear with the investments they received from the ICO projects. Some token projects may first run normally after issuing the tokens, but the project owners who possess most of the tokens will monetize their tokens when the price increases. This type of scams is also known as the "Pump-and-dump Scheme" [52], which has been studied extensively by many researchers [19], [26].

Figure 1 shows the official webpage of the CoronaCoin[1] (Token symbol: NCOV), which is claimed to be the first token related to COVID-19. It has received more and more attention since reported by medias like Reuters, Nasdaq and New York Times [53]. It is designed to be burned per 48 hours according to the number of infections and casualties from the Coronavirus. The founding team calls this mechanism "proof of death". It is advertised that by this way, the token will be deflationary and its value will increase. Although they donated about $235 on March 6th to the Red Cross for the first time, which seems to prove they operated this project with a good will, three consecutive *exit scams* happened afterwards. The CoronaCoin's developers and administrators monetized the large amount of tokens they managed based on the "Pump-and-dump Schemes". These scams broke the project, leading to its current failure. From the scam accusation reports on BitcoinTalk [54], many investors have found that this token was a scam at the very beginning and they condemn the behaviors of designing scams by exploiting the pandemic, but there are still many unsuspecting investors who were deceived.

B. COVID-19 Giveaway Scam

Giveaway scam is a type of commonly used trick in the field of cryptocurrency scam, and it is no exception when it comes to the COVID-19 themed scams. The malicious actors promise to reward users based on the money (tokens) that the users send, but they will not fulfill their promises in the end. The giveaway scam can be delivered using both social network (e.g., Twitter) and content sharing services (e.g., YouTube).

Figure 2(a) shows an example of giveaway scam reported on BitcoinAbuse. This YouTube video shows Bill Gates' speech about Bitcoin and pandemic investment, which inserts a giveaway scam Bitcoin address 1Gatesk17u25gLEk4JNYMDTg8WkCmLpn47. It asks users to send Bitcoins to this address so that they will gain a double payback. It is interesting to see that there is a "Gates" in the address, which may increase the credibility of the scam.

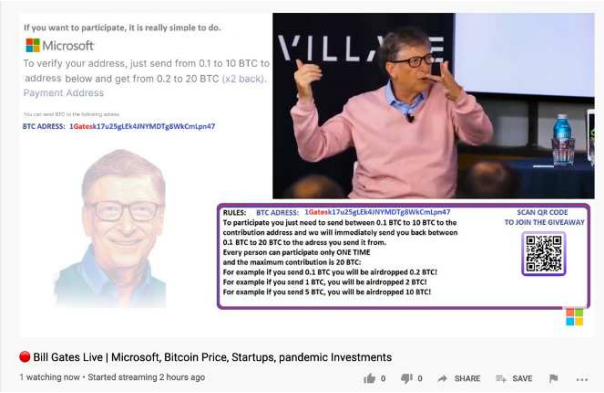
Giveaway scams are also prevalent on social network. Note that, our investigation reveals that the scams can be distributed by either the *scam social network accounts* or the *hacked accounts*. For the scam social network accounts, they are usually fake accounts that act as the famous people. For example, there are many fake accounts that have the same name, avatar and other information with Vitalik Buterin (one of the co-founders of Ethereum). In this way, they can post giveaway scam tweets to cheat unsuspecting users. For the hacked accounts, one of the largest campaigns is the Twitter's massive attack on July 15th, 2020 [55]. The twitter accounts of major companies and individuals were compromised and these accounts were controlled to conduct a COVID-19 themed giveaway scam. Figure 2(b) shows one of the scam tweets. The attackers used Warren Buffett's account to ask for sending Bitcoins to their addresses and promised to return a double payback. Till July 16th, the scam address bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh has received 12.02 BTC (about 110K US dollars[2]).

C. COVID-19 themed Blackmail

The cryptocurrency-related extortion emails are mainly focused on sextortion, according to previous work [56]. During this pandemic, attackers have adopted some other social engineering techniques for extortion. For example, attackers can ask for money by threatening that they are able to infect the emails' receivers with coronavirus. There are also some scam emails claiming that they have a cure for coronavirus.

[1]Ethereum address: 0x10Ef64cb79Fd4d75d4Aa7e8502d95C42124e434b

[2]As the prices fluctuate all the time, we estimate the prices of cryptocurrencies based on their closing prices on July 16th (the same below).



(a) A YouTube video that promotes *http://gatesbtc.live* (a domain involved in COVID-19 themed giveaway scams).

(b) A tweet posted by the hacked Twitter account *Warren Buffett*.

Fig. 2. Two examples of COVID-19 themed giveaway scams.

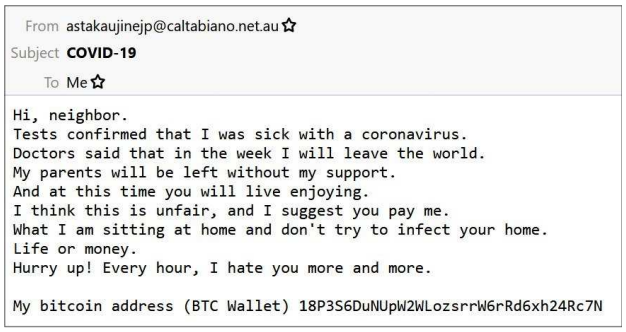


Fig. 3. An example of a COVID-19 crypto extortion email.

Figure 3 shows an example of a COVID-19 themed crypto extortion email. The attacker claims to be the victim's neighbour that was infected with COVID-19. He asks the receiver to send Bitcoins to 18P3S6DuNUpW2WLozsrrW6rRd6xh24Rc7N, otherwise he will spread the virus. This address has been reported 15 times on BitcoinAbuse by the time of this study. Fortunately, it only receives 0.06 US dollars in total. We will further discuss the social engineering techniques used in these scams and their impacts in Section V.

D. COVID-19 Crypto Malware

Ransomware is a type of crypto malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. Ransomware is quite popular in recent years, which has been widely studied by both cybersecurity industry and academia [57]–[59]. Ransomware attack is typically carried out using a Trojan that is disguised as a legitimate application. COVID-19 has been invoked for malicious purposes by the ransomware creators. They usually impersonate COVID-19 themed apps to trick users into installing them. Once launched, it will encrypt the victim's mobile phone files or force a lock screen and extort a high ransom. Besides, there are also other crypto malware like crypto miners in the wild.

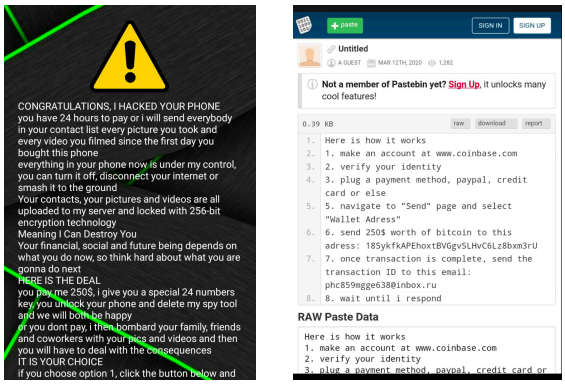


Fig. 4. An example of a COVID-19 themed ransomware.

Figure 4 shows an example of a mobile ransomware[3], which was distributed on a malicious COVID-19 themed domain *http://coronavirusapp.site*. Once launched, the malware will lock user's phone and ask for Bitcoins. Clicking the button on the screen will redirect users to a Pastebin link (https://pastebin.com/GK8qrfaC) where records the attacker's Bitcoin address *18SykfkAPEhoxtBVGgvSLHvC6Lz8bxm3rU*.

E. Covid-19 themed Ponzi scheme

Ponzi scheme is a kind of scam promising high rates of return with little risk to investors [60]. In fact, the attackers will only pay back the early investors using the money that the subsequent investors deposit, and they will finally take all the money they get and leave. Lots of studies were focused on this kind of scam, both on normal blockchain Ponzi schemes [17] and Ponzi schemes built on smart contracts [15], [16]. Malicious actors also exploit the pandemic to carry out Ponzi schemes, claiming to help people reduce economic pressure of income fluctuations during quarantine.

Figure 5 shows an example of a Ponzi scheme domain. The attackers claimed that they will invest in coronavirus' vaccine and give stable and high return to the investors. With such a promise, the website did not survive for a long time. According to Wayback Machine[4], the website can be accessed earlier than March 15th and it was shut down by the time of March 29th.

F. Fake Crypto Donation

Besides some traditional scams on cryptocurrency, we also identify a number of coronavirus-themed crypto donation scams spread via emails, social network and websites. Attackers may act as some health-related official organizations or

[3]MD5:d1d417235616e4a05096319bb4875f57
[4]http://web.archive.org/web/20200315040815/https://coronainvest.io/

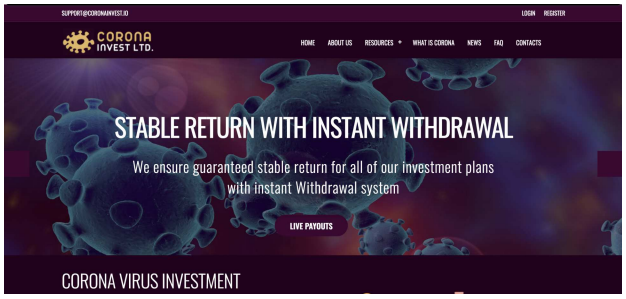


Fig. 5. Screenshot of *http://coronainvest.io* (a Ponzi scheme domain.)

Fig. 6. Screenshot of *http://covid-coin.com/* (a donation scam domain).

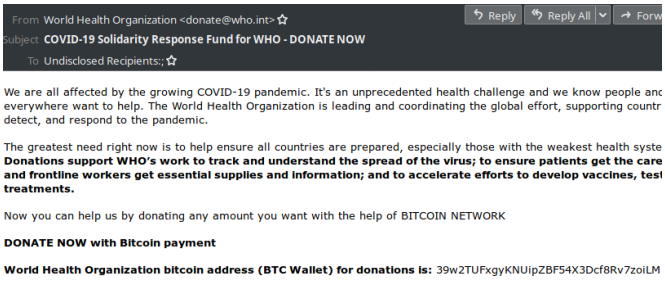


Fig. 7. Screenshot of an Email sent from "donate@who.int" (donation scam).

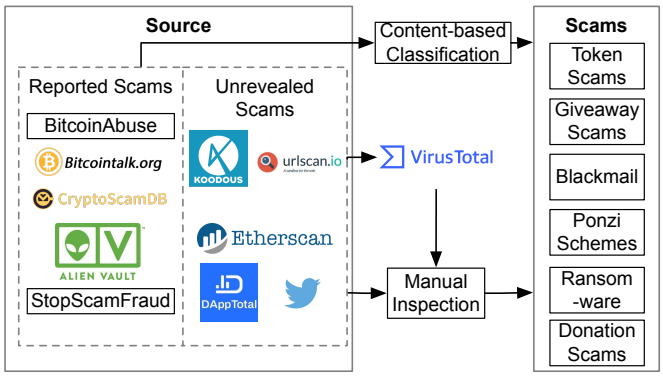


Fig. 8. Our approach to collecting COVID-19 themed cryptocurrency scams.

departments like Centers for Disease Control and Prevention (CDC), World Health Organization (WHO) and the United Nations International Children's Fund (UNICEF). Moreover, some of them act as a charity group or individual to ask for help during this pandemic. In general, they will ask people to send money to their cryptocurrency wallet addresses in the name of donation.

Figure 6 shows a fake donation domain, which was flagged as malicious by VirusTotal. The attackers call for the cryptocurrency community to fight against the virus by donating to them. The domain is built on top of WordPress, which supports donations from 7 kinds of cryptocurrencies. As another example, Figure 7 shows a donation scam in which the attacker pretended to be WHO (using the email address "donate@who.int"). Its sole purpose is to ask for donations to COVID-19 Solidarity Response Fund.

IV. Collecting COVID-19 Themed Crypto Scams

In order to fully understand the prevalence of COVID-19 scams in the wild, we have adopted a hybrid approach to conduct the investigation by: 1) collecting reported scams in the wild; and 2) detecting undisclosed ones based on information collected from various sources. Figure 8 shows the overall procedure of our approach.

A. Harvesting Reported Scams

Based on the taxonomy of COVID-19 scams summarized in Section III, we resort to the following scam databases for collecting known ones reported by users.

1) BitcoinAbuse. BitcoinAbuse [48] is a database where users can report malicious or scam Bitcoin addresses they encountered. By the time of this study, BitcoinAbuse has aggregated more than 170K Bitcoin addresses, which are mainly used in ransomware, blackmails, and giveaway scams. To identify the COVID-19 themed scams, we use keywords like "COVID" or "Corona" to fetch related scam reports. Through this, 31 COVID-19 themed scam Bitcoin addresses are identified from BitcoinAbuse. Based on the tags and descriptions provided by users, we manually classify them into 17 donation scams, 9 blackmail scams, and 5 giveaway scams.

2) CryptoScamDB. CryptoScamDB [61] aims at collecting malicious cryptocurrency domains and related blockchain addresses using a crowd-sourcing based method. By the time of this study, there are over 7,700 malicious cryptocurrency domains collected by CryptoScamDB. To identify COVID-19 related scams, we use the heuristics to search keywords like "COVID" or "corona" in both the domain names and the labels provided by CryptoScamDB. However, we did not find any scams related to COVID-19 from CryptoScamDB.

3) BitcoinTalk. BitcoinTalk [47] is an online forum devoted to the discussion of Bitcoin and other cryptocurrencies. It hosts a "Scam Accusations" board for people to report scams. Thus, we have implemented a crawler to get all the related posts, and then identify scams related to COVID-19 using keywords matching. Finally, we get 9 related posts. We then manually analyzed the archived pages and corresponding user reports to label them. At last, we have identified 4 token scams, 2 Ponzi schemes, 2 ransomware and 1 donation scam from these posts.

4) Threat Intelligence Platforms. Threat intelligence platforms like AlienVault [50] and some security companies like McAfee provide reports related to coronavirus-themed attacks.

These reports often contain indicators of compromise (IoCs), which can reflect attackers' intentions to a certain extent. We use a crawler to fetch all the reports and identify 9 COVID-19 cryptocurrency scam reports (with 11 blockchain addresses). Based on the detailed descriptions provided by these reports, we have categorized them into 4 donation scams, 5 crypto ransomware and 2 giveaway scams.

5) StopScamFraud. StopScamFraud [62] is a platform devoted to collecting users' reports on scam emails. By the time of this study, there are over 900 mail accusations related to COVID-19. As we only consider cryptocurrency related scams, we search the scams using blockchain related keywords (e.g., Bitcoin, Ethereum, etc.). However, we do not find any related scam accusations.

B. Detecting Unrevealed Scams

To further identify unrevealed COVID-19 themed cryptocurrency scams in the wild, we first perform a semi-automated analysis to identify suspicious scam entities, and then manually verify them. As summarized in Table I, the scams can be delivered via entities including tokens, domain, malware, smart contract (DApp), email, and social network. Thus, our goal is to first identify the scam entities related to COVID-19.

1) Scam Tokens. Etherscan [63] is an Ethereum blockchain explorer that tracks tokens on Ethereum. We resort to Etherscan to search for COVID-19 themed ERC-20 and ERC-721 tokens[5] using keywords like "corona" and "COVID-19". By the time of our study, we have identified 87 tokens that target the pandemic. To verify whether they are indeed scams, on one hand, we search these tokens (with their corresponding addresses) in Google to check whether they have related websites, social accounts or scam reports. On the other hand, we manually analyzed all their smart contracts, to see if they use simple ERC-20 or ERC-721 code templates without additional functions. Based on our manually verification, we believe all of them are trashy tokens without any value. COVID-19 is only used as the publicity stunt to cheat unsuspecting users.

2) Scam Domains. We seek to identify the malicious domains related to COVID-19 first, and then try to detect whether some of them belong to the scams we summarized. Here, we take advantage of URLScan [64], an online service that provides history snapshots, IP resolutions and other detailed information of massive domains. We use a number of keywords including "coronavirus", "COVID-19" and their squatting ones (e.g., cor'a'navirus, cor'oo'navirus)[6] to identify the domain names that contain the keywords from URLScan. Combining with COVID-19 themed domains fed by RiskIQ [67], we have identified $175,966$ newly registered domains that contain COVID-19 related keywords since January 2020.

Note that, the COVID-19 themed domains reported by these threat intelligence platforms are not necessary to be malicious, as some of them were found via newly registered domain feeds, which never served any malicious activities. Thus, we further take advantage of VirusTotal [68], a widely-used online service that aggregates over 60 anti-virus engines, to check whether the COVID-19 domains are malicious. At last, we identify $101,004$ COVID-19 domains flagged as malicious by at least one anti-virus engine on VirusTotal. For the malicious domains, after excluding the domain parking web pages, we use a heuristic approach to identify and classify the cryptocurrency related scams. Since domains that contain words like "crypto", "bitcoin", "invest", "donation" tend to carry out coronavirus-themed cryptocurrency scams, we select such domains that contain keywords in their domain names, as the scam candidates (over 150 domains found). Then, we perform a manually inspection to determine whether they are cryptocurrency scams. For example, if a malicious domain claims that it will give high excess returns to the investors (i.e., high-yield investment program), we will label it as a Ponzi scheme. If a malicious domain camouflages as reputable organizations to ask for donation, we will label it as a donation scam. If a domain claims to reward users based on the cryptocurrency that they transferred, we will label the domain as a giveaway scam and further label its corresponding blockchain address as a scam address. At last, we have manually verified 7 Ponzi schemes, 2 donation scams, and 2 giveaway scams in this way.

3) Malware. To identify the COVID-19 themed crytocurrency malware, we rely on two data sources. On one hand, for the aforementioned $101,004$ COVID-19 domains flagged as malicious, we use a premium API provided by ViusTotal to get files related to these malicious domains, i.e., files that communicate to these domains or files that are downloaded from these domains. After this step, we have collected $7,294$ binaries and $2,362$ of them are flagged as malicious by at least one engine on VirusTotal. On the other hand, we use Koodous [69], a large Android app repository with over 62 million apps in total by the time of this work, to find suspicious COVID-19 themed malware. Koodous contains historical apps from various sources. In this work, we collect the apps whose app names or package names contain COVID-19 related keywords. In this way, $2,378$ apps are collected. For all the collected binaries, we further use VirusTotal and AVClass [70] for labelling their malware families. Note that, not all the samples can be assigned families, as AVClass needs a number of AV engines' detection results to achieve an agreement on family name. As we only consider COVID-19 themed ransomware and cryptomining malware in this work, all the malware whose families are labelled "Ransomware", "Locker" or "Coinminer" are kept to the further research. Thus, 4 COVID-19 ransomware and 5 COVID-19 cryptomining malware are identified. All of them were labelled by at least 6 anti-virus engines, and 5 of them were flagged by at least 30 anti-virus engines.

4) Scam Social Network Posts/Accounts. Social network is one of the major channels for distributing and advertising COVID-19 themed scams. Thus, we resort to Twitter and

[5]ERC-20 and ERC-721 are both token standards in Ethereum. ERC is a set of rules that the developers have to follow so they can implement a token in the Ethereum blockchain ecosystem. It includes information about the protocol specifications and the description of the contract.

[6]Previous work suggested that typosquatting [65] and combosquatting [66] attacks are prevalent in malicious domains.

TABLE II
THE DISTRIBUTION OF SCAMS HARVESTED FROM DIFFERENT SOURCES.

Type of Scams	Total Found	Reported Scams	Unrevealed Scams	Related Tokens	Related Domains	Related Binaries	Related Social Accounts	Extracted Addresses
Token Scams	91	4	87	91	14	0	7	91
Giveaway Scams	19	7	12	0	5	0	10	21
Blackmails	9	9	0	0	0	0	0	9
Crypto Malware	14	5	9	0	6	14	0	4
Ponzi Schemes	9	2	7	0	9	0	0	0
Donation Scams	53	21	32	0	23	0	30	76
Total	**195**	**48**	**147**	**91**	**57**	**14**	**47**	**201**

Telegram to identify more scams. To be specific, we first identify Tweets and Telegram discussions that contain both the COVID-19 keywords and cryptocurrency keywords. Then, we manually inspect their contents. For example, if we find a Twitter account that imitates an official account of reputable organizations to publish donation information, we will flag it as a donation scam. If we identify Tweets that advertise giveaway information, we will mark it as a giveaway scam. We have analyzed all the related Tweets and Telegram discussions from January 2020 to July 2020, and identified 30 donation scams and 10 giveaway scams, which were distributed by 37 Twitter accounts and 3 Telegram accounts.

5) Scam Smart Contracts (DApps). Previous work [16], [19] suggested that some DApps (smart contracts) are actually Ponzi schemes. To verify whether the Ponzi DApps take advantage of COVID-19, we resort to DAppTotal [71], a well-known DApp explorer to find whether there are coronavirus-themed DApps. However, our keywords searching does not find any DApps related to COVID-19.

Note that, as we cannot get unrevealed email scams from public information, we did not identify any new scam emails besides the reported ones. For all the detected scams, we further analyze them using a semi-automated approach to identify their correlated blockchain addresses (if available). To be specific, we first use regular expressions[7] to identify blockchain address candidates, and then we manually verify whether they are real addresses.

C. Dataset Overview

Table II shows the statistics of scams we collected. **Overall, we have identified 195 COVID-19 cryptocurrency scams**, including 91 token scams, 19 giveaway scams, 9 blackmails, 14 crypto malware, 9 Ponzi schemes and 53 donation scams. These scams correspond to 91 COVID-19 tokens, 57 malicious COVID-19 domains, 14 COVID-19 themed malware, and 47 social accounts on Twitter and Telegram. Besides, we have identified 201 blockchain addresses correlated with them.

V. MEASUREMENT OF COVID-19 CRYPTO SCAMS

In this section, we analyze the overall trends of COVID-19 crypto scams, investigate the tricks and social engineering techniques used in scams, and further measure the impacts.

[7]For example, the regular expressions (bc1—[13])[a-zA-HJ-NP-Z0-9]25,39 is used to identify Bitcoin address.

A. The Trends of COVID-19 Cryptocurrency Scams

1) Distribution of Scams: The distribution of scams is shown in Table III. Obviously, the *token scams* (46%) and *donation scams* (27%) are dominant in the ecosystem. There might be two reasons. First, cryptocurrencies are claimed to be the *Safe Haven Asset* (compared with the fiat currency). Thus, during the pandemic, attackers have the motivation to use COVID-19 token scams to cheat inexperienced users. Second, most people want to help fight the pandemic, so the scammers take advantage of this opportunity to act as the official agencies (e.g., WHO) to advertise a number of donation scams.

2) Overall Impacts of Scams: We further estimate the overall impacts of scams. It is non-trivial to estimate the impacts, as we can only resort to the blockchain transactions related to these scam addresses, which is a lower-bound estimation. We have collected all the transaction records related to these scam addresses till July 16th 2020. Since a few scam addresses have been active for a long time before 2020, we only consider the transactions related to these scam addresses since the beginning of the pandemic (early 2020) when calculating the overall financial losses of scams. Note that token scam is a special case. Here, we only consider the holders who have the corresponding COVID-19 trashy tokens. As there are 91 scam tokens, we estimate their prices based on the latest value shown in exchanges. For the tokens we cannot get their latest value from exchanges (which means that they have no trade records on exchanges), we do not count their value. Thus, *our estimation is definitely a lower bound of the COVID-19 cryptocurrency scam ecosystem*.

As shown in Table III (column 4 and column 5), the overall number of financial losses is over 333K US dollars, contributed by $6,329$ victims. *Giveaway scam* is the most profitable category (over \$287K), with over 500 victims were scammed. Besides, at least \$21K contributed by 103 victims were received by *donation scams*, and the volume of *token scams* is over \$23K. We will further investigate each scam category in the following subsections.

3) The Distribution of Scam Blockchain Addresses: Table IV shows the distribution of the 201 scam addresses[8]. It can be observed that, Bitcoin addresses dominate the scams

[8]Note that we list token scams' addresses separately, because these scams are based on comprehensive designs like "Pump-and-dump" schemes and these addresses can not be simply measured with transactions on addresses.

TABLE III
THE DISTRIBUTION OF 6 TYPES OF SCAMS.

Category	# of Scam Cases	# of Addresses	Est. Victims	Est. Scammed Money ($)
Token Scams	91	91	5,701	23,178.0
Giveaway Scams	19	21	516	287,663.5
Donation Scams	53	76	103	21,788.9
Blackmails	9	9	6	514.5
Ransomware	14	4	3	102.1
Ponzi Schemes	9	0	0	0
Total	**195**	**201**	**6,329**	**333,247.0**

TABLE IV
THE 8 TYPES OF CRYPTOCURRENCY ADDRESSES IN THE DATASET.

Coin or Token	# of Addresses (# of Addresses Active in 2020)	Incoming Transactions in 2020	Total Received in 2020	Current Value($)
BTC	81 (38)	550	33.2	303,100.5
ETH	18 (6)	73	13.7	3,218.2
BCH	5 (0)	0	0.0	0.0
LTC	2 (1)	1	2.0	84.1
TRX	1 (1)	2	211,254.3	3,621.7
USDT	1 (1)	1	44.5	44.5
DOGE	1 (0)	0	0.0	0.0
XRP	1 (0)	0	0.0	0.0
Scam Tokens	91 (91)	-	-	23,178.0
Total	**201 (138)**	**627**	**-**	**333,247.0**

(40.3%), followed by Ethereum with 18 addresses. Among these scam addresses, 138 of them have transactions in 2020.

The Evolution of Scam Addresses. We further analyze the evolution of all the 151 scam addresses that ever have transaction records (including 13 addresses only received transactions before 2020), as shown in Figure 9. It is interesting to see that, there are 20 addresses in total that were active before 2020. We manually analyzed the 20 addresses, and observed that 2 of them were involved in known scams in 2018 and 2019, respectively. For the remaining 18 scam addresses, 17 of them were COVID-19 donations scams. However, we did not identify any obvious scam activities of them before this pandemic. Thus, it is quite possible that they were ordinary addresses before, which were then used in scams during COVID-19. Most of the scam addresses (86.8%) are active after 2020. *It is obvious that, there is a sharp increase in March and April 2020, which is inline with the time of the global outbreak of COVID-19*. Among these 131 addresses that are new emerging in 2020, the first address that succeeded in receiving crypocurrencies is 0x4e4f4153C6DA6c6df6ecA1f3BF367E5461Ad8F88, which was a giveaway scam that extracted from a Telegram account "Help_covid19funds". It received 0.1 ETH on 7th February and has received 6.5 ETH (about $1518.7) in total.

The Distribution of Transactions. The distribution of the scam addresses' incoming transactions is shown in Figure 10. For the amount of financial losses, most of them are small transactions, i.e., *over 90% of the transactions are below* $1,000$ *US dollars and 67.6% of the transactions are below 100 US dollars*. The largest transaction happened on July 15th, when the address[9] associated with the Twitter hack

[9]bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

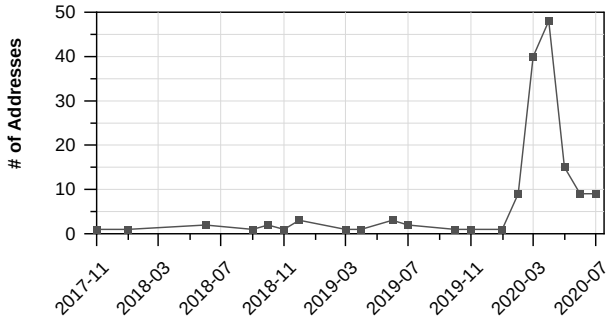


Fig. 9. The distribution of the first transaction time of scam addresses.

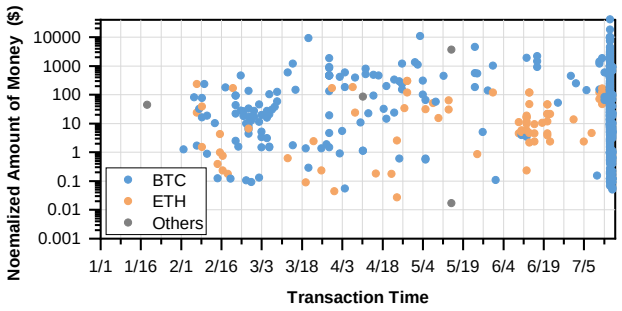


Fig. 10. The distribution of the time when these scam addresses first received cryptocurrencies. Some scam addresses were active before this pandemic.

event received 4.56 BTC (roughly $41,642$ US dollars). As to the transaction time, first transaction to the scam address happened on January 19th, 2020, and the donation scam address 0x376624e29f8c52b0181bdd794c76fd1058963334 received 44.5 USDT. The Twitter hack campaign on July 15th accounts for over half of incoming transactions in our dataset, suggesting its great impact on the blockchain community.

The Most Profitable Addresses. On average, each active scam address has received 13.3 transactions. The most active address bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh has received 321 transactions. We further analyze the distribution of money each scam address received, as shown in Figure 11. It can be observed that over 61.7% of the active addresses have received less than $\$1,000$ equivalent cryptocurrencies. Table V shows the top-5 most profitable addresses in our dataset. Notably, three of them belong to the Twitter hack related addresses. The largest one has received 14.75 Bitcoins, which is equivalent to roughly $\$134,781.2$.

The Relationship among Scam Addresses. Furthermore, we attempt to investigate relations among scam addresses, i.e., *whether they are controlled by the same malicious campaigns*. For addresses that have ever received transactions on Bitcoin and Ethereum, we analyze their relationship based on the *money flow*, i.e., transactions from one address to another. Figure 12 shows the relationship between scam addresses. There are 3 types of addresses in the graph: 1) the labelled *scam addresses* (we exclude silent scam address that have no transaction records); 2) the *victim addresses*, which have ever transferred money to scam addresses but did not receive money from them; and 3) the *fund transfer addresses*, which are

TABLE V
THE TOP 5 PROFITABLE ADDRESSES IN THE DATASET.

Address	Description	Scam Category	# of Incoming Transactons	# of Cryptos Received	Est. Value ($)
1Ai52Uw6usjhpcDrwSmkUvjuqLpcznUuyF	A Twitter hack address	Giveaway Scams	39	14.75BTC	134,781.2
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh	A Twitter hack address	Giveaway Scams	321	12.02BTC	109,799.9
182P8T7MM9assMo7V9YpqZ925yJX8HZurL	A campaign posing as Bill Gates' fundatoin	Giveaway Scams	23	1.4BTC	12,838.2
142pEjfSBh8cnvE7BMJXMjoSBedJWvRKAG	A campaign reported by Spam404	Donation Scams	1	1.0BTC	9,132.2
1cv4tEUqUY7PciJaJWzFCxRuK75veTQNS	A Twitter hack account	Giveaway Scams	6	0.7BTC	6,440.2

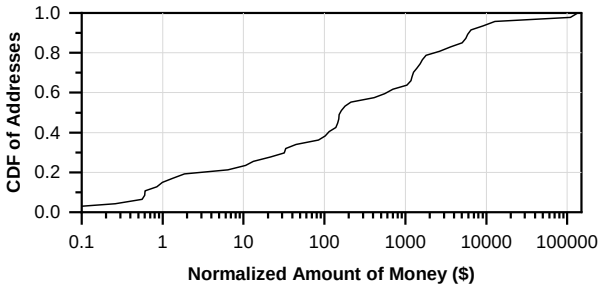


Fig. 11. The normalized amount of money distribution of BTC and ETH addresses' transactions.

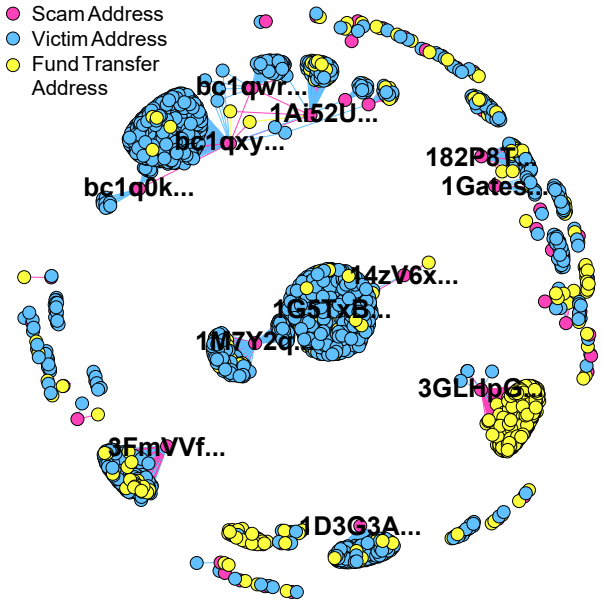


Fig. 12. The relationship between scam addresses.

served as the *money laundering channels*, i.e., receive money from scam addresses and help the attackers transfer the money they have scammed.

There are 56 scam addresses, 1,741 victim addresses and 600 fund transfer addresses shown on Figure 12. On average, each BTC scam address is connected to 37.1 victim addresses and each ETH scam address is connected to 6.5 victim addresses. *Interestingly, some scam addresses are clustered into the same group.* Here, we perform the connected component analysis. As long as there are paths between two scam addresses, we will cluster them together. Note that, we have excluded the

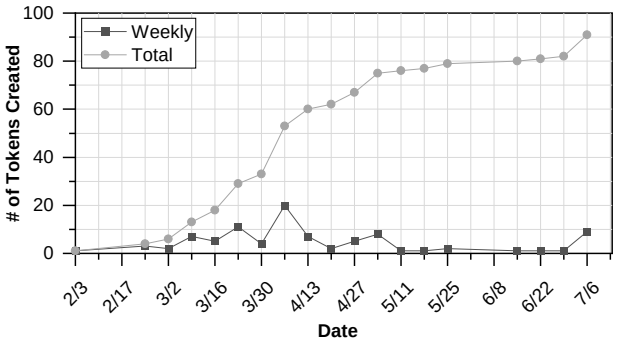


Fig. 13. Creation time of COVID-19 themed scam tokens.

impacts introduced by exchange addresses, as different scam addresses can exploit the same exchange address for money laundering. As a result, 9 scam addresses are clustered into 3 clusters. For example, the address cluster centred on address bc1qwr30ddc04zqp878c0evdrqfx564mmf0dy2w39l is the Twitter hack address group. They have connected to 533 victim addresses and 38 transfer addresses. Most of the money they received was finally transferred to 1Ai52Uw6usjhpcDrwSmkUvjuqLpcznUuyF, another scam address in the group, and was then transferred to multiple addresses for money laundering. We also find a new scam campaign based the relationship of the addresses. They are 182P8T7MM9assMo7V9YpqZ925yJX8HZurL and 1Gatesk17u25gLEk4JNYMDTg8WkCmLpn47, which are connected by 2 fund transfer addresses. It is interesting to see that they both carried out giveaway scams and used similar domain names (`gatesbtc.live` and `gatesmicrosoft.tech`) that impersonated as Bill Gates' foundation.

B. COVID-19 Token Scam

1) The Evolution of Tokens: There are 91 COVID-19 scam tokens in our dataset. The distribution of their creation time is shown in Figure 13. After 2 test tokens created, the first CoronaCoin[10] was officially released on 4th February 2020, and a large number of tokens are created after that. Notably, when the coronavirus raised global concern in March, there are 31 (34.1%) newly emerging tokens created.

2) Current Status of Tokens: The number of token's holders and transfers can reflect the activity of a token to a certain extent. Figure 14 shows the current[11] status of these tokens. 84.62% of the tokens have less than 60 transfers and 86.81%

[10]Address:0x10Ef64cb79Fd4d75d4Aa7e8502d95C42124e434b

[11]We crawled the data until block 10,473,613, i.e. UTC 2020-07-16 11:59:59 PM.

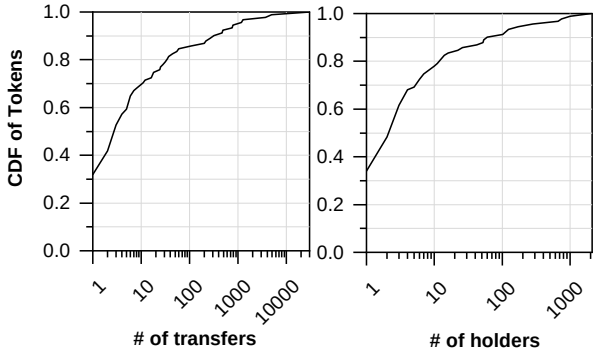


Fig. 14. The number of holders and transfers of scam tokens.

TABLE VI
TOP 5 TOKENS WITH THE MOST NUMBER OF HOLDERS.

Token Name	Token Address	# of Holders	# of Transfers	Online Date
CoronaCoin #1	0x10Ef64cb79Fd4d75d4Aa7e8502d95C42124e434b	2016	29896	Feb 4th
CoronaCoin #3	0x0c2c5E2b677dEa43025B5DA5061fEcE445f0295B	998	3666	Apr 3rd
CoronaCoin #2	0xb80112E516DAbcaC6Ab4665f1BD650996403156C	740	4906	Mar 30th
COVID19	0x26ADdc98fF2321A91a776E52be171a963720A42C	659	1270	Apr 2nd
Corona Coin	0x170467C28C4BF99f2D3840E730498F730a526Da2	281	320	Apr 5th

of the tokens have less than 50 holders, indicating that most scam tokens do not infect too many victims. Among them, 5 tokens have more than 200 holders (see Table VI). Note that, the first 3 tokens have the same name 'CoronaCoin', we add the suffix based on their online time to distinguish them.

3) Price and Volume: Among these tokens, several tokens are listed on some decentralised cryptocurrency exchanges (DEX), so that we can fetch the daily price and volume of them. We choose the price and volume from Saturn Network Exchange[12] because most available tokens (16) are listed there. Their daily average volume is shown on Figure 16[13]. Figure 15 shows the daily closing price of top 3 tokens that have the most average volume. The highest price 0.001 ETH of CoronaCoin #1 occurred on Feb 11th, but considering its normal volume that day, we believe it is just a single case that the transaction is likely to be initiated by the founders of CoronaCoin #1. Their sole purpose is to increase the price of this token. After that, the price of CoronaCoin #1 rises due to increasing attention. On March 4th, a developer of the founding team made an exit scam by dumping all the tokens he had, which makes the price decreased sharply. The CoronaCoin #2 and #3 both created as forks of their former version because of exit scams, and that is why the price curve of CoronaCoin #1 and #2 dropped rapidly in late March and early April.

4) ICO Scam and Exit Scam: By manually investigation, we found 7 out of the 91 scam tokens have behaviors like *ICO scam* and *exit scam*. For the CoronaCoin #1, it has two evident exit scams. One is on March 4th, when a developer dumped 5 million tokens from the developers' wallet, which profited him 14.94 ETH ($\$3,490.6$)[14]. On March 30th, the lead developer

[12]https://www.saturn.network/

[13]Note that due to space limitation, we only list the top-12 tokens based on their volumes.

[14]The actor's address:0x1865E7b66c3996Bd55e7dD88a16B897f4123D2A7

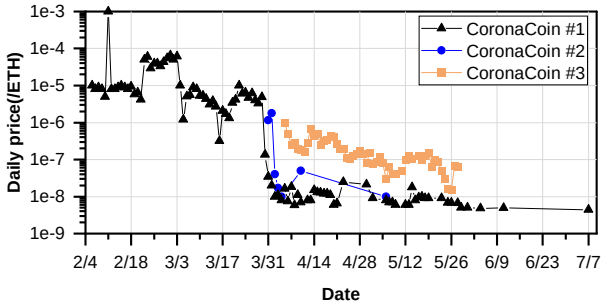


Fig. 15. Daily closing price of the top 3 tokens ranked by average volume.

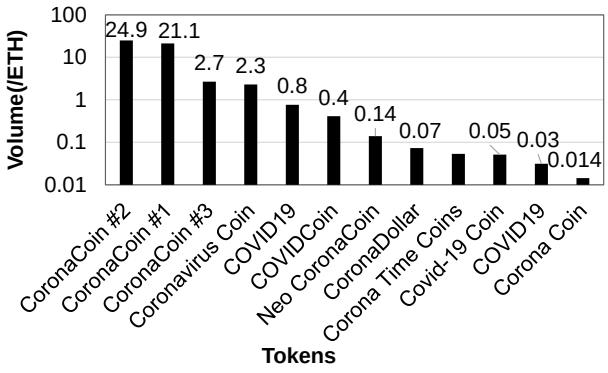


Fig. 16. Daily average volume of tokens on Saturn Network.

compromised the wallet[15] that originally intended to donate to the Red Cross, and he got 63.43 ETH (about $\$14,819.8$). The rest of the team migrated the project to the CoronaCoin #2, and shortly after that, the third dump happened where the malicious actors[16] got 10 ETH (about $\$2,336.4$). Similar Pump-and-dump scams are found in VaccinaCoin[17] and COVID19 token[18]. There are two scam tokens involved in the ICO scams, i.e., they either provide fake information or entice users to buy the token using giveaway-like tricks. Luckily, these ICO scams have not scammed many users yet. For the Corona Virus Coin[19], it only tricked 1 victim successfully with merely 2.6 dollar profit. Another one is CoronaAid[20], which has not received money yet by the time of this study.

5) The Creators of Scam Tokens: We further analyze the creators of scam tokens, as shown in Figure 17. Overall, 73 creators released 91 tokens. Over 81% (74) of the tokens are created by external addresses (i.e., by humans), while the remaining tokens (17) are created automatically (i.e., by smart contracts). We observe that, some creators (9 external addresses and 2 contract addresses) have released more than one COVID-19 scam token. For example, the address 0xec9005224daa378598aa0ea8f4c656d5a7c6de76 created 4 tokens. After creating 3 tokens that are less popular, this

[15]Address:0xf19afb42e574831776e7af0898f05c1b306bf3b7

[16]Address:0x4121CB0d7AA53AAbc7596c9cAfaa02B1863a2aC7

[17]Address:0x567d297d0cbb66195b268162a4547f220ef49c51, which is found on BitcoinTalk and claims to help COVID-19 vaccine production.

[18]Address:0x6b466b0232640382950c45440ea5b630744eca99

[19]Address:0x49017D1cE3359a3b81AE8417731298126Ff751F1

[20]Address:0xd3CD8Ce0c357CAdC16F812884c2dDb89F8A22103

TABLE VII
TOP-5 ADDRESSES INVOLVED IN GIVEAWAY SCAMS.

Address	# of Incoming Transactions	# of Cryptos Received	Est. Value ($)
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh	321	12.02 BTC	109,799.9
0xd03dc334fb65cea1b83e654b26515e72694a713f	41	5.92 ETH	1,383.2
1Ai52Uw6usjhpcDrwSmkUvjuqLpcznUuyF	39	14.75 BTC	134,781.2
bc1qwr30ddc04zqp878c0evdrqfx564mmf0dy2w39l	36	0.55 BTC	5,050.4
182P8T7MM9assMo7V9YpqZ925yJX8HZurL	23	1.41 BTC	12,838.2

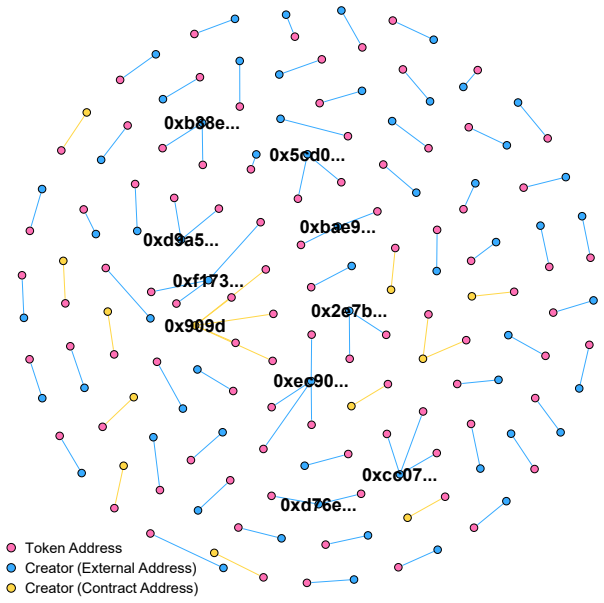


Fig. 17. The creator graph of scam tokens.

address created the 4th token named "Corona Coin"[21], which has 281 holders by the time of this study. Interestingly, 5 scam tokens are created by token template contract MiniMe[22], which has reduced the efforts of creating scam tokens.

TABLE VIII
CRYPTO BLACKMAILS RELATED TO COVID-19.

Address	Trick	# of Incoming Transactions	# of Received Cryptos	Est. Value ($)
1PQMFqfnEtddpPwHyB3E3jWvakDZRmZtCg	Selling products	2	0.023 BTC	213.0
1NM8LLAGcMHjPZJ5ysUWvNrVjwFtQnYjYe	Selling products	1	0.017 BTC	151.5
1JoWQUtGcP2yYdQwDcjsUxgrZjntrBqLLQ	Selling products	2	0.016 BTC	149.9
18P3S6DuNUpW2WLozsrrW6rRd6xh24Rc7N	Virus spread threat	1	594 Satoshi	0.1
bc1q9l5tvr322w36ky9ex8kfhzjhffahmqmxg8s3we	Virus spread threat	0	0	0
bc1q9tpt4dffddj4dgtt8c8meeghvcqveml8j4n9wz	Virus spread threat	0	0	0
bc1qxaujxahx5wvfe4dy4eq5q939yw7ffmj8tctwpj	Virus spread threat	0	0	0
bc1q2868603740f4y3yq6x7ksmqq2gyynyeegpvtc4	Virus spread threat	0	0	0
3EWMDjjY3zimYkbNb9od2uxVeuVREcDpGw	Selling cure	0	0	0

C. COVID-19 Giveaway Scam

In total, we find 19 giveaway scams, to which 5 domains and 10 social accounts are related. Among them, 14 of 21 extracted addresses have succeeded in receiving cryptocurrencies in 2020. Table VII shows top-5 active addresses. The most popular address is *bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh*, which received 321 transactions. This address is a Twitter hack address, which is not used until July 15th. Besides the Twitter hack addresses, the most active address in Ethereum is 0xd03dc334fb65cea1b83e654b26515e72694a713f, whose attackers pretend to be *Vitalik Buterin*, a co-founder of Ethereum. The attacker gets $1383.2 equivalent profit. It can be observed that COVID-19 themed giveaway scams impersonating famous persons or organizations are more effective.

[21] Address:0x170467C28C4BF99f2D3840E730498F730a526Da2

[22] https://github.com/Giveth/minime, address: 0x909d05F384D0663eD4BE59863815aB43b4f347Ec

Fig. 18. An example of a scam description on https://coronainvest.io/.

D. COVID-19 Crypto Blackmail

We have collected 9 addresses related to blackmails, all of which are Bitcoin addresses. They are totally reported 23 times on BitcoinAbuse by users. The profit they made is shown in Table VIII. To our surprise, attackers do not make too much profit through these tricks. The most profitable address has received 0.023 BTC, which claims to sell products during the pandemic. 6 of the scam addresses do not even receive any money. It might because people's awareness of such scams has increased, while scaring people with virus by email is difficult to cheat people.

E. COVID-19 Crypto Malware

As to COVID-19 themed crypto malware, we have identified 5 Android ransomware and 9 Windows malware binaries (4 labeled as Ransomware and 5 labeled as Coinminer). By manually investigation, we found 4 addresses in them (1 address shared by 4 Android apps and 2 addresses embedded in 1 windows ransomware). Their profits are shown in Table IX. The only address which made a profit is related to the domain `http://coronavirusapp.site` and its distributed apps are disguised as coronavirus tracker apps.

F. COVID-19 Ponzi Scheme

We find 9 websites that are suspicious to carry out Ponzi schemes. For example, they claimed that they will invest in vaccine of COVID-19 and make the investors get financial freedom, as shown in Figure 18. Table XI lists the 9 websites. We can see that, most of them contain the keyword "invest" in their domain names, and the descriptions shown on their websites indicate they are highly suspicious to be scams. However, by the time of our study, none of them can function well or they are just unreachable during our manually analysis. Thus, we cannot get their scam blockchain addresses, so that we cannot estimate their impacts and the number of victims.

TABLE IX
CRYPTO MALWARE WITH BLOCKCHAIN ADDRESSES.

App Name	Source	MD5	Address	Total Received($)
Coronavirus Tracker	coronavirusapp.site	d1d417235616e4a05096319bb4875f5, 1602c0258f39b2b032edd7d6160befe7, 339de9104962d6c8cfd6d8b4a68bcb4d, 69a6b43b5f63030938c578eec05993eb	18SykfkAPEhoxtBVGgvSLHvC6Lz8bxm3rU	98.4
Covid19	Koodous	362dac3f2838d2bf60c5c54cc6d34c80	3HEtt3VHoAj18rDbJoYv6mbojBK4DY9zyu	0
WSHSetup.exe	www.wisecleaner.best	ec517204fbcf7a980d137b116afa946d	bc1qkk6nwhsxvtp2akunhkke3tjcy2wv2zkk00xa3j, bc1q8r42fm7kwg68dts3w70qah79n5emt5m76rus5u	0

TABLE X
TOP 5 MOST PROFITABLE DONATION SCAM ADDRESSES.

Address	# of Incoming Transactions	# of Cryptos Received	Est. Value ($)
142pEjfSBh8cnvE7BMJXMjoSBedJWvRKAG	1	1 BTC	9,132.2
TVBkqA4BuAoy8p3tNXMvHeC45BuC7PHJw3	2	211,254.33 TRX	3,621.7
3GLHpGWbBi1cAWUbn4mSx5RJygDmA6d89o	3	0.29 BTC	2,661.3
1G5TxBiZ8JDYNgUnjsY8KoAQxq2Sj6dKby	45	0.19 BTC	1,805.2
15f7eGQt2CLJJB86jt5whrZQ5RRERCT574	5	0.14 BTC	1,257.4

TABLE XI
A LIST OF COVID-19 THEMED PONZI SCHEME DOMAINS.

Ponzi Scheme Websites	
coronainvest.io	covidinvestmenthelp.com
coronabit.cc	covid19invest.com
coronafeverinvest.com	covid-19investmentchallenge.azonixtech.com
covid-invest.tk	covid-invest.laber.ru
coronacoin.xyz	

G. COVID-19 Fake Crypto Donation

We have identified 76 blockchain donation scam addresses, which are related to 23 domains and 30 social accounts. Table X shows the top 5 most profitable addresses. The most profitable address 142pEjfSBh8cnvE7BMJXMjoSBedJWvRKAG received 1 BTC on March 22nd. In total, 28 of 76 addresses have made a profit of 21788.9 US dollars, which accounts for the third largest scam category by profit in our dataset. Because of donation's close connection with this pandemic, such a serious condition deserves our vigilance.

VI. DISCUSSION

A. Implication

Our observations are of key importance to the stakeholders in the blockchain ecosystem and the researchers who are interested in COVID-19 themed cybersecurity. On one hand, considering the prevalent COVID-19 themed crypto scams in the wild and their great impacts, it is urgent for the community to detect these scams and eliminate possible losses. On the other hand, it suggests that the attackers are taking advantage of this kind of public event to perform cyber-attacks. Although the six types of scams studied in this paper follow the similar behavior patterns as other non-Coronavirus scams suggested in previous work, they have adopted a number of social engineering techniques to deceive users, and similar techniques can be easily adopted to other social events or domains. Thus, the governance of the cyberspace on social events should be improved. For example, paying special attentions to the newly released domains/tokens/social network accounts that related to the public events can help us identify these scams timely. Furthermore, identifying the distribution channels (e.g., Twitter, Telegram, and malicious domains, etc.) of these scams can greatly reduce the impacts.

B. Limitation

Our study carries several limitations. First, the taxonomy of scams might not be complete. As the taxonomy is summarized based on public known scams reported by users in the wild, it is quite possible that there are new tricks we did not identified. Nevertheless, we believe we have covered most kinds of the COVID-19 themed crypto scams. Second, as suggested in Section V-A3, a few scam addresses were active before 2020. Although we only count their transactions after the break of COVID-19 (only 7 of them have transactions in 2020), it is hard to differentiate how many of them are actually involved in COVID-19 scams. Nevertheless, we found that most of them have very few transactions before 2020, and there is usually a quiet period till their rejuvenation in COVID-19. As a result, we believe most of the revenue should be credited to COVID-19. Furthermore, it is quite possible that one scam address can be used to fulfill more than one type of scam activities, while is hard to us to differentiate. At last, this work relies on some manually efforts to identify the unrevealed scams, which might not be scalable. Although we have tried our best to reduce the efforts, i.e., by using VirusTotal to label the suspicious scams first, and applying heuristics to mark COVID-19 related scams, we admit that some advanced techniques (e.g., machine learning techniques) can be implemented to identify and classify the scams in the future. However, while the study is by no means comprehensive, we are able to provide a lower bound estimate of the prevalence and criminal profits associated with these COVID-19 scams.

VII. CONCLUSION

In this paper, we take the first step to characterize COVID-19 themed cryptocurrency scams. We investigated six types of cryptocurrency scams related to COVID-19 by collecting existing scam reports and detecting the unrevealed ones. Specifically, we revealed how the scams work, measured their prevalence in the wild, studied their evolution and characterized their impacts. Besides, we released the labeled scam dataset to the research community to help fight against the COVID-19 attacks in cyberspace.

REFERENCES

[1] "Facing down the myriad threats tied to COVID-19," 2020, https://news.sophos.com/en-us/2020/04/14/covidmalware/?cmp=30728.

[2] "Threat Intel — Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic," 2020, https://labs.sentinelone.com/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/.

[3] R. He, H. Wang, P. Xia, L. Wang, Y. Li, L. Wu, Y. Zhou, X. Luo, Y. Guo, and G. Xu, "Beyond the virus: A first look at coronavirus-themed mobile malware," *arXiv preprint arXiv:2005.14619*, 2020.

[4] "Phishing Activity Trends Reports," 2020, https://apwg.org/trendsreports/.

[5] "Americans lost $77 million to Covid-19 fraud," 2020, https://www.cnbc.com/2020/07/07/covid-19-fraud-has-cost-americans-at-least-77-million.html.

[6] "FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic," 2020, https://www.fbi.gov/news/pressrel/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic.

[7] "Scammers Impersonate World Health Organization to Steal BTC COVID-19 Donations," 2020, https://cointelegraph.com/news/scammers-impersonate-world-health-organization-to-steal-btc-covid-19-donations.

[8] "CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware," 2020, https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware.

[9] "Corona Coin - Another Exit Scam, Yes, It Is The Third Time!" 2020, https://www.publish0x.com/boyka/corona-coin-another-exit-scam-yes-it-is-the-third-time-xklnxp?tid=scam3.

[10] "All Cryptocurrencies — CoinMarketCap," 2020, https://coinmarketcap.com/all/views/all/.

[11] T. Chen, Y. Zhang, Z. Li, X. Luo, T. Wang, R. Cao, X. Xiao, and X. Zhang, "Tokenscope: Automatically detecting inconsistent behaviors of cryptocurrency tokens in ethereum," in *Proceedings of the SIGSAC Conference on Computer and Communications Security*. ACM, 2019.

[12] W. Chen, T. Zhang, Z. Chen, Z. Zheng, and Y. Lu, "Traveling the token world: A graph analysis of ethereum erc20 token ecosystem," in *Proceedings of The Web Conference 2020 (WWW '20)*, 2020, p. 1411–1421.

[13] "Year in review: biggest cryptocurrency scams of 2019," 2019, https://currency.com/biggest-cryptocurrency-scams-of-2019.

[14] M. Vasek and T. Moore, "There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams," in *International conference on financial cryptography and data security*. Springer, 2015, pp. 44–61.

[15] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting ponzi schemes on ethereum: Towards healthier blockchain technology," in *Proceedings of the 2018 World Wide Web Conference*, 2018, pp. 1409–1418.

[16] M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, "Dissecting ponzi schemes on ethereum: identification, analysis, and impact," *Future Generation Computer Systems*, vol. 102, pp. 259–277, 2020.

[17] M. Bartoletti, B. Pes, and S. Serusi, "Data mining for detecting bitcoin ponzi schemes," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018, pp. 75–84.

[18] M. Vasek and T. Moore, "Analyzing the bitcoin ponzi scheme ecosystem," in *International Conference on Financial Cryptography and Data Security*. Springer, 2018, pp. 101–112.

[19] W. Chen, Y. Xu, Z. Zheng, Y. Zhou, J. E. Yang, and J. Bian, "Detecting" pump & dump schemes" on cryptocurrency market using an improved apriori algorithm," in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*. IEEE, 2019, pp. 293–2935.

[20] K. Toyoda, T. Ohtsuki, and P. T. Mathiopoulos, "Identification of high yielding investment programs in bitcoin via transactions pattern analysis," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[21] K. Toyoda, P. T. Mathiopoulos, and T. Ohtsuki, "A novel methodology for hyip operators' bitcoin addresses identification," *IEEE Access*, vol. 7, pp. 74 835–74 848, 2019.

[22] D. Liebau and P. Schueffel, "Crypto-currencies and icos: Are they scams? an empirical study," *An Empirical Study (January 23, 2019)*, 2019.

[23] D. A. Zetzsche, R. P. Buckley, D. W. Arner, and L. Föhr, "The ico gold rush: It's a scam, it's a bubble, it's a super challenge for regulators," *University of Luxembourg Law Working Paper*, no. 11, pp. 17–83, 2017.

[24] N. Gandal, J. Hamrick, T. Moore, and T. Oberman, "Price manipulation in the bitcoin ecosystem," *Journal of Monetary Economics*, vol. 95, pp. 86–96, 2018.

[25] W. Chen, J. Wu, Z. Zheng, C. Chen, and Y. Zhou, "Market manipulation of bitcoin: evidence from mining the mt. gox transaction network," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 964–972.

[26] J. Hamrick, F. Rouhi, A. Mukherjee, A. Feder, N. Gandal, T. Moore, and M. Vasek, "The economics of cryptocurrency pump and dump schemes," 2018.

[27] ——, "An examination of the cryptocurrency pump and dump ecosystem," *Available at SSRN 3303365*, 2018.

[28] C. F. Torres, M. Steichen *et al.*, "The art of the scam: Demystifying honeypots in ethereum smart contracts," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 1591–1607.

[29] J. Wu, Q. Yuan, D. Lin, W. You, W. Chen, C. Chen, and Z. Zheng, "Who are the phishers? phishing scam detection on ethereum via network embedding," *arXiv preprint arXiv:1911.09259*, 2019.

[30] R. Phillips and H. Wilder, "Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites," *arXiv preprint arXiv:2005.14440*, 2020.

[31] Y. Bai, L. Yao, T. Wei, F. Tian, D.-Y. Jin, L. Chen, and M. Wang, "Presumed asymptomatic carrier transmission of covid-19," *Jama*, vol. 323, no. 14, pp. 1406–1407, 2020.

[32] Z. Y. Zu, M. D. Jiang, P. P. Xu, W. Chen, Q. Q. Ni, G. M. Lu, and L. J. Zhang, "Coronavirus disease 2019 (covid-19): a perspective from china," *Radiology*, p. 200490, 2020.

[33] G. Onder, G. Rezza, and S. Brusaferro, "Case-fatality rate and characteristics of patients dying in relation to covid-19 in italy," *Jama*, vol. 323, no. 18, pp. 1775–1776, 2020.

[34] C. Shen, Z. Wang, F. Zhao, Y. Yang, J. Li, J. Yuan, F. Wang, D. Li, M. Yang, L. Xing *et al.*, "Treatment of 5 critically ill patients with covid-19 with convalescent plasma," *Jama*, vol. 323, no. 16, pp. 1582–1589, 2020.

[35] G. Pennycook, J. McPhetres, Y. Zhang, J. G. Lu, and D. G. Rand, "Fighting covid-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention," *Psychological science*, p. 0956797620939054, 2020.

[36] W. Nelson and M. Osman, "Sociological and psychological insights behind predicted changes as a result of covid-19," 2020.

[37] J. Zhang, Y. Xie, Y. Li, C. Shen, and Y. Xia, "Covid-19 screening on chest x-ray images using deep learning based anomaly detection," *arXiv preprint arXiv:2003.12338*, 2020.

[38] L. Wang and A. Wong, "Covid-net: A tailored deep convolutional neural network design for detection of covid-19 cases from chest x-ray images," *arXiv preprint arXiv:2003.09871*, 2020.

[39] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *arXiv preprint arXiv:2006.11929*, 2020.

[40] A. R. Mathew, "Cybersecurity pros warn–covid-19 pandemic as a tool."

[41] P. Radanliev, D. De Roure, and M. Van Kleek, "Digitalization of covid-19 pandemic management and cyber risk from connected systems," *arXiv preprint arXiv:2005.12409*, 2020.

[42] J. Kallberg and S. S. Hamilton, "What covid-19 can teach us about cyber resilience," *Fifth domain*, 2020.

[43] T. Ahmad, "Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity," *Available at SSRN 3568830*, 2020.

[44] R. Sun, W. Wang, M. Xue, G. Tyson, S. Camtepe, and D. Ranasinghe, "Vetting security and privacy of global covid-19 contact tracing applications," 2020.

[45] "Year in review: biggest cryptocurrency scams of 2019," 2020, https://www.domaintools.com/.

[46] "McAfee," 2020, https://www.mcafee.com.

[47] "Bitcointalk," 2020, https://bitcointalk.org/.

[48] "BitcoinAbuse," 2020, https://www.bitcoinabuse.com/.

[49] "Consumer Information Blog ," 2020, https://www.consumer.ftc.gov/blo.

[50] "AlienVault," 2020, https://otx.alienvault.com/.

[51] "COVID-19 MISP Project," 2020, https://covid-19.iglocska.eu/.

[52] "How Cryptocurrency Pump-and-Dump Scams Work," 2020, https://www.investopedia.com/news/how-cryptocurrency-pumpanddump-scams-work/.

[53] "CoronaCoin: crypto developers seize on coronavirus for new, morbid token," 2020, https://www.reuters.com/article/us-china-health-crypto-currency/coronacoin-crypto-developers-seize-on-coronavirus-for-new-morbid-token-idUSKCN20M32A.
[54] "CoronaCoin More drama, third exit scam and discord deleted," 2020, https://bitcointalk.org/index.php?topic=5237350.0.
[55] "Major US Twitter accounts hacked in Bitcoin scam," 2020, https://www.bbc.com/news/technology-53425822.
[56] M. Paquet-Clouston, M. Romiti, B. Haslhofer, and T. Charvat, "Spams meet cryptocurrencies: Sextortion in the bitcoin ecosystem," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies (AFT '19)*, 2019, p. 76–88.
[57] "THE STATE OF RANSOMWARE 2020," 2020, https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf.
[58] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem," *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz003, 2019.
[59] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, K.-K. R. Choo, and D. E. Newton, "Drthis: Deep ransomware threat hunting and intelligence system at the fog layer," *Future Generation Computer Systems*, vol. 90, pp. 94–104, 2019.
[60] "Ponzi Scheme," 2020, https://www.investopedia.com/terms/p/ponzischeme.asp.
[61] "CryptoScamDB," 2020, https://cryptoscamdb.org/.
[62] "StopScamFraud," 2020, https://stopscamfraud.com/.
[63] "Etherscan," 2020, https://etherscan.io/.
[64] "URLScan," 2020, https://urlscan.io.
[65] J. Szurdi, B. Kocso, G. Cseh, J. Spring, M. Felegyhazi, and C. Kanich, "The long "taile" of typosquatting domain names," in *Proceedings of the 23rd USENIX Conference on Security Symposium*, ser. SEC'14. USA: USENIX Association, 2014, p. 191–206.
[66] P. Kintis, N. Miramirkhani, C. Lever, Y. Chen, R. Romero-Gómez, N. Pitropakis, N. Nikiforakis, and M. Antonakakis, "Hiding in plain sight: A longitudinal study of combosquatting abuse," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17, 2017, p. 569–586.
[67] "RiskIQ," 2020, https://community.riskiq.com/.
[68] "VirusTotal," 2020, https://www.virustotal.com/.
[69] "Koodous," 2020, https://koodous.com.
[70] M. Sebastián, R. Rivera, P. Kotzias, and J. Caballero, "Avclass: A tool for massive malware labeling," in *Research in Attacks, Intrusions, and Defenses*, F. Monrose, M. Dacier, G. Blanc, and J. Garcia-Alfaro, Eds. Springer International Publishing, 2016, pp. 230–253.
[71] "DAppTotal," 2020, https://dapptotal.com/.