

# Bitcoin Phishing Scam

James Mc Ginty, Tapan Soni, and Vahid Heydari

Department of Computer Science, Rowan University  
Glassboro, NJ, 08028

Email: {mcgintyj1, sonit9}@students.rowan.edu, heydari@rowan.edu

**Abstract**—The act of scamming a victim out of money is nothing new. It has been going on for many years. The idea of a scam is to extort money out of a victim by offering some type of fake service in exchange for money. Many classical scams such as the IRS [1] and Microsoft Windows technical support [2] scams have been used by countless scammers for many years and have yielded millions of dollars. In recent years, a new type of scam has surfaced. Scammers are now targeting Bitcoin as the new currency to exploit because of its decentralized structure and anonymity features. In this paper, a detailed description and analysis of a Bitcoin scam accidentally discovered by two students are presented. It targets users who try to reverse search anonymous phone calls on Google and lures them in with an option to withdraw thousands of dollars worth of Bitcoin by just depositing a few hundred dollars to meet an immutable minimum withdraw limit.

**Index Terms**—bitcoin, BTC, blockchain, security, phishing, scam, OSINT

## I. INTRODUCTION

Bitcoin [3] a virtual currency established in August of 2008 has been on the rise in recent years as an upcoming decentralized method of payment. Bitcoin (BTC) has steadily risen in value to 9,225 USD per one Bitcoin as reported by a Statista report for October 2019. [4] Bitcoin’s popularity is due in part to greater efficiency of transferring funds across the Internet via a decentralized network with a transparent set of rules. Its popularity is also attributed to the fact Bitcoin can be mined through the process of adding transaction records to Bitcoin’s public ledger of past transactions or blockchain. [5] [6] With these reasons for Bitcoin’s success in mind, one can begin to understand how valuable owning any form of Bitcoin can be.

On November 4th, 2019, we discovered a sizeable phishing scam after missing a phone call from the number 1-201-794-4601 located in Fair Lawn, NJ. Research of the phishing scam was conducted with assistance from the Rowan Center for Cybersecurity Education and Research [7], and Michael Ghen founder of Philadelphia Blockchain Security Company. [8] Upon returning the phone call, the number presented by the caller id was found to be spoofed and not currently in service. This was most likely an attempted spam call from an external unrelated party. Deciding to take further action regarding the matter, the phone number was immediately reverse searched through Google in an attempt to discover if it was reported in the past for malicious behavior. The first three websites on the search page were accessed but all of which did not turn up any relevant information on the number until the fifth listed

website. The fifth website phone-book.xyz/1201/J8YAK.php listed the spoofed phone number as well as hundreds of randomly generated numbers all under the 1-201 area code. This website was discovered to be an archive of 1,300 pages of randomly generated numbers all of which were under various international and United States area codes. With this discovery in hand, further research was conducted to discover the origins of the creator and true purpose of the websites which formed the foundation of the phishing scam.

The rest of this paper is organized as follows. In the next two sections, the steps taken to research and document the discovery of the phishing scam are presented. This is followed by the final section regarding the steps taken to remove the phishing scam from operation as well as a conclusion with lessons learned and future work.

## II. DESIGN OF THE PHISHING SCAM

The phishing scam revolving around extorting a payment in Bitcoin from a victim was a highly sophisticated and re-occurring operation. The website phone-book.xyz containing the phone number was structured to be a plain HTML dump of thousands of numbers as well as a fake but convincing error message.

The original URL, phone-book.xyz/1201/J8YAK.php, was a page cataloging many 1-201 area code numbers but upon removal /J8YAL.php had lead to a listing of all other PHP files on the site for the 1-201 area code. Every .php file contained an area code from the United States or another country with hundreds of randomly generated phone numbers and the same error message at the top of the page. Figure 1 shows the design of the phone-book.xyz website with the error message on the top of the page and the dump of phone numbers following the error message. Upon removing /J8YAL.php from the end of the URL, it led us to a listing of all the other PHP files on that were hosted which belonged to the 1-201 area code. Figure 2 shows the listing of all the PHP files for the 1-201 area code. To discover the other area codes’ files, we had to change the area code in the URL, for example, phone-book.xyz/1856/ which would then show all the PHP files for the 1-856 area code. The mere scale of the website had suggested it was auto-generated using a script from the website’s malicious owner to create the 1,300 plus pages in the site’s directory targeting many different US area codes. The figure of 1,300 pages was discovered by entering the domain name into the Google search bar to specify the number of results only from said website. This also leads us to the conclusion that the

owner(s) of this scam were trying to target as many people as possible by generating a large number of numbers for each area code.

Caller Number Lookup

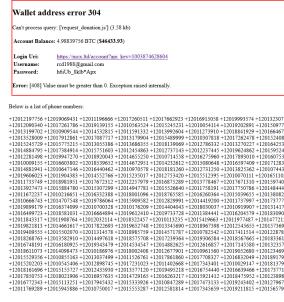


Fig. 1. Design of phone-book.xyz



Fig. 2. Directory of .phps on phone-book.xyz

The top of each of the PHP files for every area code listed on the website included a fake but convincing error message from a failed donation form. This error message presented the user with the belief that the JavaScript code enabling mining of Bitcoin due to people viewing the website or some other reason, had failed to run thus exposing the credentials of the linked account. The error message was labeled "Wallet address error 304" claiming "Can't process query: ['request\_donation.js']" with the error code "[408] Value must be greater than 0. Exception raised internally." An account balance was visible with 4.98839756 BTC worth \$46,433.93 USD at the time of discovery as well as a login URL of [https://mcx.ltd/account?api\\_key=1003874628604](https://mcx.ltd/account?api_key=1003874628604). [9] Below the login URL was a username of rcd1988@gmail.com and password of h6iUb\_8klb\*Ap. The error message was proven to be false, not only because it appeared on every page, but because it was hard-coded through an iframe HTML element as seen in figure 3. Even the password was in the comments of the code. The use of the provided login URL had lead to the website Miner Coin Exchange claiming to be an online wallet for Bitcoin-based out of London, UK.

Miner Coin Exchange [10] provided a very convincing dashboard for BTC management upon login as seen in figure 4. This dashboard presented various features to the user such as hash rate, mining performance, account transaction history,

```

<html>
  <head>
    <title>codingground - Online HTML Editor (HTML-4)</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0" />
    <script>
      // ...
    </script>
  </head>
  <body>
    <div>
      <div>CodingGround</div>
      <div>Online HTML Editor (HTML-4)</div>
      <div><a href="#">Home</a> <a href="#">About</a> <a href="#">Contact</a> <a href="#">Logout</a> <a href="#">Sign Up</a> <a href="#">Sign In</a></div>
      <div>Wallet address error 304</div>
      <div>Can't process query: ['request_donation.js'] (3.58 kB)</div>
      <div>Account Balance: 4.98839756 BTC (546433.93)</div>
      <div>Login URL: https://mcx.ltd/account?api_key=1003874628604</div>
      <div>Username: rcd1988@gmail.com</div>
      <div>Password: h6iUb_8klb*Ap</div>
      <div>Error: [408] Value must be greater than 0. Exception raised internally.</div>
    </div>
  </body>
</html>

```

Fig. 3. Source code for fake error message of phone-book.xyz as result of a failed donation link web application

support section, and a live account balance both in BTC and USD. The conversion from BTC to USD was the only legitimate part of this entire operation. The phishing scam at the stage of login began to take effect, which started with the user excitedly seeking to withdraw a large amount of currency. To withdraw the currency using the transfer menu, it was discovered that a minimum account balance of 5.0 BTC was required for the transfer to authorize. The transfer requirement was visible from both the Settings menu where it was permanently set to 5.0 BTC as shown in figure 5 and an error message would arise after any attempted transfers out of the account with a balance of less than 5.0 BTC.

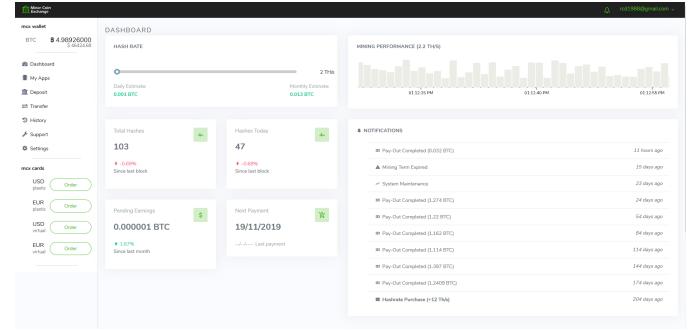


Fig. 4. Miner Coin Exchange user dashboard

Personal Information

Personal details

First name\*: Roger

Last name\*: Daniels

Country of residence\*: United States

Gender\*: Male

Minimum withdrawal (BTC)\*: 5

Note: Withdrawal can be charged. Learn more

Email\*: rodd1988@gmail.com

Provide info

IMPORTANT INFORMATION

ATTENTION

Provide only personal information you will be able to confirm in case of applying for verification

Fig. 5. Miner Coin Exchange profile settings

The only available option to transfer in or out of the account was through Bitcoin which meant to achieve 5.0 BTC in the account individuals had to transfer in the appropriate amount

of BTC which satisfied the 5.0 BTC minimum balance from their accounts. To transfer into the account, a deposit address could be generated from the Deposit menu. Upon transferring the appropriate amount of BTC into the account a window would appear stating the transaction amount as a success. The transaction history page would then update with a fresh entry to show said transaction succeeding. The scam was so successful because it preyed on people who followed their instincts to seize the funds of the account instead of contacting its owner or even examining the website to first ensure it was legitimate.

The phishing scam could also be identified in various other ways through browsing the features of the dashboard. Examining the account history showed a very precise withdrawal behavior of every 30 days, though it stated the most recent withdraw as oddly only 24 days ago with a worth of almost the exact amount to reach 5.0 BTC. Figure 6 shows many transactions that were seemingly occurring in the account but the amounts and dates didn't match up with the notifications on the dashboard. This was a sure sign the account may have been set up to maliciously lure individuals into withdrawing a similar valued amount. This may have seemed like a small amount of BTC but was easily worth hundreds of USD. Another sure sign the account was fake was the live counter for BTC mining showing the account balance would never reach 5.0 BTC, so it always relied on an individual transferring in external funds to the account to bring the balance to 5.0 BTC. If you attempted to place the funds onto a card provided by MTX the options would always lead to an invalid page.

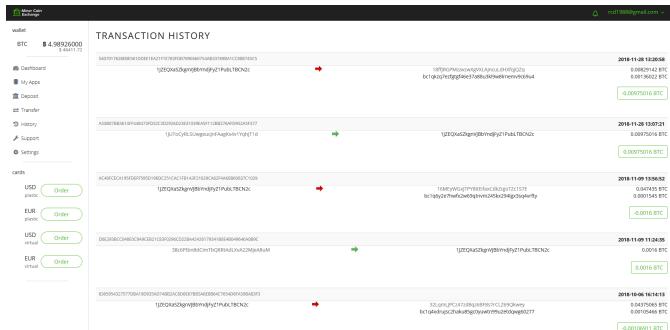


Fig. 6. Miner Coin Exchange account transaction history

The support page of the website provided users the ability to leave a help desk ticket explaining their problem. Though the issue with the ticketing functionality was that when submitting the tickets they would not appear after logging back into the account. The process of removing the visibility of these tickets was to ensure no warning messages of the scam were left behind by other users who discovered the account in the past. Figure 7 shows the support page offered by Miner Coin Exchange. An exposed admin panel [11] of the website was discovered as well by adding a /admin suffix to the mcx.ltd domain. Figure 8 shows the exposed admin panel. This exposed admin panel archived all submitted support tickets available from non-paying and paying customer accounts. Each ticket

was comprised of a reply function, reply subject, ticket title, message body, ticket account owner, time, and date. Upon browsing the hundreds of tickets submitted throughout the website's lifetime the messages left behind included various Bitcoin addresses, pleas for help of those scammed, offers to join the scam's operations, attempted SQL injections, and the contact information of various individuals. New tickets were shown to be submitted on an almost daily basis which brings to concern that there may be numerous other feeder websites leading to more successful scams on victims. A filter was also present on the exposed admin panel which sorted the tickets by paying and non-paying customers. Paying customers were identified as accounts containing Bitcoin balances which included the fake Roger Daniels account and victims who created their accounts and deposited money. Non-paying customers were individuals who had made their accounts but hadn't transferred any money. Figure 9 shows the filter of the admin panel in effect. The admin panel was also plagued with various pop-ups that presented messages such as "hello world" and a random hash of characters with btcserpent.com [12] linked within. These pop-ups prevented the use of the admin panel until dismissed and their origins may be linked to prior attempted SQL injections. Due to the pop-ups, the console of any web browser would show "refused to display" errors leading to r87.com [13] and netsparker.com [14], both of which belonged to Netsparker, a web application security solution. Netsparker may have been being used as the security solution for mcx.ltd and coinkeeper.cc but the prior SQL injections seem to have been affecting mcx.ltd/admin from correctly communicating with the security solution. Figures 10 and 11 show the popups on the admin panel and the errors linking to r87 and netsparker.

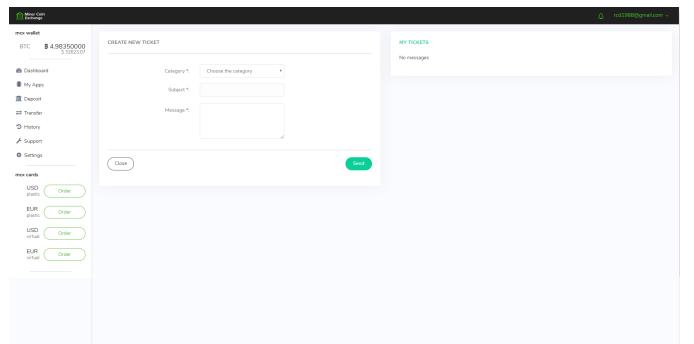


Fig. 7. Miner Coin Exchange support ticket system

Regarding the structure of mcx.ltd a series of connected hidden pages were also found outside of the admin panel such as mcx.ltd/index [15] and mcx.ltd/tokensale. [16] Figures 12 and 13 show the index and tokensale pages for mcx.ltd. The index page leads to a very convincing looking homepage for the Miner Coin Exchange which detailed the services available for customers as well as a fake staff team and set of advisors. The set of staff and advisors linked were believed to not be related to the scam upon investigating the legitimate LinkedIn accounts linked under each person's description. The

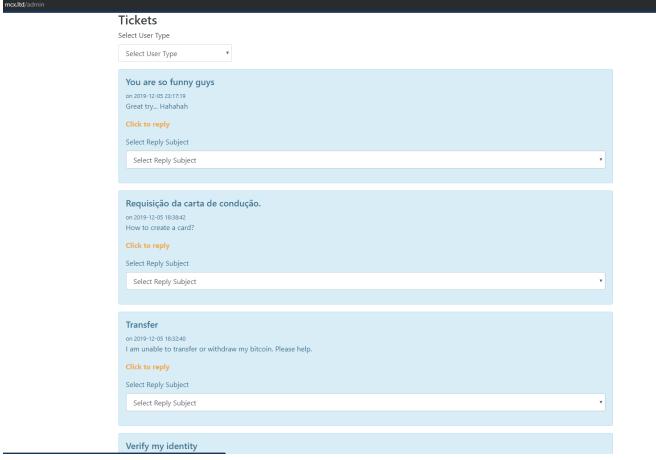


Fig. 8. Exposed admin panel detailing all support tickets for every account on mcx.ltd

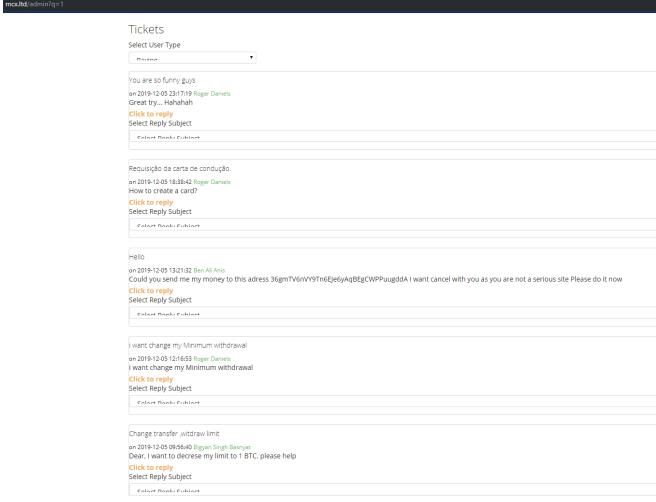


Fig. 9. The filtered mcx.ltd support tickets for every account considered paying which included Roger Daniels

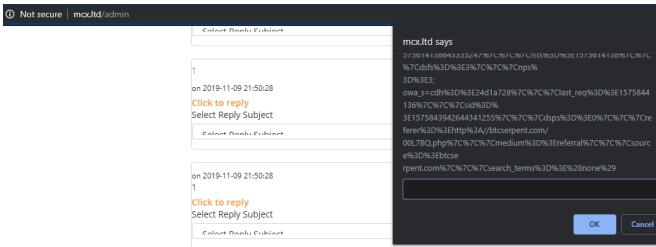


Fig. 10. Example of the pop-ups rampant while visiting the mcx.ltd admin panel

operators of this scam most likely used a template website that included these individuals or they purposely compiled a list of said individuals to present the website as a legitimate Bitcoin exchange. The index page also lists several partners and investor companies who were most likely not related in any capacity to the scam. At the bottom of the index page were three social media accounts, Slack [17], a forum

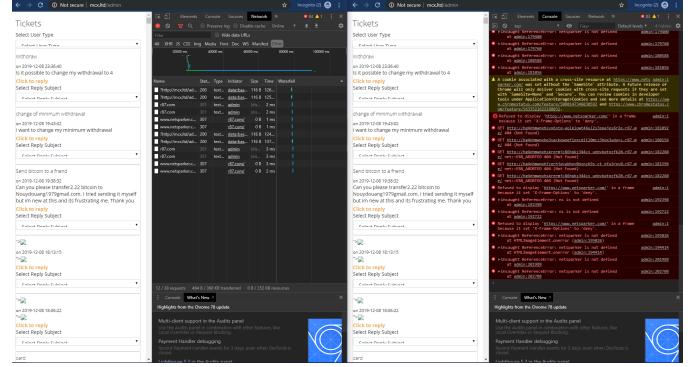


Fig. 11. Web browser console showing reference to r87.com and netsparker.com

[18], and reddit [19] all of which simply were locations which already existed with names conveniently related to MCX such as www.reddit.com/mcx. The Slack invite link provided by Herokuapp states the maximum number of invites was already reached showing it was no longer available. The forum lead to a discussion hub related to Bitcoin and the subreddit which seemed to be a non-related location filled with random posts from the account /u/mccxx. [20] The index page also leads to a "Token Sale" web page which detailed a countdown clock, as well as the various other cryptocurrencies Miner Coin Exchange, claimed to be associated with. The "Token Sale" while not exactly certain seems to allude to a possible new cryptocurrency being created by Miner Coin Exchange purchasable by other cryptocurrencies. Figure 14 shows the cryptocurrencies listed on mcx.ltd/tokensale. The countdown timer till the start of the "Token Sale" was currently paused, so one was only left to speculate what the purpose of said tokens would have been. A whitepaper button was also provided on the Token Sale web page leading to the inactive cryptomerchantbank.co/whitepaper [21] leaving its true purpose unknown.

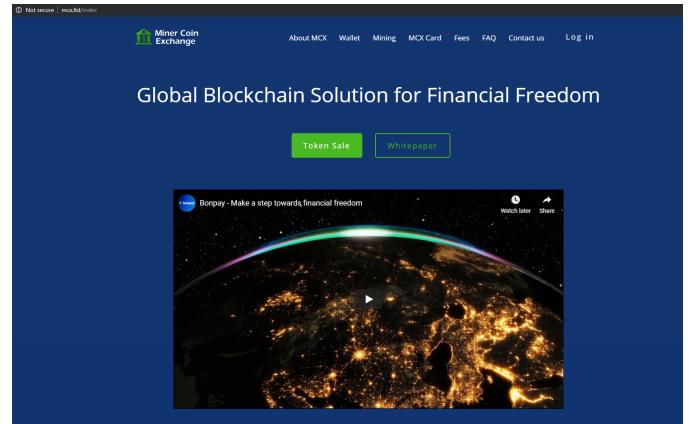


Fig. 12. The hidden index page for mcx.ltd including the Token Sale and Whitepaper buttons

The security of the site was also at risk as the site URL was not an HTTPS [22] but instead an HTTP [23] website.

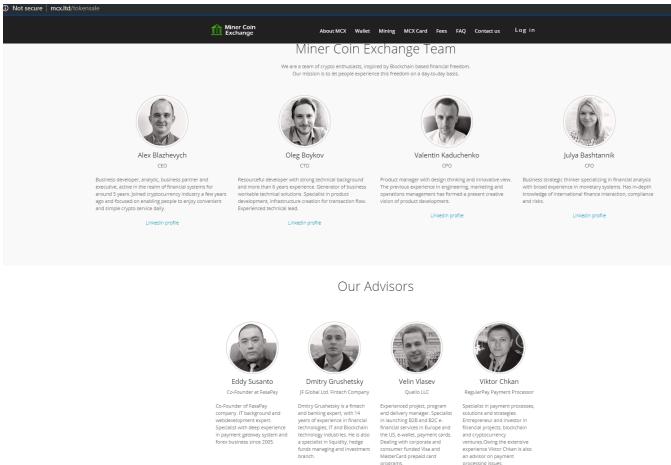


Fig. 13. The Token Sale page for mcx.ltd detailing the fake staff and advisors team

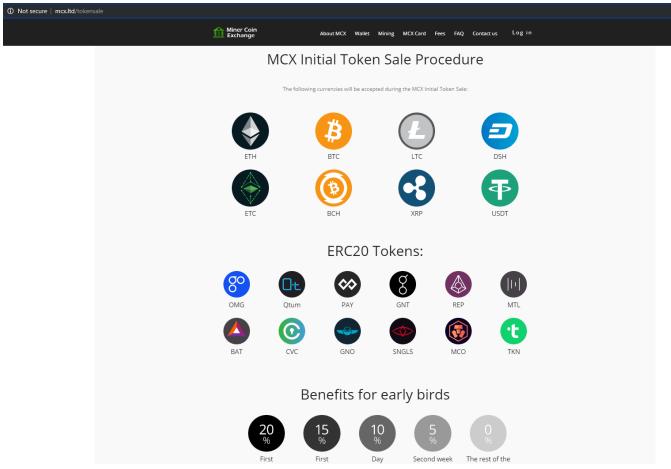


Fig. 14. The list of accepted cryptocurrencies the Tokens would supposedly be purchased with

Though if the URL was changed to HTTPS a secure version of the website did load, this secure version was not linked on any of the prior discovered fake error messages. This meant packets of data transferred to the HTTP site such as passwords were not encrypted leaving it vulnerable to interception by others on the individual's network through programs such as Wireshark. [24] The fact that the owner of the website chose not to provide this extra layer of security common among the linked websites currency-related or other, was a major red flag to prove malicious intent with all other signs included. The HTTPS variant of mcx.ltd certificate upon inspection was valid and issued on 7/30/2019 by the commercial Certificate Authority Sectigo.com [25] as shown in the figure. 16 The HTTPS variant of mcx.ltd most likely was not linked to during the scam to avoid the certificate from being revoked due to a report on the website. Once a certificate is removed websites were permanently placed on a Certificate Revocation List leading to any connecting web browser, to promptly warn users of an untrustworthy website.

The certificate may have been purchased to help improve the website's search engine optimization so a few more innocent users could be lured in without the use of the feeder websites. Lastly, another large sign of this being an orchestrated phishing scam attempt can be proven immediately at the login page of the Mining Coin Exchange. At the login page, by using the rcd1988@gmail.com username and any password as long as it was not blank allowed entry to the account. Figure 15 shows the password field in the login form. With all of these signs documented, any individual who instead of following their instincts to immediately withdraw, could have found this was a scam after devoting a small amount of time to test the website functionality.

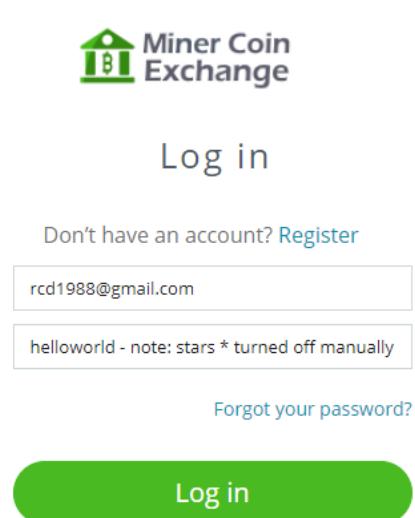


Fig. 15. Demonstration of any password being used for MCX.ltd rcd1988@gmail.com account

This phishing scam as prior mentioned was so successful because it relied on people who followed their instincts to remove the balance from the account because they wanted an instant monetary gain instead of reporting the exposed credentials. So individuals overall must be more aware of their surroundings on the Internet while accessing various websites to prevent overreactions and theft of personal information.



Fig. 16. Certificate Information issued by Sectigo for mxc.ltd

### III. OSINT INVESTIGATION

Aside from the investigation of the functionality for the Mining Coin Exchange website, an Open Source Intelligence (OSINT) [26] investigation was also conducted to detect signs of malicious intent. Open Source Intelligence refers to information derived from public sources on the "surface-web" such as through Google or Bing. Websites like Reddit, Facebook, Wikipedia, and general forums have contained valuable information in the past regarding all sorts of past scams such as Bitcoin phishing scams. A Reddit post from seven months ago by user BrandoGil discovered a past iteration of phone-book.xyz under a different domain name but with the same function of compiling a directory of thousands of numbers on pages with the same error message. [27] The discovered scam had also claimed to hold an account of 4.9 BTC with a minimum withdraw amount of 5.0 BTC. The post included an image similar to the one before showing the credentials and login URL to an iteration of the Miner Coin Exchange Website. Figures 17 and 18 show information of the Reddit post.

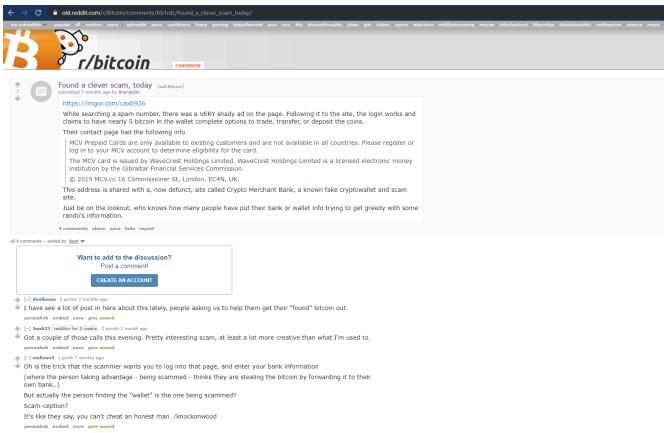


Fig. 17. Reddit post referencing past iteration of the Miner Coin Exchange scam

It was believed at the time of the post the URL for the Miner Coin Exchange was not mxc.ltd but instead themcx.co which has since been taken down proving past iterations existed. The news website Omnia was the first website to be found which had reported on the covariant of the Miner Coin Exchange. [28] Figure 19 shows the story from Omnia.

The screenshot shows a mobile browser with the URL 'caller-idx.xyz'. The page title is 'Caller Number Lookup'. A red box highlights a section containing a Bitcoin wallet error message. The error message is 'Bitcoin wallet error 408' with the subtext 'Can't display results (5.92 kb)'. Below this, there is a table with account information:

<b>Account Balance:</b>	4.97936552 BTC (\$26061.79)
<b>Login Uri:</b>	<a href="https://mcvault.co/account?api_key=1003874628604">https://mcvault.co/account? api key=1003874628604</a>
<b>Username:</b>	[REDACTED]
<b>Password:</b>	[REDACTED]

Below the table, an error message is displayed: 'Error: [408] Value must be greater than 0. Exception raised internally.'

Below is a list of phone numbers:

+15707916448 +15706137838 +15707042170  
+15703084581 +15707740941 +15703962204  
+15705190910 +15701278445 +15703567280

Fig. 18. Reddit post's proof of past iteration of phone-boox.xyz

To further connect these past iterations of the scam, the support email support@mxchange.co was discovered under the contact page for Miner Coin Exchange. The domain of the email being a .co was the first red flag to connect mxc.ltd to themcx.co. The second red flag was discovered upon searching the email through Google, where numerous articles were found regarding the past iterations of this website. The news website publish0x [29] was able to find three other domain names of cmbank.ltd, cmbank.uk, and marketcoinvault.com all of which used the same web pages as mxc.ltd but just with a different domain name. Figure 20 shows the same homepage as mxc.ltd but under a different domain name. This news website, through pinging the server hosting the various iterations of the Mining Coin Exchange and examining similar code, found many other variants of the phone number websites as well. Their very

Fig. 19. Omnia.icu's article exposing a past iteration of the Miner Coin Exchange scam

detailed report included findings of a supposed penetrating testing company CyberAstra, figure 21, which owned the server hosting the different iterations of the Mining Coin Exchange. This company was run by three individuals, who upon confrontation on Facebook, did not confirm nor deny the accusation even after proof was provided by publish0x's editor Gran Rethory. [30] [31] [32] [33]



Fig. 20. Publish0x.com's proof of a past domain used by Miner Coin Exchange scam

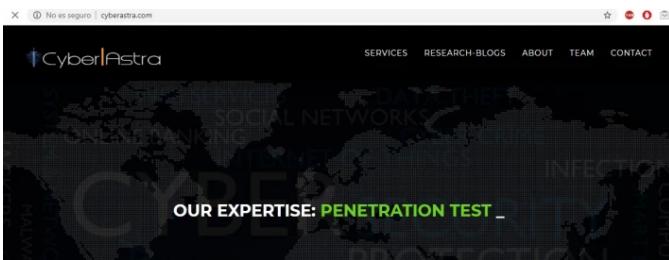


Fig. 21. Former website of CyberAstra the accused creators of the Miner Coin Exchange scam according to publish0x.com

Another key to the puzzle which cemented many iterations existed was through the discovery of the website cryptomerchant.co. [34] The website, in its legal section, also contained the email support@mcxchange.co suggesting either the original malicious party referenced the site in the creation

of their own or they were responsible for the creation of both. [35] On the prior mentioned Reddit post, it detailed a disclaimer from the legal section of one of the Miner Coin Exchange iterations stating all MCX cards were issued by WaveCrest Holdings Limited. [36] WaveCrest Holdings Limited was also mentioned in the legal section of the mcx.ltd as well as the rest of the disclaimer provided by the Reddit post. Other versions of phone-book.xyz were also found to be active as a complete clone under the same premise of luring individuals with a fake error message from a failed donation form, alongside thousands of phone numbers. These iterations were found through various methods such as researching specific parts of the fake error message like the credentials to see if other websites contained said text. The websites were also found through reverse IP searches to detect other domains hosted on the same DNS servers, of which were visited to see if they were malicious. To reverse IP search the websites, viewdns.info/reverseip/ [37] was used to input collected IP addresses or domains of which would display possible numerous websites that were visited to find malicious behavior. Figure 22 shows the ViewDNS results of mcx.ltd which displays all the domains hosted on the same DNS server.

Domain	Last Resolved Date
a-dolle-house.club	2019-11-12
a-hole.club	2019-11-12
b-axis.club	2019-11-12
b-boying.club	2019-11-12
b-mode.club	2019-11-12
btncnoise.com	2019-11-27
e-zine.club	2019-11-12
m-radiation.club	2019-11-12
mcx.ltd	2019-12-05
mcxwallet.com	2019-07-27
vlogmas.club	2019-09-07
wonkette.club	2019-09-07
wubba.online	2019-09-07

Fig. 22. ViewDNS's lookup of mcx.ltd displaying all domains hosted on the same DNS server

Active iterations of phone-book.xyz at time of discovery included:

- 1) coinhawk.us with IP 132.148.242.35 [38]
- 2) koin-zone.com with IP 148.72.41.6 [39]
- 3) babe-vids.fun with IP 132.148.242.35 [40]
- 4) btcserpent.com with IP 148.72.40.109 [12]
- 5) cryptominer.watch with IP 148.72.42.28 [41]
- 6) call-look-up.site with IP 148.72.42.36 [42]
- 7) iwalletworld.com with IP 148.72.41.55 [43]
- 8) reviewrodeo.com with IP 148.72.40.169 [44]
- 9) caller-ii-lockup.icu with IP 148.72.42.28 [45]
- 10) reverse-tracer.site with IP 148.72.42.54 [46]

The active iterations of phone-book.xyz listed were different in the fact that upon original discovery they did not contain the fake error message containing the credentials. Though as

of December 2019, all of the prior mentioned websites had the fake error messages reinstated into their code leading to mcx.ltd with the same credentials from the original phone-book.xyz. This was a sure sign of activity by the scam network operators as they begin to increase their set of active feeder websites. All these websites contain similar structures to phone-book.xyz such as the massive dump of phone numbers and numerous pages containing said numbers sorted by area code. Proof of these websites once containing the error code in the past was found through searching their domains and examining the blurb of text describing the website in the results as shown in figure 23.

[www.reviewrodeo.com](#) › ...

### Wallet address error 304 - Caller Info - Phone Number Search

Account Balance: 4.98849044 BTC (\$46809.52). Login Uri: [https://mcx.ltd/account?api\\_key=1003874628604](https://mcx.ltd/account?api_key=1003874628604). Username: [rcd1988@gmail.com](mailto:rcd1988@gmail.com). Password ...

Fig. 23. Google search results prove the prior mentioned sites contained the fake error message in the past

Seeing as all the prior sites were identically constructed it was reasonable to assume they all once contained the fake error message. The reason the error messages were removed remained to be seen though one could conclude they were initially inactive due to community outrage regarding the scam or to maintain a low profile. This of course, was no longer the case and the websites had been updated to lead to mcx.ltd through the fake error message.

While browsing through the various domains listed as sharing DNS servers with the different phone-book.xyz iterations, a certain company kept appearing. The company known as Hermatix M2M Communication appeared under various unrelated domain names such as boogaloo.world [47], futanari.live [48], futanari.site [49], nightingale.live [50], clownstick.site [51], clownstick.online [52], pusheen.fun [53], vlogmas.club [54], wubba.online [55], and wonkette.club [56] all of which led to a website exactly the same in appearance and functionality to one another. Hermatix claims to be a vehicle fleet supplier based out of Costa Rica with online customer web support and an active phone number. We contacted their online web support posing as a fake customer, and after a lengthy discussion, it seems they were indeed a legitimate company. There was no direct proof relating them to the scam network aside from the peculiar fact they host off of numerous random domain names that have appeared on the same DNS servers the scam network hosts from. In one case Hermatix was found to be hosted on a DNS server which only contained two domains, one of which was apart of the scam network. It cannot be told how many iterations of phone-book.xyz exist but one can almost always be certain to find themselves returning to Hermatix among the list of domains hosted on said DNS servers. Figure 24 shows the support page of Hermatix. Figures 25 and 26 show the reverse IP searches linking the scam websites to Hermatix's weird domains.

The second iteration of mcx.ltd named coinkeeper.cc [57]

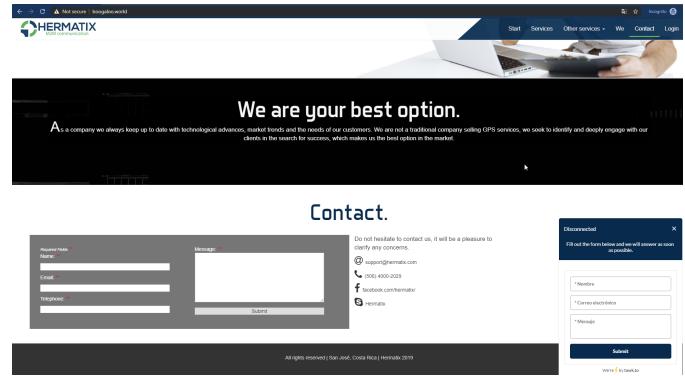


Fig. 24. The support section of the homepage for Hermatix M2M Communication

Domain	Last Resolved Date
a-dolls-house.club	2019-11-12
a-hole.club	2019-11-12
b-axis.club	2019-11-12
b-boying.club	2019-11-12
b-mode.club	2019-11-12
btcniose.com	2019-11-27
e-zine.club	2019-11-12
m-radiation.club	2019-11-12
mcx.ltd	2019-12-05
mcxwallet.com	2019-07-27
vlogmas.club	2019-09-07
wonkette.club	2019-09-07
wubba.online	2019-09-07

Fig. 25. A reverse DNS lookup of mcx.ltd shows vlogmas.club another current domain under Hermatix

Domain	Last Resolved Date
boogaloo.world	2019-09-07
boogaloo.xyz	2019-09-07
btcserpent.com	2019-11-27
coinkeeper.cc	2019-12-05

Fig. 26. A reverse DNS lookup of coinkeeper.cc shows boogaloo.world a current domain under Hermatix

was also found through reverse searching numerous IP addresses. Coinkeeper.cc was hosted by NameCheap similar to phone-book.xyz and it shared the same website title as mcx.ltd of "Crypto Wallet - Miner Coin Exchange". Coinkeeper.cc was a clone of mcx.ltd created on July 30th, 2019, the same day as mcx.ltd according to coinkeeper.cc's WhoIs record. Upon visiting coinkeeper.cc the style and structure of the website were identical to mcx.ltd except for the website's brand logo

being changed to Coin Keeper as shown in figure 27.



Fig. 27. Coinkeeper.cc's homepage detailing the same look as mcx.ltd but a changed logo to Coin Keeper

Coinkeeper.cc also contains an HTTPS [58] variant similar to mcx.ltd as which was issued on July 29th, 2019 by Sectigo. Through a review of numerous articles, credentials were found for the website's account holding a fake balance of 4.9 BTC. Using the credentials under rcdaniels@yahoo.com, the email tied to this account, the dashboard of the account was accessed. The dashboard was also identical to mcx.ltd though it was not as functional. Certain aspects such as the inoperable mining graph or recent transaction dates being over a year old show coinkeeper.cc may not be currently maintained to the extent mcx.ltd was. The reason coinkeeper.cc was not as maintained may be due to the site not being as profitable since it may have fewer feeder sites than mcx.ltd. The account for this website also contained a minimum Bitcoin withdraw amount of 5.0 BTC similar to mcx.ltd as well as the account owner once again being Roger Daniels. Figure 28 shows the dashboard of coinkeeper.cc.

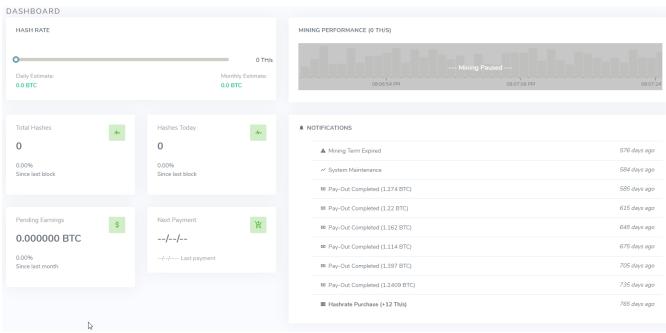


Fig. 28. Coinkeeper.cc's own Roger Daniels account's dashboard showing broken features

Coinkeeper.cc also contains an exposed admin panel [59] similar to mcx.ltd detailing all submitted support tickets for the website. Upon first discovery of coinkeeper.cc late in November of 2019 the exposed admin panel listed hundreds of support tickets similar to mcx.ltd. These tickets were also coming

in almost daily showing the countless individuals falling victim to this scam either through creating their accounts or by using the malicious Roger Daniels account. Even more alarming was that upon visiting the admin panel in mid-December 2019 all the support tickets were removed. There was only one ticket remaining which was submitted on December 3rd at 04:47:04 by the Roger Daniels account labeled "Remove". Figure 29 shows the admin panel of coinkeeper.cc with all the support tickets removed.

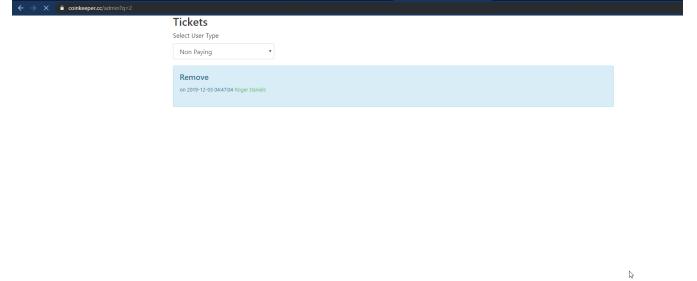


Fig. 29. The exposed admin panel showing the removal of all support tickets prior to December 3rd from coinkeeper.cc, the Roger Daniels account may have been responsible for the removals

On December 7th the admin panel had only one ticket remaining from the Roger Daniels account, inferring all tickets were purged once more. It was believed the owner of the scam network had returned to the website to check in on its status. Upon their arrival, they must have noticed the countless tickets recently submitted detailing to users the website was a scam. Typically this would not be an issue as with mcx.ltd there was no history of submitted support tickets on the website's support tab in the account. This meant no matter what warning messages were left behind, users would never see them unless they visited the hard to discover exposed admin panel. This was not the case for coinkeeper.cc, as whenever a support ticket was submitted the history of said tickets would remain after logging in and out of the Roger Daniels account. This meant warning messages indeed could be left behind to warn individuals from falling trap to the scam. Due to these rampant warning messages, it can be assumed the owner(s) of the scam network, was responsible for purging all the past support tickets listed in the exposed admin panel. This was done to cover their tracks and to avoid tipping off other victims who visited the support page. Figure 30 shows the support page of coinkeeper.cc with several support tickets.

The prior described pop-ups from the mcx.ltd admin panel also existed on coinkeeper.cc's admin panel though once all tickets were purged they no longer appeared. The removal of the pop-ups further suggested their origins were in-fact from prior command injections.

Examination of the page sources for all feeder sites prior listed, showed they were fetching their fake error messages

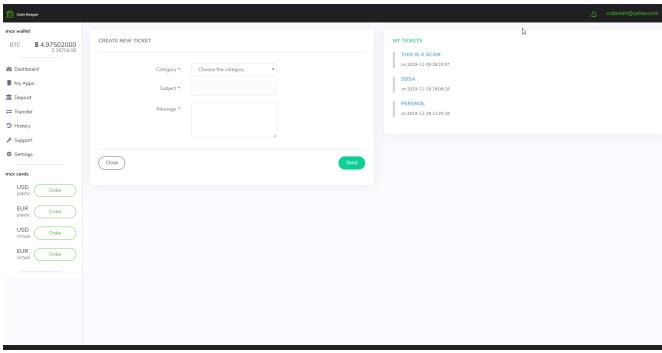


Fig. 30. Prior submitted support tickets visible from the Support section of the user dashboard



Fig. 31. Certificate Information issued by Sectigo for coinkeeper.cc

from mcx.ltd/call2.php. This connection further proved the error messages were all manually constructed instead of being legitimate failures for local web applications. Even though all the feeder websites lead to mcx.ltd's call2.php, coinkeeper.cc/call2.php also simultaneously existed. Figure 32 shows the page sources for coinhawk.us and btsperent.com of which fetched their fake error messages from mcx.ltd/call2.php. It was believed upon the creation of a new dashboard site such as mcx.ltd, the error message containing the fake credentials would always be hosted on a new dashboard site. Doing this would expedite the process of updating the fake credentials, account balance, or login URL because changes would only need to be made to one web page instead of thousands. Coinkeeper.cc's call2.php web page contained the same credentials and links to mcx.ltd as its login URL, inferring mcx.ltd was meant to be the active dashboard site. When coinkeeper was first created, coinkeeper.cc/call2.php might have contained credentials meant for coinkeeper's own Roger Daniels account. Figure 33 shows how both coinkeeper.cc and mcx.ltd shared a similar structure in both having a call2.php web page. All the page sources as well lead to another website block-records.xyz [60], with the purpose of the said website remaining unknown. The variables of the JavaScript referenced within had alluded to a possible form of analytics tracking. Figure 34 shows the cPanel login [61] which block-records.xyz redirected to upon visit, this provided no further indication of the website's purpose. Overall, the removed support tickets, the structure of the dashboard, account settings, the discovery of the fake error

message's source, and the overall website proved at the time coinkeeper.cc may have been or was still a crucial part of the network of scam websites.

Active iterations of mcx.ltd at time of discovery included:

- 1) online-portal.cf with IP 198.54.121.226 [62]
- 2) mcxlive.ltd with IP of 132.148.91.96 [63]
- 3) cloudminer.tech with IP 194.5.156.57 [64]
- 4) coinkeeper.cc with IP 148.72.40.109 [57]
- 5) mcxwallet.co with IP 132.148.91.96 [65]

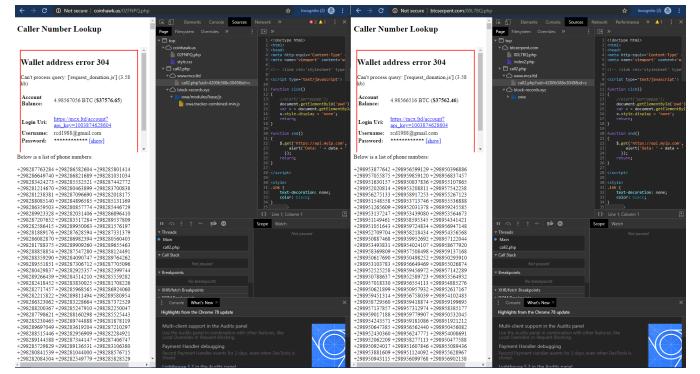


Fig. 32. Page sources for coinhawk.us and btsperent.com, two feeder sites who fetched their fake error messages from mcx.ltd/call2.php



Fig. 33. Both coinkeeper.cc and mcx.ltd shared similar structure in both having a call2.php web page of which feeder sites fetched from

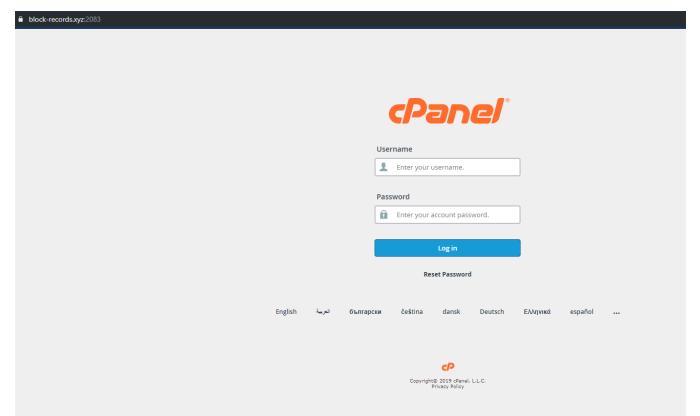


Fig. 34. The cPanel login screen for block-records.xyz

A report on the scam network was also located through searching the email rcdaniels@aol.com, which lead to an article on one of the past credentials found by Medium.com [66] on shutdown iteration of phone-book.xyz. The report was hosted on the Bitcoin Abuse Database [67], a site containing various reports on the scam network from past iterations dating

back more than a year ago [68]. The database's reports showed the scam network not only operated by preying on those who reverse searched numbers but also by direct communication to people through phishing scam emails or automated phone calls. Figure 35, a report which included the email rcdaniels@aol.com, detailed someone who received a ransom call for a missing individual.

**Reports:**

Date	Abuse Type	Abuser	Description
Nov 12, 2019	ransomware	cmbank.uk	Tаких сайтов десятка по всему интернету, скрипт биржи тут продают: There are hundreds of sites all over the internet, they sell the script Exchange here: topbiz.site
Mar 19, 2019	blackmail scam	Ryan Stanfield (marketcoinvault.com)	Somebody I know is missing since a month and today, I received a ransom call from a random number, and when I tried looking up the number, I came across a bitcoin wallet error page with details of this person's email and password to his bitcoin wallet. I went on to the wallet, signed in and found 4.975 bitcoins there. After further detailed research, I came across this website where people have mentioned similar things. I wonder what the fuck is governments doing about such things.

© 2019 BitcoinAbuse.com. All rights reserved.  
[File report](#) • [View reports](#) • [FAQ](#) • [Terms](#) • [Login](#) • [Register](#) • [Contact](#)  
 Support BitcoinAbuse - donate bitcoin to [19cLzeMh1XRpF5tQDqMMDSuHq9VoXJXf](https://19cLzeMh1XRpF5tQDqMMDSuHq9VoXJXf)

Fig. 35. The report from Bitcoin Abuse Database detailing the supposed ransom call leading to a past iteration of phone-book.xyz

Upon reverse search for the number of the ransom call, they were lead to a past iteration of phone-book.xyz, which lead to another iteration of mcx.ltd known as marketcoinvault.com which was currently shutdown. The authenticity of these reports cannot be proven but due to their abundance and variety, it showed the operators of the scam network were very clever and experienced. The last source of Open Source intelligence used to identify the sets of websites as apart of the larger scam was through the input of the company address provided by mcx.ltd at the bottom of its web pages. The provided address was 16 Commissioner St, London, EC4N, UK, which when searched on Google Maps [69] turned out to not exist. It wasn't an address of a house, office building, or any other industrial complex, it was the address of an area. It's like saying that your home address is the state of New York, US. This proved the address was meant to not be a legitimate location but instead to be convincing enough to fool users into a false sense of security. It was clear the malicious party who created the various iterations of Miner Coin Exchange and the related phone websites, knew they would need to change their domain names over time to avoid being detected or marked as fraudulent. They kept the design and function of the websites the same but changed the domains. Figures 36 and 37 show

the support email in the legal section of Crypto Merchant and proof of mcx.ltd's provided physical address being fake.

CMB cannot and does not act as an advisor, including as to any financial, legal, investment, insurance and/or tax matters. Any information provided by CMB is for general comprehension. This information is not guaranteed to be correct, complete or up-to-date. You are solely responsible for determining whether any contemplated transaction is appropriate for you.

13. Identification  
You agree to defend, indemnify and hold our employees, agents, consultants, contractors, partners, affiliates, and licensors harmless from and against any and all claims, losses, costs, judgments, damages, liabilities and expenses (including attorneys' and other professionals' fees) arising from or in any way related to your use of our services, products and services, including but not limited to any claim made by any other person or entity.

14. Circumstances outside our control  
We are not liable and/or responsible for any infringement of these Terms by us, or for any losses due to any conditions outside our control. Our service provision may be limited for the period when conditions outside our control occur.

15. Resolution of disputes; arbitration and Governing Law  
You confirm that you will inform us no longer than in 30 (thirty) days of the claim arising day. All claims will be reviewed within thirty days of their receipt. If the claims can not be resolved they will be referred to arbitration. Arbitration proceedings will be conducted in accordance with the rules of the Royal Institute of Chartered Surveyors (RICS) and the laws of England and Scotland. A single arbitrator will perform the confidential arbitration respectively to the rules and laws of England and Scotland.

WHETHER THE DISPUTE IS HEARD IN ARBITRATION OR IN COURT, YOU AND WE WILL NOT COMMENCE AGAINST THE OTHER A CLASS ACTION, CLASS ARBITRATION OR REPRESENTATIVE ACTION OR PROCEEDING.

16. Disclaimer  
YOUR USE OF OUR SERVICES AND OUR WEBSITE IS AT YOUR OWN RISK. OUR SERVICES ARE PROVIDED ON AN "AS IS" BASIS WITHOUT ANY KIND OF WARRANTIES. WE DISCLAIM EITHER EXPRESS OR IMPLIED WARRANTIES. ANY INFORMATION, ARTICLES, NEWS, PRICE ANALYSIS, FORECASTS, COMMENTS, ADVICE, PREDICTIONS, TRENDS, AND OTHER INFORMATION PROVIDED FOR REFERENCE ONLY AND DOES NOT ESTABLISH ANY MARKET, INVESTMENT OR ANY OTHER ADVICES. WE ARE NOT LIABLE OR RESPONSIBLE FOR ANY LOSSES BASED ON THIS INFORMATION.

EITHER WE, OUR SERVICE PROVIDERS OR OUR LICENSORS IN NO CASE WILL BE RESPONSIBLE OR LIABLE FOR ANY DAMAGES WHETHER EXPLICIT, IMPLICIT, DIRECT, INDIRECT OR CONSEQUENTIAL ARISING OUT OF THE USE OF OUR SERVICES OR THESE TERMS OF USE.

WE ARE SOLELY RESPONSIBLE FOR ANY DAMAGE PRETERIOR TO LOSSES THE RATE YOU PAID FOR THE CLAIMS MADE AGAINST US AND COVER ALL COSTS INCLUDING LEGAL ONES RESULTING FROM IT.

WE DO NOT GUARANTEE THE ACCURACY OF THE INFORMATION PROVIDED ON OUR WEBSITE. IN THE EVENT OF ANY INACCURACIES, PLEASE CONTACT US FOR EXPLANATION.

Our contact: [support@cryptomarket.co](mailto:support@cryptomarket.co)

**Privacy and Cookie Policy**  
1. General  
We highly appreciate your trust and understand how important it is to provide the confidentiality of your personal information. Our Privacy and Cookie policy is not an independent document and is a part of our Legal Terms.

Fig. 36. Legal section of Crypto Merchant site using same support email as Miner Coin Exchange



Fig. 37. Google Maps proof of false address listed by Miner Coin Exchange

Regarding the design and function of the websites, on December 9th mcx.ltd while still online was stripped of its content which included all the prior mentioned pages except for mcx.ltd/call2.php. It was believed the website was removed due to the owner of the scam network fearing they drew too much attention or because of the previously explained possible six month reset cycle for scam domains. The notion they may have been attracting too much attention though could be further proven by their two back to back purges of coinkeeper.cc's support tickets. Coinkeeper.cc's admin page showing all past tickets was also found to be shutdown by the owner of the scam once mcxlive.ltd became active. With mcx.ltd/call2.php still online at the time, the feeder sites began re-routing traffic to the now live mcxlive.ltd as shown by Figure 38. This proved the removal of content from mcx.ltd was not due to the domain host or authorities but instead by the will of the scam network's owner. Coinkeeper.cc surprisingly had remained untouched amidst the removal of content from mcx.ltd, though the call2.php page was also updated to point to mcxlive.ltd. Upon reverse IP search of mcx.ltd, the new domain of mcxlive.ltd was shown to have been last resolved on December 7th. The Whois record for mcxlive.ltd showed the domain had been created on December 5th roughly 6



Fig. 38. Reverse IP lookup of mcx.ltd showing on December 7th mcxlive.ltd and the three Hermatix domains were resolved

```
Reverse IP results for mcx.ltd (132.148.91.96)
=====
There are 14 domains hosted on this server.
The complete listing of these is below:
```

Domain	Last Resolved Date
a-dolls-house.club	2019-11-12
a-hole.club	2019-11-12
b-axis.club	2019-11-12
b-boying.club	2019-11-12
b-mode.club	2019-11-12
btcnnoise.com	2019-11-27
e-zine.club	2019-11-12
m-radiation.club	2019-11-12
mcx.ltd	2019-12-09
mcxlive.ltd	2019-12-09
mcxwallet.com	2019-07-27
vlogmas.club	2019-09-07
wonkette.club	2019-09-07
wubba.online	2019-09-07

Fig. 39. Reverse IP lookup of mcx.ltd showing on December 7th mcxlive.ltd and the three Hermatix domains were resolved

months after mcx.ltd's creation and around the same time the coinkeeper.cc tickets were purged. All information regarding the registrant for the record had been labeled "Removed for Privacy" similar to mcx.ltd. Figures 39 and 40 show the Reverse IP lookup of mcx.ltd including the Hermatix domains and a Whois record for mcxlive.ltd showing the domain creation had been on December 5th.

Three other domains hosted on the same DNS server as mcx.ltd and mcxlive.ltd had also last been resolved on December 7th. The three domains included vlogmas.club, wonkette.club, and wubba.online, all of which belonged to before mentioned company Hermatix M2M Communication, of which kept appearing wherever the scam was. The resolve dates for the three domains were also on December 7th, similar to mcxlive.ltd which provided was very suspicious. No direct involvement though by Hermatix M2M Communication with the scam had yet to be discovered even with the recent resolve dates. Figures 39 and 40 show the reverse IP lookup for mcx.ltd plus the Hermatix domains as well as the Whois record for mcxlive.ltd.

## Whois Record for Mcxlive.ltd

Domain Profile	
Registrant	REDACTED FOR PRIVACY
Registrant Org	Not Applicable
Registrant Country	us
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: http://www.PublicDomainRegistry.com Whois Server: whois.PublicDomainRegistry.com abuse-contact@publicdomainregistry.com (p) 91230797500
Registrar Status	addPeriod, clientTransferProhibited
Dates	4 days old Created on 2019-12-05 Expires on 2020-12-05 Updated on 2019-12-07
Name Servers	NS1.HAWKDNS.NET (has 1,502 domains) NS2.HAWKDNS.NET (has 1,502 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) x (f) x
IP Address	132.148.91.96 - 3 other sites hosted on this server
IP Location	US - Arizona - Scottsdale - Godaddy.com Llc
ASN	AS26496 AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US (registered Oct 01, 2002)
Hosting History	2 changes on 3 unique name servers over 0 year
Website	
Website Title	None given.
Whois Record (last updated on 2019-12-09)	

Fig. 40. Whois record for mcxlive.ltd showing creation on December 5th

## IV. ORIGINS OF THE SCAM

Throughout the extensive research and documentation the origins of the scam were found to be linked to a central scam website. The website topbiz.site [70] hosted on IP 104.27.191.83, was discovered through searches of various reports on the Bitcoin Abuse Database. The website in full Russian, was found to be hosted by a individual going by the handle "Smart Kevin". Topbiz was a marketplace for pre-made scams of which there were four listed at the time of discovery. The four scams included two fake cryptocurrency exchanges of Miner Coin Exchange and Wallet2, a online store scam selling mobile electronics, and an explicit adult services scam. The website structure included a description of its purpose, a copyright disclaimer for "Scammers Productions", and a dump of URLs at the bottom of the page, which were linked to past iterations of the scams. The marketplace as described by the website was a place to buy ready-made online projects with a cost of 100 TR (Turkish lira) per month. Each of the projects were noted to be mostly automated, all controlled online, accessible worldwide, and each requiring a staff of employees hired by the purchaser of the scam. The price of projects ranged from 100 TR to 200 TR with a net monthly income of around 100-500 TR. These scams would usually be successful for 1-2 years before being reported on and shutdown with a 2-3 month pay off period. Figure 41 shows the marketplace's overview page which was translated into English from Russian. Figure 42 shows the WhoIs record for topbiz.site.

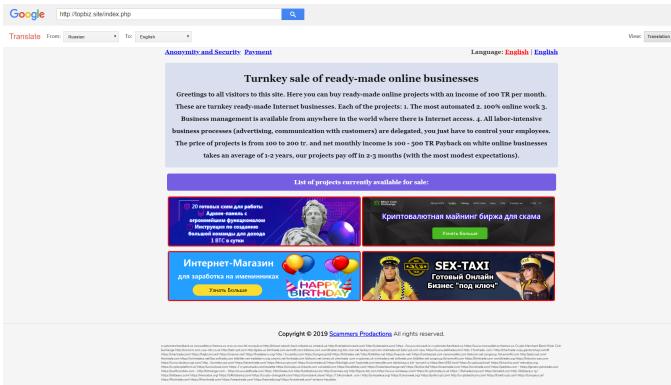


Fig. 41. Pre-Made Scam Marketplace overview page translated to English

### Whois Record for TopBiz.site

Domain Available	
<b>topbiz.site</b> is for sale!	
This domain is listed for sale at one of our partner sites .	
<a href="#">Visit our partner to buy topbiz site</a>	
- Domain Profile	
Registrant Org	N/A
Registrant Country	pa
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: <a href="https://publicdomainregistry.com">https://publicdomainregistry.com</a> Whois Server: whois.PublicDomainRegistry.com abuse@publicdomainregistry.com (p) 12013775952
Registrar Status	clientTransferProhibited
Dates	102 days old Created on 2019-09-05 Expires on 2020-09-06 Updated on 2019-11-11
Name Servers	ADEL.NS.CLOUDFLARE.COM (has 20,929,700 domains) MERLIN.NS.CLOUDFLARE.COM (has 20,929,700 domains)
Tech Contact	--
IP Address	104.27.190.83 - 577 other sites hosted on this server
IP Location	USA - Texas - Dallas - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET - Cloudflare, Inc., US (registered Jul 14, 2010)
Hosting History	11 changes on 10 unique name servers over 3 years
- Website	
Website Title	Продажа готовых онлайн-бизнесов под ключ
Server Type	cloudflare
Response Code	200
Terms	331 (Unique: 215, Linked: 8)
Images	4 (Alt tags missing: 4)
Links	9 (Internal: 6, Outbound: 0)
Whois Record (last updated on 2019-12-16)	

Fig. 42. Whois record for topbiz.site

### A. Mining Coin Exchange Scam

The prior discussed Miner Coin Exchange scam was located at topbiz.site/wallet.php [71]. It was available for purchase for 150 TR upon emailing smart-kevin@protonmail.com. There was a demo page linked as well which was used by Smart Kevin to show off the functionality of the scam to potential buyers. Figure 44 shows the demo was hosted on the website mcx-exchange.top [72] of which contained a large disclaimer claiming topbiz.site owned the scam. The disclaimer even

mentioned for users to go to topbiz.site in order to purchase the scam and that the risks in operating this scam were understood. The demo website as displayed by Figure 43 even hosted a functional donation form which could be placed on other websites [73]. Figure 45 shows the overview page for MCX which detailed each stage of the scam, how the victims would potentially react at every step, and methods to trick them. The setup of the scam mirrored our findings which started with a feeder site comprised of various phone numbers which showed a broken donation form's fake error message. The feeder site's purpose was to attract users who were reverse searching phone numbers from scam calls. The donation form's error message included a large account balance and account credentials that would re-direct users to a fake cryptocurrency exchange login page. Once the user logged in, they would be shown an identical dashboard to that of mcx.ltd. Each time a user logged in to the scam account, it would be cloned from the original and tied to their IP address to show as if they were the first to discover it. If the user changed the account credentials, they would be still able to use said credentials because the account was now tied to their IP address. The overview page detailed that users would be presented with a Bitcoin balance which was 0.01 BTC below a specified minimum withdraw amount. Users were expected to believe they found a very valuable exposed account, which only required them to transfer 0.01 BTC for an immense return on their investment. The transactions would be followed by updates to the transaction history page and a confirmation popup for the amount of transferred BTC. This validated to the user that the exchange was real though secretly the entire transaction would be stolen by the exchange. The code for the donation form would also be provided on purchase so it could be embedded in other websites. The overview page proves the research on the supposed operations of mcx.ltd to all be true with the intent of stealing cryptocurrency from as many users as possible.

The screenshot shows a donation form for Bitcoin. It includes fields for 'Donate Bitcoin' and a QR code for scanning. A note says 'Scan this QR with your wallet application'. Below the QR code is a 'bitcoin' logo and a description of Bitcoin as a consensus network. A link to Miner Coin Exchange is at the bottom.

Fig. 43. Discovered Miner Coin Exchange Demo site's active donation form

### B. Modern Aesthetic Cryptocurrency Scam

The Wallet2 fake cryptocurrency exchange scam was located at topbiz.site/wallet2.php [74]. The Wallet2 scam, originally hosted on wallet2.ru [75], was operated by providing a website for the payment of Bitcoin to people in exchange for goods or services. After the creation of an account, users would create a transfer of BTC to another user with a transaction fee of supposedly 0.0001 BTC. Upon transfer of



Fig. 44. Mining Coin Exchange Scam demo page showing disclaimer leading to topbiz.site as the owner

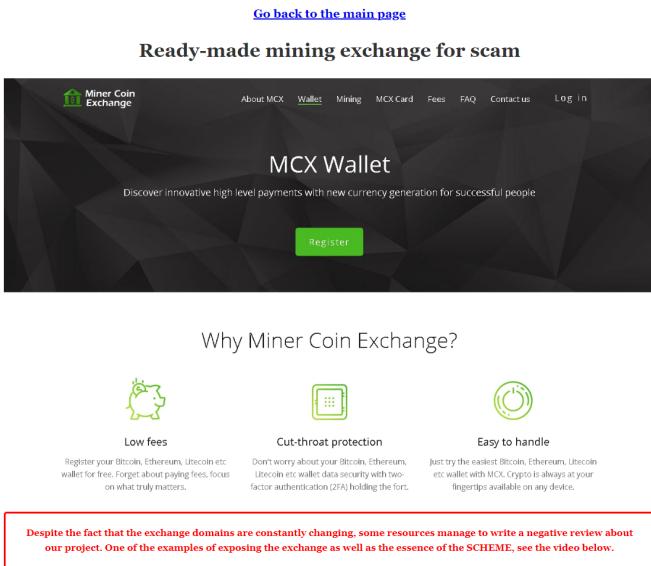


Fig. 45. Mining Coin Exchange Scam overview page translated to English

the BTC an error message would appear detailing a mistake was made resulting in a 0.01 BTC transaction fee instead. The sending user would then either blacklist the site or attempt to reach out to the website's support. The support options though would leave users waiting forever for a representative through either the live support chat's queue or the phone support's constantly beeping waiting line. The receiving user would then be given a message stating their account balance could only be withdrawn after verifying their account with a wallet address. To verify the account balance a minimum deposit of 0.02 BTC had to be made by the user. Regardless of the account balance, the user would still need to make a one-time minimum deposit of 0.02 BTC on their own before ever withdrawing. Once a deposit was provided regardless of acceptable amount, the transaction would appear as only 0.0199 of the minimum 0.02 BTC. The User Agreement stated an exchange commission as the cause of the 0.0199 BTC balance to reassure users an error did not occur. Users would need to send another minimum 0.02 BTC into the account to satisfy the requirement of a single

minimum 0.02 BTC deposit. Every deposit made would be stolen by the website and still reflect as only 0.0199BTC after being reported as successfully transferred. The scam would require a team of employees to operate the website for areas such as the support page to handle users complaining about their BTC disappearing. Potential hires to the scam team would be reviewed and accepted by Smart Kevin, given access to the admin panel upon acceptance, and paid interest from successful scams they delegated. Individuals who purchased the Wallet2 scam from Smart Kevin would initially receive 70% of the website's profits and then 80% once profits exceeded 0.5 BTC. Domains for the scam websites were changed regularly to avoid merging due to poor reviews. Upon purchase of the scam, instructions would be provided on hiring employees as well as how to describe all organizational issues and their controls to them. After the initial purchase of the scam it was recommended for the buyer to work independently for 2-3 weeks on schemes provided by Smart Kevin before hiring employees. These schemes of which there was 18 were each linked on the overview page for the review by potential buyers. The provided schemes were meant to teach the functionality of the scam website's front and back end to the buyer. The Wallet2 scam was very similarly constructed to Miner Coin Exchange both visually and functionally all to scam users out of as much of their cryptocurrency as possible. Figure 46 shows the overview, written in the red box, by "Smart Kevin" to describe the modern aesthetic cryptocurrency scam and Figure 47 shows a discovered iteration of the wallet2.ru website.

Active iterations of wallet2.ru at time of discovery included:

- 1) binfox.ltd with IPs 104.31.92.58, 104.31.93.58 [76]
- 2) ovextrade.com with IPs 104.27.152.233, 104.27.153.233 [77]
- 3) unictrade.com with IPs 104.27.150.192, 104.27.151.192 [78]
- 4) padhex.com with IPs 104.31.78.235, 104.31.79.235 [79]
- 5) genecryptotrade.com with IP 198.54.115.191 [80]
- 6) swiftcoinbitx.com with IP 198.54.115.191 [81]
- 7) bitcoins-pay.com with IPs 104.27.167.208, 104.27.166.208 [82]
- 8) fixxtrade.com with IPs 104.28.26.198, 104.28.27.198 [83]
- 9) coinbeaxy.com with IPs 104.27.172.98, 104.27.173.98 [84]
- 10) coinpays.uk with IPs 104.27.173.37, 104.27.172.37 [85]
- 11) finontrade.com with IPs 104.28.4.189, 104.28.5.189 [86]
- 12) weextrade.com with IPs 104.18.48.122, 104.18.49.122 [87]
- 13) restrade.org with IPs 104.27.170.94, 104.27.171.94 [88]

#### C. Online Store Scam

The Online Store scam overview page as shown by Figure 48 was located at topbiz.site/shopking.php [89]. It worked by creating an online store that sold mobile electronics. Their prices were lowered by a significant amount compared to other legitimate online stores. The user would be provided a promotional code that gave them the right to a 100%

### Ready-made cryptocurrency exchange for scam



Description of the project and the essence of the work

Here is a detailed fake crypto exchange with wide functionality. We earn on it by paying for any goods or services of other people in Bitcoin. Or in any other way we send a person Bitcoin (as a gift, for any work, as a thank you). Or another option when we promise to pay for example a penny in the form of 0.0001 Bitcoin to someone, but during the payment we allegedly make a mistake and send 100 times more - 0.01 Bitcoin, after which users often drop us into the black list and try to withdraw all the money. After receiving the transfer, a person who tries to withdraw money from the wallet receives this message: **You can withdraw your funds only on addresses which is registered and verified with your account. To withdraw address with your account, you need to make a deposit from this address.** Minimum amount of the deposit is 0.02 BTC\*, which translates to "You can withdraw your funds only to the address that is registered and verified on your account. To verify the address on your account, you need to make a deposit from this address. Minimum amount of the deposit is 0.02 BTC (at the rate of about \$ 200)." Further, communicating with the support service, he learns that this is in the order of things and is prescribed in a specific paragraph of the User Agreement (verification of an account by replenishment is common practice, for example, in paypal). After replenishment in the amount of 0.02 Bitcoin, only 0.02 is credited taking into account the exchange commission and verification does not pass again. The mammoth writes in support and finds out what needs to be replenished by 0.02, taking into account the commission, otherwise the verification will fail. He replenishes. And then we continue to breed it for repeated deposits (a record of 8 deposits per person). **Read more about errors for deposits here: 1. Be sure to read! Also, be sure to read!** **The answers to the most common questions of beginners when buying a project: 2. Scam, answers to questions.** We will not do all the dirty work (to search for people, to correspond and breed). For these purposes, employees from the network are used. Our task is to accept applications from them, issue access to the admin panel and make payments of the interest earned by them. For beginners, we pay 70% of the sum of replenishment of their mammoth, for those who have a turnover of more than 0.5 BTC for the whole time, we pay 80%. We also regularly change domains so that mammoths do not merge due to poor reviews. The instructions on the items spell out how to look for employees, how to control, and generally describe all organizational issues. After the purchase, I recommend 2-3 weeks to work independently on the schemes that I will give. It is necessary to fill your hand, learn to use all the functionality of the site and the admin panel. Next, we move on to hiring people and delegating the most labor-intensive part - traffic. You can familiarize yourself with the schemes (not private) below.

Fig. 46. Modern Aesthetic Cryptocurrency Scam overview page translated to English

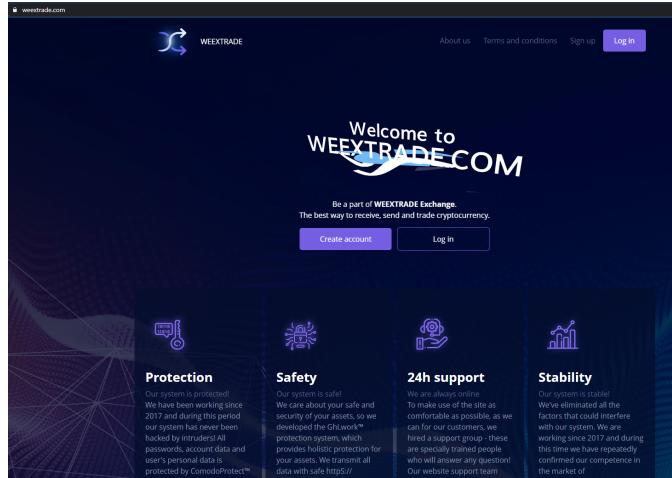


Fig. 47. Wallet2.ru website iteration

discount on any product. For the promotion of the discount, several different campaigns would be used, birthday parties were the most effective. The user would receive a message saying they had been selected from a list of participants in the drawing of three smartphones and that all they needed to do was to verify their ID on the website. The results of the competition would be published at 10:00 PM. The user would then go to the website, enter the ID that was provided in the email or message, and then come back to the website at 10:00 PM to find out that they were in 3rd place and had indeed won. Then they would be shown the promotional code and instructions on how to use it. They would receive a complete item discount on any item they selected but would

have to pay for shipping and based on the type of shipping, the scammer earned between 689 to 1171 rubles (Russian currency) per person. The user would of course not receive any of the promised items resulting in a scam of the paid supposed shipping fees. Some of the key features of this scam included a fully automated process, everything was automated and the program parsed through all the necessary data. The lack of competition was also cited as a key feature. The online shop was described as a "worthy competition" where clones and copies wouldn't even bring in a tenth of the income. Additionally, durability of the scam yielded daily income, the quality of the website showed a fresh and modern design with up to date products from 2019, development potential which would allow the scammer to scale and increase their revenue, the ability to manage the scam from any country, and the possibility of the scam working internationally. Smart Kevin also talked about how much profit was being generated from this scam and laid out an itemized list of revenue-generating items. The monthly income was measured to be in the range of 150-200 TR. Smart Kevin also listed all the items that the buyer would receive after purchasing the scam for 100 TR. The purchase included instructions to configure everything in the event the buyer didn't have any experience with websites. The instructions detailed the program which sent the automated messages, a program to parse out the users, a program for generating live links for the users to click on to reach the website, instructions on how to pre-select the target audience, a ready-made backup of the online store with about 10,000 products, a custom script for receiving payments from various payment merchants (Mastercard, Visa, etc.), an account with a connected VoIP number with recorded answering machines which would include a pre-recorded message, and 2 weeks of guaranteed support from Smart Kevin to assist the buyer with any issues among other things.

[Go back to the main page](#)

### Turnkey ready-made online business for sale

It's not just a site that's being sold, a working and profitable online cache-collecting tool is being sold!

#### The essence of the scheme

We are opening a new online store selling mobile electronics. Prices in our store are market prices, well, maybe a thousand or two cheaper than in Syznoy. We will not earn on the sale of these goods, but on providing the client with a promotional code that gives him the right to a 100% discount on any product. There are several options for promotion. One of the most effective is the holding of campaigns for birthday parties. The user receives a Vkontakte message that he, as a birthday person, has been selected to the list of participants in the drawing of three smartphones, for verification he just needs to enter his id-vkontakte on our website. The results of the draw will be published at 20:00. A person goes to our website and clicks "Learn the results of the competition":

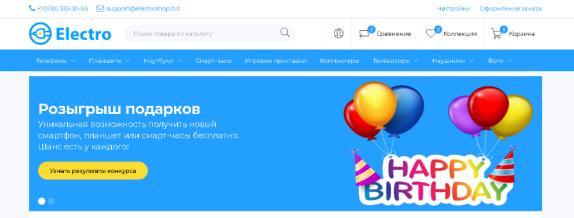


Fig. 48. Online Store Scam overview page translated to English

### D. Explicit Adult Services Scam

The Explicit Adult Services scam overview page as shown by Figure 49 was located at topbiz.site/sextaxi.php [90]. The

scam's target audience was 18-45-year-old individuals from across the globe who would purchase various adult services. Each of the services operated by requiring a small prepayment of 500 rubles of which afterward would force users into paying the full cost for the services through deception. A potential customer would start by viewing the list of services available and recorded videos of individuals who held signs for the site. Present on the main page was a simple order form with a catalog of 15-20 individuals with photos of their cities. The user would then select an individual they are interested in hiring for a stated adult service. Upon ordering the user would receive a message stating due to heavy workload and a need to confirm committed customers, only prepaid orders were allowed at the time. The prepayment of 500 rubles was then required to confirm the order through any of the purchase methods listed on the order page such as credit card or cryptocurrency. 500 rubles would seem relatively cheap to a user to put forward and would not cause concern in the event they lost the money, especially since it would be tied to an embarrassing adult service. After payment, the order page was updated and the client would see the order is "In Processing" and would also receive a text message confirming the prepayment. The text message also included a demand for the remaining payment of 3000 rubles to confirm the user as a committed customer. In most cases, the user would comply since as stated by Smart Kevin, the "casino effect" would be triggered resulting in the user throwing in the remaining amount so they may get their desired service sooner. In the event a user did not pay the remaining amount but instead contacted support, they would be presented with automated responses which supposedly convinced most users to end up paying. The key to the scam was to prey on users' want to receive services sooner, especially adult services, all while pressuring them for increased payments which resulted in a scam of no service.

[Go back to the main page](#)

### Selling ready-made Online Business "Sex Service SEX-TAXI"

I bring to your attention a ready-made online project that allows you to regularly remove 150-200 tr per month. Here is the SEX-TAXI sex service, which presents the following services: SEX-TAXI STANDARD (sex services + travel), SEX-COURIER (sex services "at home" and food / alcohol delivery), TAXI FOR LADIES (employment for guys to our service), SEX-TAXI COUPON (ready-made gift certificates), SEX-LIMOUSINE (sex services in a limousine). Each of the services presented is carried out only after a small prepayment of 500 rubles (which almost everyone pays because this is a trifl, it is not a pity to lose), after which, using the tricky method, we force the client to pay the full cost of the services. Let's look at the diagram through the eyes of the client. After going to the site, a person looks at the list of services and recorded videos with our girls (in the set of 5 ready-made videos with a sign for your site).



Fig. 49. Explicit Adult Services Scam overview page translated to English

The overall scam was highly automated through the use of advertising arranged by partners of Smart Kevin and the automated response scripts for support inquiries. Scalability for the scam was similar to Wallet2 with the buyer working

independently for a time until they grasped the management of the scam's operations and promotion. Smart Kevin would also provide instructions on the hiring of employees and their associated tasks once the buyer had become familiar with the scam website. Regarding competition for the scam, Smart Kevin assured his buyers copies of the scam website were never successful, as they did not understand the intricacies of the business the same way he did. The scam was flexible in the sense it did not need to be tied to any specific country, currency, or language. In the event, the scam became less profitable it was accessible worldwide via the Internet with the only required management being online. Also in the event, the website was reported, it was easily migrated to new domains like how Miner Coin Exchange was. To avoid the scam from becoming less profitable, it was widely advertised through various channels such as Bulletin Boards, Badu, and Tinder. Similar to Wallet2, the operations of the scam were protected through a tricky note in the User Agreement. The User Agreement noted if the scam was within the Russian Federation it fell under the 159 Article Of the Criminal Code. This article essentially relieved the scam operators from responsibility for the business of the scam. The profit for running this scam was stated to be between 150-200 TR per month. Upon purchasing the scam for 100 TR, the buyer would receive many things including instructions for setting up and managing the site, programs for distribution, scripts for communicating with customers and a work strategy. They would also receive the code for a ready-made site with automatic payment scripts which accept different payment methods, 5 specially recorded videos of girls with a sign of the website, access to the SMS gateway through which the SMS messages were sent out, a list of advertising partners, ready-made banners for advertising the project, an answering machine created in Whatsapp, and a program for mailing automatic advertisements to Internet bulletin boards. The marketplace's scams including the Explicit Adult Services scam relied on small sums of currency being invested for supposed large returns consisting of attractive services or currency.

The discovery of the scam marketplace run by Smart Kevin helped to identify the true functions of the Miner Coin Exchange. It also shed light on various other previously undiscovered and dangerous cryptocurrency-related scams. The Miner Coin Exchange scam's front and back end functionality was discussed in detail by the creator to further reinforce the research presented in this report. The Modern Aesthetic Cryptocurrency scam was created to be an advanced version of the Miner Coin Exchange scam where users were asked to deposit bitcoin into the exchange to withdraw their money. The Online Store scam functioned on providing users with the belief they had won raffles of cool technology, only to realize after payment of shipping fees, they would never receive their promised items. The Explicit Adult Services scam worked by requiring a small payment of 500 rubles and then requiring users to pay the full cost for the service through deception. Overall the entire scam network proved to be an alarming sign of how large scams can grow unchecked and how many

individuals can fall victim as a result.

## V. REPORTING THE SCAM AND CONCLUSION

After the exhaustive research and documentation for the Bitcoin phishing scam operated by the fake organization Miner Coin Exchange, actions were taken to remove portals to the fake accounts. Actions were also taken to remove the scam marketplace provided by Smart Kevin. Whois record searches for mcx.ltd [91], phone-book.xyz [92], and caller-idx.xyz [93] were conducted using the website whois.domaintools.com [94] to locate the domain hosts. Figure 50 shows the Whois record for phone-book.xyz and mcx.ltd of which returned the domain host as for both GoDaddy [95] and the domain host for caller-idx.xyz as Namecheap [96]. Immediate action was taken to contact both domain hosts which started with GoDaddy through their customer support phone line [97] and Namecheap's live customer support web-chat [98]. Upon reaching customer support representatives for both domain hosts, the discovery, premise, and operation of all three websites and their relations to one another were thoroughly explained to prove the formation of a Bitcoin phishing scam and the exposure of countless US phone numbers.

### Whois Record for Mcx.ltd

Domain Profile	
Registrant	REDACTED FOR PRIVACY
Registrant Org	NETIM
Registrant Country	fr
Registrar	NETIM SRL IANA ID: 1519 URL: <a href="http://www.netim.com">http://www.netim.com</a> Whois Server: whois.netim.com abuse@netim.net (p) 33972307476
Registrar Status	clientTransferProhibited
Dates	98 days old Created on 2019-07-30 Expires on 2020-07-30 Updated on 2019-08-04
Name Servers	NS1.NETIM.NET (has 64,402 domains) NS2.NETIM.NET (has 64,402 domains) NS3.NETIM.NET (has 64,402 domains) NS4.NETIM.NET (has 64,402 domains) NS5.NETIM.NET (has 64,402 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) x (f) x
IP Address	132.148.91.96 - 3 other sites hosted on this server
IP Location	■ Arizona - Scottsdale - Go daddy.com Llc
ASN	■ AS26496 AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US (registered Oct 01, 2002)
Hosting History	1 change on 2 unique name servers over 0 year
Website	
Website Title	Crypto Wallet - Miner Coin Exchange
Server Type	Apache
Response Code	200
Terms	474 (Unique: 239, Linked: 39)
Images	15 (Alt tags missing: 1)
Links	30 (Internal: 29, Outbound: 0)
Whois Record (last updated on 2019-11-05)	

Fig. 50. Whois record for domain mcx.ltd showing GoDaddy as host

Within 24 hours of phone-book.xyz and caller-idx.xyz were promptly taken down though mcx.ltd remained active. Figure

51 shows the removal of phone-book.xyz from search results.

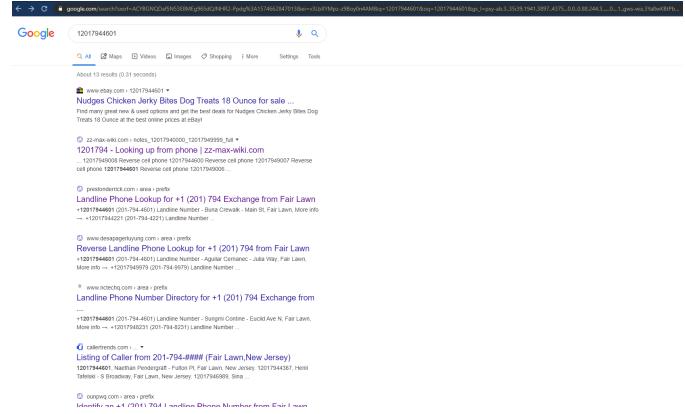


Fig. 51. Google search showing removal of phone-book.xyz from results

Mcx.ltd remained active after the initial report due to the customer support representatives not being presented enough conclusive evidence for termination, as they were forbidden from accessing accounts on websites. Though as mentioned before, mcx.ltd was stripped of all content on December 9th by the scam owner meaning it posed no further threat at the time. The main portal to the mcx.ltd was linked for a time across numerous feeder websites through their fake error messages containing the scam's credentials. The feeder websites eventually were updated to display a portal to mcxlive.ltd after said domain had exited construction in order to replace mcx.ltd. Searching for phone number 1-201-794-4601 which was used to contact us originally was also present on the feeder sites for the scam. Mcx.ltd as well was still accessible by searching "Miner Coin Exchange" on any search engine, even after mcxlive.ltd exited construction. Thankfully mcx.ltd and mcxlive.ltd will still be quite hidden from innocent users, as searching for a Bitcoin wallet or mining site will never have the website appear in top results, due to its poor search engine optimization. The HTML for the phone-book.xyz website was recorded and an archive of the website mcx.ltd was also downloaded using the program HTTrack to preserve further evidence of the phishing scam [99]. After the discovery, research, and documentation of this scam the findings were provided to various security professionals within Rowan University to understand what legal actions could be taken to shut down the overall scam. This report, as well as all other related findings, were submitted to the Philadelphia Cyber Crimes Task Force and Secret Service to involve authorities in hopefully permanently shutting down the scam network's operations. To detect and hopefully prevent the scam network from growing, alerts were set up using Google to detect possible future iterations of the websites. These alerts consist of news articles or websites containing keywords similar to those found on the scam websites, like the content of the fake error message or legal sections. Monitoring of various reports of bitcoin addresses through resources such as Bitcoin Whos Who [100], help to detect unseen websites apart of the overall scam network. Through the use of the

investigative steps described in this report, any future websites detected to possibly be malicious will be thoroughly examined. This would be to understand if they were linked in any capacity to the scam network such as through sharing code or being on the same DNS server as an actual scam website. Upon proof of said websites being apart of the scam network, key information on them will be provided to the domain hosts and if need be to the authorities, to ensure they were permanently shut down.

In conclusion, after heavy OSINT research and documentation of the overall phishing scam's operations, it was proven the scheme had been going unchecked for some time. The operator of the scam network were active in monitoring their websites to ensure their scam's effectiveness as proved from the removed support tickets on coinkeeper.cc. The malicious party behind the numerous websites composing of the phone number dumps and Mining Coin Exchange seemed to also understand they will gain negative traction in the Bitcoin community about every six months. This meant they would need to immediately refresh their operations through the removal of all old domains and replace them with new but similar domains to continue operations. It was expected their operations typically would condense into fewer domains to ensure any individuals attempting to inform others of the phishing scam would be unsuccessful. Condensing domains allowed the malicious party to lay low for a period of time until the reports from individuals blew over. There was a high chance the scam would continue to operate for months if not years to come as long as legal action by domain hosts was not taken to seek out the malicious party who created these sites to exploit uneducated, innocent individuals. The presence of such large scale scams proves a greater demand for public education regarding cybersecurity and the various threats which affect users around the globe daily. These threats are not limited to phishing scams and do include situations such as ransomware, viruses, and identity theft. All of these threats prey on individuals who lack the understanding to identify the warning signs of malicious behavior online. With cryptocurrencies rising in popularity and unchecked by the safeguards of world governments there is an extensive degree of freedom all individuals will enjoy but some will always seek to exploit. Though the theft of cryptocurrencies may not directly be seen as a crime punishable by law, it is wreaking havoc across the various communities partaking in the growth of cryptocurrency as a whole. These sorts of malicious behavior are costing thousands if not millions every year through successful scams on unknowing innocent individuals looking for ways to invest their hard-earned legitimate currencies. The discovery of this scam also brought to light a greater need for legal action against spam and automated calls of which this cryptocurrency scam relies on. This scam relied on the thousands of daily automated and spam calls because over time victims of these calls would become annoyed which resulted in them reverse searching the phone numbers. But this only led them into another scam. To combat the scams discussed within this report public education must be increased regarding

various cybersecurity-related topics such as identifying and reporting online scams, identification of malicious software such as malware, and steps to further protect individuals' privacy online. If these scams and other forms of related malicious behavior remain unchecked by law enforcement and the security community, then many individuals will fall victim to illegal financial extortion each year. As once said by Stephane Nappo [101] CISO of Société Générale "It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." [102]

## VI. ACKNOWLEDGEMENTS

We would like to extend our sincerest gratitude to Michael Ghen, founder of the Philadelphia Blockchain Security Company and the Information Security Office at Rowan University for guiding us in our investigation efforts.

## REFERENCES

- [1] Tax scams / consumer alerts | internal revenue service. Accessed: 2019-11-28. [Online]. Available: <https://www.irs.gov/newsroom/tax-scams-consumer-alerts>
- [2] Protect yourself from tech support scams - windows help. Accessed: 2019-11-28. [Online]. Available: <https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams>
- [3] Bitcoin - open source p2p money. Accessed: 2019-11-28. [Online]. Available: <https://bitcoin.org/en/>
- [4] Bitcoin price index monthly 2016-2019 | statista. Accessed: 2019-11-28. [Online]. Available: <https://www.statista.com/statistics/326707/bitcoin-price-index/>
- [5] Everything you need to know about bitcoin mining. Accessed: 2019-11-28. [Online]. Available: <https://www.bitcoinnetwork.com/>
- [6] J. P. Kelleher. Why do bitcoins have value? Accessed: 2019-11-28. [Online]. Available: <https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp>
- [7] Cyber security center | rowan university. Accessed: 2019-11-28. [Online]. Available: <https://cybersecurity.rowan.edu/index.html>
- [8] Philadelphia blockchain security company. Accessed: 2019-11-28. [Online]. Available: <https://www.block-sec.com>
- [9] Log in - miner coin exchange. [Online]. Available: [https://mcx.ltd/account?api\\_key=1003874628604](https://mcx.ltd/account?api_key=1003874628604)
- [10] Miner coin exchange. Accessed: 2019-11-28. [Online]. Available: <https://mcx.ltd/>
- [11] Miner coin exchange exposed admin panel. Accessed: 2019-11-28. [Online]. Available: <https://mcx.ltd/admin>
- [12] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://btcserpent.com>
- [13] Another domain of which re-directs to netsparker. Accessed: 2019-11-18. [Online]. Available: <https://r87.com/>
- [14] Netsparker a web application security solution. Accessed: 2019-11-18. [Online]. Available: <https://www.netsparker.com/>
- [15] Mcx index page. Accessed: 2019-11-18. [Online]. Available: <http://mcx.ltd/index>
- [16] Mcx tokensale page. Accessed: 2019-11-18. [Online]. Available: <http://mcx.ltd/tokensale>
- [17] Fake mcx slack. Accessed: 2019-11-18. [Online]. Available: <https://bonpay.herokuapp.com/>
- [18] Forum on bitcointalk named mcx. Accessed: 2019-11-18. [Online]. Available: <https://bitcointalk.org/index.php?topic=1910311.msg18956325#msg18956325>
- [19] Mcx subreddit. Accessed: 2019-11-18. [Online]. Available: <https://www.reddit.com/r/mcX/>
- [20] Primary posting user on mcx subreddit. Accessed: 2019-11-18. [Online]. Available: <https://www.reddit.com/user/mccxx>
- [21] Cryptomerchant. Accessed: 2019-11-18. [Online]. Available: <http://www.cryptomerchantbank.co/whitepaper>
- [22] What is HTTPS? Accessed: 2019-11-28. [Online]. Available: <https://www.cloudflare.com/learning/ssl/what-is-https/>

- [23] What is HTTP? Accessed: 2019-11-28. [Online]. Available: <https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/>
- [24] Wireshark · go deep. Accessed: 2019-11-28. [Online]. Available: <https://www.wireshark.org/>
- [25] Sectigo a commercial certificate authority (ca) and web security solutions company. Accessed: 2019-11-18. [Online]. Available: <https://bitcoinwhoswho.com/scams>
- [26] What is open source intelligence and how is it used? Accessed: 2019-11-28. [Online]. Available: <https://www.recordedfuture.com/open-source-intelligence-definition/>
- [27] r/bitcoin · found a clever scam, today. Accessed: 2019-11-28. [Online]. Available: [https://www.reddit.com/r/Bitcoin/comments/bb1rdc/found\\_a\\_clever\\_scam\\_today/](https://www.reddit.com/r/Bitcoin/comments/bb1rdc/found_a_clever_scam_today/)
- [28] Serhii. Scammers lured out bitcoins from victims wishing to withdraw cryptocurrency from a fake wallet. Accessed: 2019-11-28. [Online]. Available: <https://www.omnia.icu/2019/07/15/moshenniki-vymanivali-bitkoiny-u-zhertv-zhelayushhih-vyvesti-kriptovalyuq>
- [29] Publish0x - earn cryptocurrency for blogging. Accessed: 2019-11-28. [Online]. Available: <https://www.publish0x.com>
- [30] G. Rethory. The irony scam - new scam method - (english version). Accessed: 2019-11-28. [Online]. Available: <https://www.publish0x.com/granrethory/irony-scam-new-scam-method-english-version-xjmeew>
- [31] —. The irony scam - those responsible for this - new scam method -investigation part 2. Accessed: 2019-11-28. [Online]. Available: <https://www.publish0x.com/granrethory/irony-scam-those-responsible-new-scam-method-investigation-p-xpmnk>
- [32] —. The irony scam - new scam method -investigation part 3 - suspended domains. Accessed: 2019-11-28. [Online]. Available: <https://www.publish0x.com/granrethory/irony-scam-new-scam-method-investigation-part-3-suspended-do-xgppqm>
- [33] —. The irony scam - in the end i made it - new scam method -investigation part 4 - namecheap is good! Accessed: 2019-11-28. [Online]. Available: <https://www.publish0x.com/granrethory/irony-scam-end-i-made-it-new-scam-method-investigation-part-xvwsgm>
- [34] Cryptomerchant - best crypto wallet. Accessed: 2019-11-28. [Online]. Available: <https://cryptomerchant.co/>
- [35] Cryptomerchant - best crypto wallet. Accessed: 2019-11-28. [Online]. Available: <https://cryptomerchant.co/legal.php>
- [36] Digital prepaid payment solutions | WaveCrest. Accessed: 2019-11-28. [Online]. Available: <https://www.wavecrest.gi/>
- [37] Reverse dns lookup. Accessed: 2019-11-28. [Online]. Available: <https://viewdns.info/reverseip/>
- [38] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://coinhawk.us>
- [39] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://koin-zone.com>
- [40] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://babe-vids.fun>
- [41] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://cryptominer.watch>
- [42] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://call-look-up.site>
- [43] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://iwalltworld.com>
- [44] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://reviewrodeo.com>
- [45] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://caller-ii-lockup.icu>
- [46] Discovered iteration of phone-book.xyz. Accessed: 2019-11-28. [Online]. Available: <http://reverse-tracer.site>
- [47] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://boogaloo.world/>
- [48] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://futanari.live/>
- [49] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://futanari.site/>
- [50] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://nightingale.live/>
- [51] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://nightingale.live/>
- [52] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://clownstick.site/>
- [53] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://pusheen.fun>
- [54] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://vlogmas.club>
- [55] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://wubba.online>
- [56] Domain of hermatix m2m communication. Accessed: 2019-11-28. [Online]. Available: <https://wonkette.club>
- [57] Coinkeeper.cc a current iteration of mcx.ltd. Accessed: 2019-11-28. [Online]. Available: <https://clownstick.online/>
- [58] Https variant of coinkeeper.cc. Accessed: 2019-11-18. [Online]. Available: <https://coinkeeper.cc/>
- [59] Exposed admin panel of coinkeeper.cc. Accessed: 2019-11-28. [Online]. Available: <https://www.coinkeeper.cc/admin>
- [60] The other website referenced in the feeder site page sources, this website also contained the cpanel login. Accessed: 2019-11-18. [Online]. Available: <https://block-records.xyz/>
- [61] <http://podelnohosting.com> control panel. Accessed: 2019-11-18. [Online]. Available: <https://cpanel.net/>
- [62] Discovered iteration of mcx.ltd. Accessed: 2019-11-28. [Online]. Available: <http://online-portal.cf>
- [63] Discovered mcx.ltd replacement domain. Accessed: 2019-12-16. [Online]. Available: <http://mcxlive.ltd/wallet>
- [64] Discovered iteration of mcx.ltd. Accessed: 2019-11-28. [Online]. Available: <http://cloudminer.tech>
- [65] Discovered iteration of mcx.ltd. Accessed: 2019-11-28. [Online]. Available: <http://www.mcxwallet.co>
- [66] A news article from medium on a past iteration of mcx.ltd. Accessed: 2019-11-28. [Online]. Available: <https://medium.com/@blackorbird/an-interesting-bitcoin-new-scam-14552fc7953b>
- [67] Bitcoin abuse database the site containing the report regarding a ransom call. Accessed: 2019-11-28. [Online]. Available: <http://67.205.141.98/>
- [68] Bitcoin abuse site with reports related to the scam network. Accessed: 2019-11-28. [Online]. Available: <https://www.bitcoinabuse.com/reports/1FqSVjPQWZGnPsRp922SYmCQpctXwwE3Gf>
- [69] Google maps - mcx.ltd address. Accessed: 2019-11-28. [Online]. Available: <https://www.google.com/maps/search/16+Commissioner+St,+London,+EC4N,+UK/@51.5123975,-0.0906387,17z/data=!3m1!4b1>
- [70] Topbiz.site - pre-made scam marketplace. Accessed: 2019-12-16. [Online]. Available: <https://topbiz.site/>
- [71] Topbiz.site - miner coin exchange scam overview page. Accessed: 2019-12-16. [Online]. Available: <https://topbiz.site/wallet.php>
- [72] Discovered miner coin exchange demo site referencing topbiz.site. Accessed: 2019-12-16. [Online]. Available: <http://mcx-exchange.top/>
- [73] Discovered miner coin exchange demo site's active donation form. Accessed: 2019-12-16. [Online]. Available: [http://mcx-exchange.top/core/donation\\_form.php?api-1Dy46qKyZ5pukQwvEnbyN4RQpuS3u6h4UE#](http://mcx-exchange.top/core/donation_form.php?api-1Dy46qKyZ5pukQwvEnbyN4RQpuS3u6h4UE#)
- [74] Topbiz.site - modern aesthetic cryptocurrency scam overview page. Accessed: 2019-12-16. [Online]. Available: <https://topbiz.site/wallet2.php>
- [75] Original website for the wallet2 exchange scam. Accessed: 2019-12-16. [Online]. Available: [wallet2.ru](http://wallet2.ru)
- [76] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [binfox.ltd](http://binfox.ltd)
- [77] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [oxetrade.com](http://oxetrade.com)
- [78] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [unictrade.com](http://unictrade.com)
- [79] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [padhex.com](http://padhex.com)
- [80] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [genecryptotrade.com](http://genecryptotrade.com)
- [81] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [swiftcoinbitx.com](http://swiftcoinbitx.com)
- [82] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [bitcoins-pay.com](http://bitcoins-pay.com)
- [83] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [fixxtrade.com](http://fixxtrade.com)
- [84] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [coinbeaxy.com](http://coinbeaxy.com)
- [85] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: [coinpays.uk](http://coinpays.uk)

- [86] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: finontrade.com
- [87] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: weextrade.com
- [88] Discovered iteration of wallet2.ru. Accessed: 2019-12-16. [Online]. Available: restrade.org
- [89] Topbiz.site - online store scam overview page. Accessed: 2019-12-16. [Online]. Available: <https://topbiz.site/shopking.php>
- [90] Topbiz.site - explicit adult services scam overview page. Accessed: 2019-12-16. [Online]. Available: <https://topbiz.site/sex-taxi.php>
- [91] Mcx.ltd WHOIS, DNS, & domain info - DomainTools. Accessed: 2019-11-28. [Online]. Available: <https://whois.domaintools.com/mcx.ltd>
- [92] Phone-book.xyz WHOIS, DNS, & domain info - DomainTools. Accessed: 2019-11-28. [Online]. Available: <https://whois.domaintools.com/phone-book.xyz>
- [93] Caller-Idx.xyz WHOIS, DNS, & domain info - DomainTools. Accessed: 2019-11-28. [Online]. Available: <https://whois.domaintools.com/caller-idx.xyz>
- [94] Whois lookup, domain availability & IP search - DomainTools. Accessed: 2019-11-28. [Online]. Available: <https://whois.domaintools.com/>
- [95] Godaddy. Accessed: 2019-11-28. [Online]. Available: <https://www.godaddy.com/>
- [96] Namecheap. Accessed: 2019-11-28. [Online]. Available: <https://www.namecheap.com/>
- [97] Godaddy support page. Accessed: 2019-11-28. [Online]. Available: <https://www.godaddy.com/contact-us>
- [98] Namecheap support page. Accessed: 2019-11-28. [Online]. Available: <https://www.namecheap.com/support>
- [99] HTTrack website copier - free software offline browser (GNU GPL). Accessed: 2019-11-18. [Online]. Available: <https://www.httrack.com/>
- [100] Bitcoin whos who - bitcoin address lookup, checker and alerts. Accessed: 2019-11-18. [Online]. Available: <https://bitcoinwhoswho.com/scams>
- [101] Cyber startup observatory. Accessed: 2019-11-28. [Online]. Available: <https://cyberstartupobservatory.com/cyber-startup-observatory-ciso-week-stephane-nappo-societe-generale/>
- [102] Cyber security quotes. Accessed: 2019-11-28. [Online]. Available: <https://www.goodreads.com/quotes/tag/cyber-security>