Uncovering Cryptocurrency Scams: A Computer Forensics Analysis

Mary Arden Pennington, Tierra Davis, Jay McMillan, & Shouzab Khan

The University of Alabama at Birmingham

Abstract

This study utilizes computer forensics methodologies to analyze cryptocurrency scams. Employing tools such as urlscan.io, Instant Data Scraper, WhoisXML, and customized Python scripts for domain-to-IP, IP-to-geolocation, and domain-to-Whois conversions, we systematically gather and thoroughly analyze data from domains tagged as "cryptoscam" on urlscan. The primary goal of this research is to provide valuable insights into fraudulent activities within the cryptocurrency community. By meticulously examining domains and utilizing IP and Whois information, we aim to identify patterns and characteristics associated with potential scams in the cryptocurrency realm. This study contributes to a deeper comprehension of the evolving challenges and deceptive practices within the cryptocurrency landscape, with the intention of promoting awareness and proactive measures against fraudulent activities.

Introduction

Cryptocurrency, a form of digital currency created from code, represents a singular unit of currency through an encrypted string or data hash. Cryptocurrency's distinct characteristic is its independence from government control, operating through a peer-to-peer internet protocol.

This research surrounds the issue of cryptocurrency scams, with a particular emphasis on understanding crypto scams within the United States. By narrowing our focus, we aim to pinpoint hotspots and identify trends within specific states or regions. This strategic approach aligns with the effective methodology of problem-solving by examining smaller areas, similar to the approach used by the Criminal Justice System.

The decision to concentrate on the U.S. was implemented for multiple reasons, including proximity, access to legal resources, collaboration with local authorities, and a methodical investigation process. Success in our research meant comprehensive data collection, detailed analysis, and the presentation of geographical mapping. These elements not only measure the effectiveness of our efforts but also contribute to the understanding of cryptocurrency scams within the community.

This research seeks to shed light on cryptocurrency scams, exploring their impact on individuals and institutions. By providing insights into the patterns and characteristics of these scams, we aim to contribute valuable information to digital security and financial fraud prevention. Through this research project, we aspire to raise awareness, enhance protective measures, and ultimately contribute to the take-down of cryptocurrency-related fraudulent activities.

Research Objectives

When considering our goals, we asked a crucial question: "How can we make a real impact and be effective?" This led us to our objective of establishing a comprehensive database

containing information about known cryptocurrency scam domains. This database is intended to serve as a valuable resource for government agencies and the broader cyber community.

By consolidating data on these scams, our aim is to provide a centralized and accessible database that can enhance cybersecurity efforts and allow faster responses to potential threats. The main goal is to provide government agencies and the cyber community with a tool that aids in collective awareness, prevention, and mitigation of cryptocurrency scams. Through the creation of this database, we aspire to make a lasting impact in combating fraudulent activities in the digital realm.

Methodology

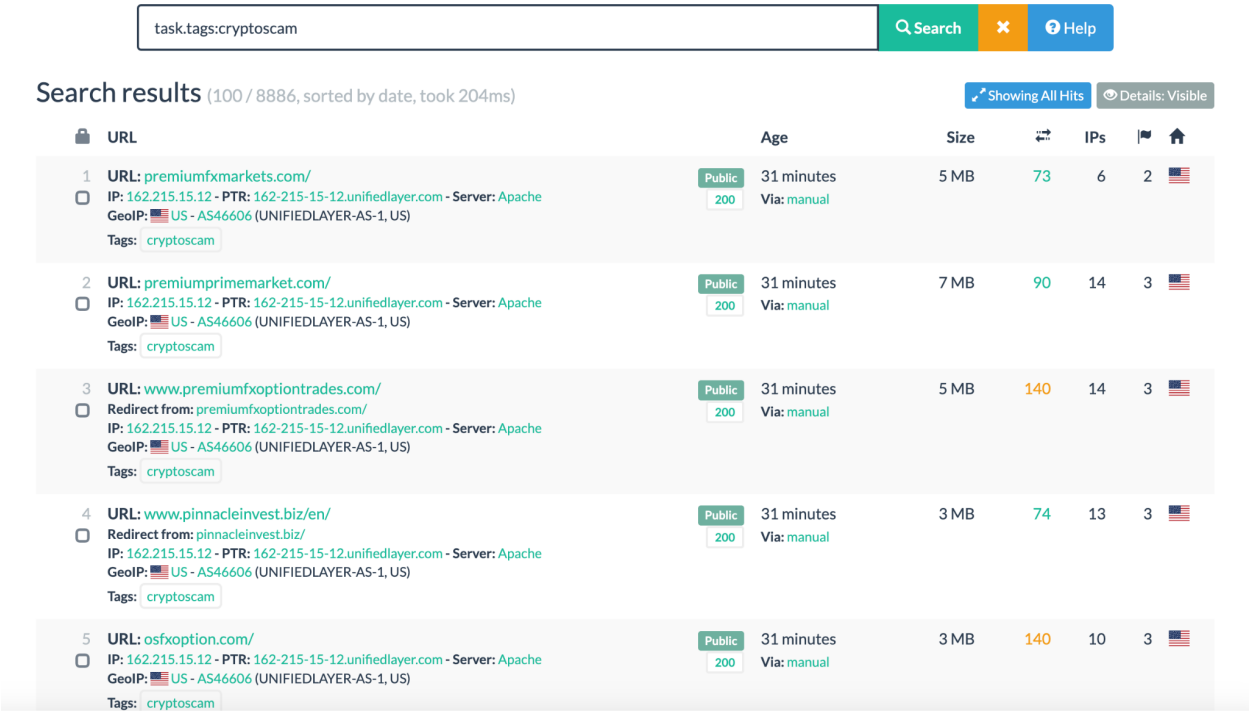
To understand 8000 domains better, we used different tools and methods. We made sure the locations of the IP addresses matched our information accurately using IP Analysis. WHOIS analysis helped us find out who owned the domains, adding valuable details to our research. We double-checked locations to be precise.

We looked for patterns and common factors among the domains. Custom Python scripts made our work faster and more accurate, especially when checking IP addresses and ownership details. We also used GeoIP Services, like Google Maps, to create a map showing where all the domains were located. Seeing all the locations together helped us understand potential groups of domains.

Understanding who the domain is registered through, the registrant, is crucial. Tools like WhoisXML helped us with this. Knowing the registrar is important for legal reasons. It ensures that if a subpoena is issued the registrar is identified in order to obtain information to locate the perpetrator. This information helps create a strong legal framework, showing a clear ownership chain and making our research more reliable and legal.

Participants

In this study, human participants were not involved. Instead, we employed URLScan.io as the primary tool to gather domains, with a specific focus on domains tagged as "cryptoscams", which will be referred to as our subjects. The use of URLScan.io facilitated the collection of data related to security parameters, potential threats, and other relevant information associated with the identified domains. The domains served as the focal points of analysis, allowing for an in-depth examination of security-related aspects without direct involvement of human subjects.



(Screenshot of URLScan.io "cryptoscam" tag)

Materials

The research embraced a comprehensive suite of tools and technologies to systematically analyze 8000 domains, focusing on security parameters, ownership details, and potential scam indicators.

The instrumental tools included:

URL Scan:

- Purpose: Domain screening and assessment of security and information parameters.
- Tool Used: URLScan.io

IP Analysis Tools:

- Purpose: Geographic verification of IP addresses associated with the scanned domains.
- Tools Used: Custom Python Scripts for precise IP lookup, GeoIP Services (e.g., Google Maps).

WHOIS Analysis Tools:

- Purpose: Gathering ownership details of the domains.
- Tools Used: WhoisXMLAPI, BulkSEOTools.com, Custom Python Scripts for WHOIS lookup.

Pattern Recognition Tools:

- Purpose: Evaluation of patterns within the data to identify potential scam indicators.
- Tools Used: Excel Pivot tables and charts.

Python Scripts:

- Purpose: Streamlining investigation processes for IP, Geolocation, and WHOIS lookup, improving accuracy and speed.
- Tools Used: Custom Python scripts for automated data retrieval.

```python
from bs4 import BeautifulSoup
import requests
import socket

# List of URLs
urls = [
    "expertprofitpro.com"

]

# Iterate through the list of URLs
for url in urls:
    try:
        # Get the IP address of the website
        ip_address = socket.gethostbyname(url)
        print(f'IP Address of {url}: {ip_address}')

        # Send an HTTP GET request to the URL
        response = requests.get(url)
        soup = BeautifulSoup(response.text, 'html.parser')

        # Find the element with the text 'Located in' if it exists
        target_element = soup.find('p', text='Located in')

        if target_element:
            text_after_target = target_element.get_text()
            print(f'Text after the target string: {text_after_target}')
        else:
            print('The target string was not found in the HTML.')

        # Check if the request was successful (status code 200)
        if response.status_code == 200:
            # You can perform additional tasks with the response content here
            # For example, you can parse the HTML content or extract specific information
            # from the webpage using libraries like BeautifulSoup.

            # For now, let's print a snippet of the content:
            print(response.text[:2000])  # Print the first 2000 characters of the HTML content
        else:
            print(f"Failed to retrieve content. Status code: {response.status_code}")

    except (socket.error, requests.RequestException) as e:
        pass


    print('-' * 50)  # Separate output for each URL
```

(Python script for URL to IP Address)

```python
import requests

def get_coordinates(ip_address):
    # Make a request to the free IPinfo.io API
    response = requests.get(f"http://ipinfo.io/{ip_address}/json")

    # Check if the request was successful
    if response.status_code == 200:
        # Parse the JSON response
        data = response.json()
        # Extract and return the coordinates
        return data.get('loc', '').split(',')

    else:
        # Print an error message if the request was not successful
        print(f"Error: Unable to retrieve data for {ip_address}. Status code: {response.status_code}")
        return None

# Example usage with multiple IP addresses
ip_addresses = ["135.181.18.187"]  # Replace with the IP addresses you want to convert

for ip_address in ip_addresses:
    coordinates = get_coordinates(ip_address)

    if coordinates:
        latitude, longitude = coordinates
        print(f"IP: {ip_address}, Latitude: {latitude}, Longitude: {longitude}")
    else:
        print(f"Failed to retrieve coordinates for {ip_address}")
```

(Python script for IP Address to Geolocation)

```python
import whois

def get_whois_info(domain):
    try:
        # Perform WHOIS lookup
        domain_info = whois.whois(domain)
        return domain_info
    except whois.parser.PywhoisError as e:
        return f"Error: {e}"

# List of domains to look up
domains_to_lookup = [
    "expertprofitpro.com"
    # Add more domains as needed
]

# Iterate through the list of domains
for domain in domains_to_lookup:
    result = get_whois_info(domain)

    if isinstance(result, dict):
        print(f"\nWHOIS information for {domain}:")
        for key, value in result.items():
            print(f"{key}: {value}")
    else:
        print(result)
```

(Python Script for Domain to WHOIS information)

GeoIP Services (Google Maps API):

- Purpose: Providing a visual representation of the geographic locations associated with the domains.
- Tools Used: Google Maps API or other GeoIP services.

These tools together created a strong toolkit, allowing us to thoroughly examine the specified domains in a systematic manner.

Procedure

The research procedure unfolded in a meticulously planned sequence, employing the aforementioned tools and technologies to achieve the research objectives:

URL Scan:

- Configured URL Scan to systematically scan the 8000 target domains.
- Collected data on security indicators, potential threats, and detailed website information.

IP Analysis:

- Utilized custom Python scripts for accurate IP lookup.
- Mapped IP addresses using GeoIP services (e.g., Google Maps) for visual representation.
- Cross-verified location data to ensure accuracy.

WHOIS Analysis:

- Employed WhoisXML and BulkSEOTools to extract ownership information.
- Utilized custom Python scripts for WHOIS lookup to gather additional details.
- Analyzed WHOIS data to understand the ownership structure.

Pattern Recognition:

- Developed and implemented advanced pattern recognition algorithms or utilized existing tools to detect scam indicators.
- Analyzed patterns in the data, focusing on commonalities among potential scam domains.

Python Scripts:

- Developed custom Python scripts to automate the retrieval of IP and WHOIS information.
- Used scripts to efficiently gather, organize, and prepare data for subsequent analysis.

GeoIP Services (Google Maps):

- Utilized GeoIP services to map the locations of IP addresses.
- Gained insights into the distribution of the domains and potential geographical clusters.

To unravel the registrant details associated with the identified domains, the research incorporated the API WhoisXML. This step was essential in understanding the ownership structure and gaining insights into the entities responsible for the registered domains. This

framework ensured a methodical and systematic approach to the research, using the specified materials to create insights into security, ownership, and potential scam indicators associated with the targeted domains.

Results and Findings

Geographic Patterns:

- Geographic analysis revealed a notable concentration of potential scam domains in urban areas, particularly in regions known for high-tech industries.
- Visualization through GeoIP Services showcased distinct clusters, hinting at possible organized efforts in specific locations.

Ownership and WHOIS Analysis:

- WHOIS analysis uncovered a prevalence of privacy-protected registrations among potential scam domains, adding a layer of anonymity to their ownership.
- Cross-verification of ownership data exposed recurring patterns, suggesting potential collaboration among certain entities in running scams.

Security Indicators:

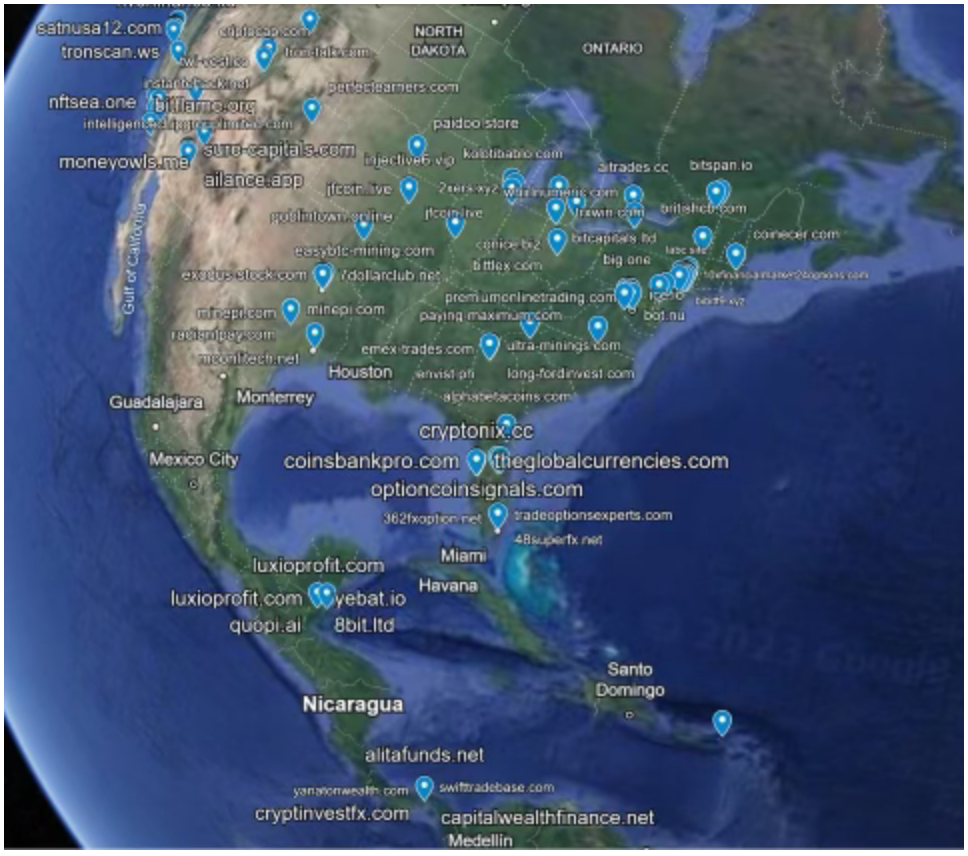
- URLScan screening identified a recurring pattern of certain keywords and structures within scam domains.

Geographical Correlations:

- Strong correlations were observed between the geographic locations of potential scam domains and the presence of tech-savvy communities.

Ownership Characteristics:

- Correlations pointed towards a connection between privacy-protected registrations and a higher likelihood of involvement in fraudulent activities.
- Patterns in ownership structures suggested potential collaboration or shared methodologies among entities behind scam domains.



(Geo Locations of CryptoScams in the United States)

Challenges and Limitations

Throughout the course of our research, we encountered several challenges and limitations that influenced the direction of our efforts. Initially, our goal was to implement an interactive database through a dedicated website. However, we faced technical difficulties in the website creation process, prompting us to reassess our approach. With time constraints in mind, we made a strategic decision to pivot our focus towards the development of a geographical map and an excel database.

While using Python Script proved to be highly beneficial for our objectives, we encountered issues when attempting to export data to a CSV file. This limitation restricted us to collecting the output of the Python script individually rather than employing a more comprehensive approach.

Despite these challenges, our adaptation to prioritize map development showcases our commitment to finding effective solutions within the given constraints, demonstrating the flexibility and resilience of our research approach.

Future Research

Looking ahead, there are exciting possibilities for future research. To start, going back to the idea of creating an interactive database, overcoming the technical challenges we faced. This would help law enforcement to easily spot active locations linked to cryptocurrency scams, offering a valuable tool for taking timely action.

Another important task is to find a faster way to get data from the Python script. If we can do this more efficiently, it will speed up our investigations and make them more effective. This might involve exploring new techniques or using additional tools to make the data extraction process smoother.

These ideas highlight the potential for making our work even better and smarter in the fight against cryptocurrency scams. By addressing these challenges, our aim is to improve our methods, strengthen our research abilities, and contribute to the ongoing efforts to tackle digital fraud.

Conclusion

In summary, our research was prompted by the growing issue of scams within the cryptocurrency space. The popularity of cryptocurrency, combined with a lack of strict regulations, has created an environment perfect for scams.

At the core of our investigation was a detailed examination of IP addresses, aiming to understand the operational dynamics of these scams and contribute to creating a safer online

environment. Recognizing the importance of public awareness, our goal was to shed light on the workings of these scams.

The choice to center our research on the United States had dual objectives. Firstly, we aimed to identify geographical trends and hotspots of scams.. Secondly, being close to home made access to resources much easier, strengthening our investigative efforts.

Leveraging tools like WhoisXML, Urlscan.io, Instant Data Scraper, and Python Scripts, we conducted a comprehensive analysis of numerous domains. Creating maps illustrating areas of heightened scam activities provided valuable visual insights.

This research not only provides a snapshot of cryptocurrency scams but also establishes a foundational framework for developing more effective methods to detect and combat these online threats. By comprehending the underlying patterns associated with scams, our goal is to contribute to ongoing efforts to strengthen cybersecurity and safeguard individuals in the evolving digital landscape.

References

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice & Epidemiology in Mental Health*, *16*(1), 24–35. https://doi.org/10.2174/1745017902016010024

Cong, L. W., Grauer, K., Rabetti, D., & Updegrave, H. (2023). *The Dark Side of Crypto and Web3: Crypto-Related Scams*. *Available at SSRN 4358572*. The Dark Side of Crypto and Web3: Crypto-Related Scams by Lin William Cong, Kimberly Grauer, Daniel Rabetti, Henry Updegrave :: SSRN

Kethineni, S., & Cao, Y. (2020). *The Rise in Popularity of Cryptocurrency and Associated Criminal Activity*. International Criminal Justice Review, 30(3), 325-344. https://doi.org/10.1177/1057567719827051

Navarro, R. R. (2019). (rep.). *Preventative Fraud Measures for Cryptocurrency Exchanges: Mitigating the Risk of Cryptocurrency Scams*. https://www.proquest.com/docview/2312801484?fromopenview=true&pq-origsite=gscholar&parentSessionId=h2Y3LpyZDs7iPcuzxV9sx47jDR%2F7zpuASjadmw03X7s%3D

Phillips, R., & Wilder, H. (2020, May). *Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites*. In *2020 IEEE international conference on blockchain and cryptocurrency (ICBC)* (pp. 1-8). IEEE. Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites | IEEE Conference Publication | IEEE Xplore

Warner, G. (2023, July 13). *Getting a Job in Pig-Butchering*. DarkTower. https://getdarktower.com/getting-a-job-in-pig-butchering/

URLScan. https://urlscan.io/search/#task.tags%3Acryptoscam

WHOISXML API. https://whois.whoisxmlapi.com/bulk-whois-lookup

Bulk SEO Tools. https://www.bulkseotools.com/bulk-domain-to-location.php

Database: https://1drv.ms/x/s!AoGB1FZ86imA5V7IJuXPgqMkzfkm