Characterizing Cryptocurrency-themed Malicious Browser Extensions

KAILONG WANG*, Huazhong University of Science and Technology, China; National University of Singapore, Singapore
YUXI LING*, National University of Singapore, Singapore
YANJUN ZHANG, Deakin University, Australia
ZHOU YU, Beijing University of Posts and Telecommunications, China
HAOYU WANG†, Huazhong University of Science and Technology, China
GUANGDONG BAI†, The University of Queensland, Australia
BENG CHIN OOI, National University of Singapore, Singapore
JIN SONG DONG, National University of Singapore, Singapore

Due to the surging popularity of various cryptocurrencies in recent years, a large number of browser extensions have been developed as portals to access relevant services, such as cryptocurrency exchanges and wallets. This has stimulated a wild growth of cryptocurrency-themed malicious extensions that cause heavy financial losses to the users and legitimate service providers. They have shown their capability of evading the stringent vetting processes of the extension stores, highlighting a lack of understanding of this emerging type of malware in our community. In this work, we conduct the first systematic study to identify and characterize cryptocurrency-themed malicious extensions. We monitor seven official and third-party extension distribution venues for 18 months (December 2020 to June 2022) and have collected around 3600 unique cryptocurrency-themed extensions. Leveraging a hybrid analysis, we have identified 186 malicious extensions that belong to five categories. We then characterize those extensions from various perspectives including their distribution channels, life cycles, developers, illicit behaviors, and illegal gains. Our work unveils the *status quo* of the cryptocurrency-themed malicious extensions and reveals their disguises and programmatic features on which detection techniques can be based. Our work serves as a warning to extension users, and an appeal to extension store operators to enact dedicated countermeasures. To facilitate future research in this area, we release our dataset of the identified malicious extensions and open-source our analyzer.

CCS Concepts: • **Security and privacy → Intrusion/anomaly detection and malware mitigation**.

Additional Key Words and Phrases: Browser extension, cryptocurrency, malware detection

ACM Reference Format:
Kailong Wang, Yuxi Ling, Yanjun Zhang, Zhou Yu, Haoyu Wang, Guangdong Bai, Beng Chin Ooi, and Jin Song Dong. 2022. Characterizing Cryptocurrency-themed Malicious Browser Extensions. *Proc. ACM Meas. Anal. Comput. Syst.* 6, 3, Article 43 (December 2022), 31 pages. https://doi.org/10.1145/3570603

*The authors contribute equally
†Haoyu Wang (haoyuwang@hust.edu.cn) and Guangdong Bai (g.bai@uq.edu.au) are the corresponding authors

Authors' addresses: Kailong Wang, Huazhong University of Science and Technology, China; and National University of Singapore, Singapore; Yuxi Ling, National University of Singapore, Singapore; Yanjun Zhang, Deakin University, Australia; Zhou Yu, Beijing University of Posts and Telecommunications, China; Haoyu Wang, Huazhong University of Science and Technology, China; Guangdong Bai, The University of Queensland, Australia; Beng Chin Ooi, National University of Singapore, Singapore; Jin Song Dong, National University of Singapore, Singapore.

2476-1249/2022/12 – Art 43. https://doi.org/10.1145/3570603

1 INTRODUCTION

The openness to third-party applications, i.e., browser extensions (*extensions* for short hereafter), is a key feature of modern browsers. Continuously-evolving extensions enhance users' browsing experience with a broad range of functionalities such as user interface modifications (e.g., Tab Wrangler [77]), password management (e.g., LastPass [55]), and ad blocking (e.g., AdBlock [1]). To facilitate their access to device resources and user data, a set of permissions and privileged APIs are exposed to them. As a result, malicious extensions could abuse these powers to launch *man-in-the-browser* attacks [30, 52, 73] for information stealing, phishing, and scams.

Recently, extensions that are themed with blockchain and cryptocurrency, one of the most popular technologies nowadays, have become targets of cyber attacks. As major cryptocurrency exchange platforms [21, 51, 54] and wallet services [19, 35, 64, 74] have launched their extensions as new portals, cryptocurrency-themed extensions have attracted great attention from cybercriminals. As reported by the blockchain security firm Ciphertrace [18], cryptocurrency-related crimes caused a total of $1.9 billion loss in 2020 alone, a huge part of which has been attributed to the malicious cryptocurrency-themed extensions. For example, a fake ledger Chrome extension has stolen at least $2.5 million worth of Ripple coins in March 2020 [42].

The existing extension stores and the blockchain community have made efforts to counter the surging attacks associated with the cryptocurrency-themed extensions. For example, Google has taken down 49 phishing Chrome extensions that reportedly stole cryptocurrency data [46], and has completely banned mining through extensions [45]. Domain names and wallet addresses involved in malicious activities have been published by several open-source databases [41, 50, 53, 89] to raise public awareness. Nonetheless, our research community still lacks an in-depth understanding of cryptocurrency-themed malicious extensions, and most countermeasures still rely on the detection techniques designed for generic malware. Consequently, elaborately crafted malicious extensions, which take cryptocurrencies as the disguise or target a specific cryptocurrency business logic, could evade the detection.

Our work. In this paper, we aim to systematically *understand the status quo of cryptocurrency-themed malicious extensions in the wild* and *unveil their main characteristics that can facilitate countermeasures*. We have monitored major official and alternative extension stores in real time for 18 months (December 2020 to June 2022), covering the time during which the major exchange platforms and wallet service providers launch their extensions. For example, Coinbase, a popular exchange platform that has a daily trade volume of more than three billion dollars, launched its Chrome extension in May 2021 [20]. Our monitoring includes 3,599 extensions in total on the radar (see **Section 3**). We then propose a systematic detection approach to identify malicious ones from them (see **Section 4**). It takes into consideration multi-dimensional characteristics including metadata features (e.g., user reviews and the number of downloads), programmatic features (e.g., requested browser permissions, frequencies of variable and function types), and execution features (e.g., high CPU usage and communication with suspicious servers). We further characterize the malicious extensions in terms of their prevalence, development ecosystem, financial damage, and features for detecting them.

Key findings. To the best of our knowledge, this is the first work on the characterization of cryptocurrency-themed malicious extensions. Our study unveils the *status quo* of cryptocurrency-themed malicious extensions. We summarize our findings below and defer more details to **Section 5**.

- **Cryptocurrency-themed malicious extensions have become prevalent**. We have identified 186 malicious extensions out of the 3,599 cryptocurrency-themed ones, at a rate of 5.17%. They can be categorized into five categories based on their purposes: *phishing*, *mining*, *scam*,

adware, and *gambling/pornography*. They target almost all popular cryptocurrency-related functionalities such as price trackers, payment, coin miners, wallets, and exchange platforms.

- **Attacks through cryptocurrency-themed malicious extensions have caused significant financial losses.** We find that an estimated $1,006,610 worth of cryptocurrencies have flowed into attacker-controlled wallet addresses during the malicious extensions' lifespan.
- **Malicious extensions tend to post fake user reviews to disguise themselves**. Owners of malicious extensions routinely attempt to post large amounts of fake positive reviews to manipulate the overall ratings. Out of the extensions with negative-sentiment reviews, 42% are proven malicious. Nonetheless, half of them post fake positive reviews to flood the negative ones (likely from victims), and lift their rating scores above 4 out of 5. This renders it nearly impossible for lay users to distinguish them based on reviews and rating scores.
- **Less popular services and cryptocurrencies are also the targets of malicious extensions**. Besides targeting popular exchange platforms and wallet services (e.g., Coinbase), malicious extensions also focus on those with small volumes (e.g., Truechain and Ledger). Similarly, less-valued cryptocurrencies (such as Monero and MintCoin) have been abused as the ideal honeypots to lure vulnerable opportunists, due to the drastic price fluctuations.
- **Cryptocurrency-themed malicious extensions are stealthy but demonstrate characteristics that detection can rely on**. The cryptocurrency-themed malicious extensions are more insidious than the generic malicious extensions. Most of them (84.4%) manage to evade detection from 31 state-of-the-art anti-virus engines, and 73.1% have remained available on the extension stores for more than one month when we detect them. Nonetheless, we find that they tend to have a high frequency of security-critical permission requests (e.g., `file://*`) and system-level API calls (e.g., *identity*, *system.cpu*, and *app.runtime*) at runtime. We distill these characteristics into a set of distinctive features to benefit anti-malware tools.

Contributions. In summary, this work mainly contributes to the following aspects.

- **An in-depth study.** We conduct the first in-depth study on cryptocurrency-themed malicious extensions. It explores the ecosystem of this emerging type of malware, from its development, circulation, and financial impacts, to illicit behaviors and detection.
- **A systematic detection approach.** We propose a detection technique based on multi-dimensional information including metadata, programmatic features, and runtime behaviors. We leverage this technique in the detection of cryptocurrency-themed malicious extensions. It also helps us reveal the features with high relevance to the malicious extensions.
- **Practical results.** We have monitored the cryptocurrency-themed malicious extensions over 18 months (December 2020 to June 2022) and detected a total of 186 malicious ones. The results suggest the urgency of research efforts in this type of understudied malware. Our work should raise awareness of extension users, developers, and the cryptocurrency community. It should also encourage the extension store operators to enact dedicated countermeasures.

We release the dataset of the identified malicious extensions [40] and open-source our analyzer to facilitate the countermeasures of the cryptocurrency-themed malicious extensions, and to encourage future research in this area.

2 BACKGROUND AND THREAT MODEL

2.1 Cryptocurrency-themed Browser Extensions

Among the browser extensions, cryptocurrency-themed ones are experiencing fast growth over the recent years, thanks to the popularity of blockchain technology and cryptocurrencies. From a broad point of view, there are two types of cryptocurrency-themed extensions. One type is the lightweight version of the web-based or application-based counterparts implemented by the official or authorized

service providers, such as the cryptocurrency wallets (e.g., Coinbase Wallet extension [22]). The other type includes extensions implemented by third-party developers for cryptocurrency services, incorporating richer and more diverse functions to enhance user experience. Typical examples include market data tracker (e.g., Crypto Price Tracker [27]), integrated portals as shortcuts for accessing various cryptocurrency applications (e.g., Metamask [60]), security and privacy-related extensions (e.g., minerBlock [61]).

2.2 Permissions and Programmatic Features of Extensions

We brief on two key features of browser extensions that our detection approach relies on.

Permissions. Most browser extensions are archived into a well-formatted *crx* or *xpi* file. Inside the archive, the code base is organized in a way similar to a web application, containing files such as HTML, JavaScript, CSS, and local images. A JSON file named *manifest.json* describes the extension's meta information, including name, version, developer, and requested browser-level permissions. In particular, the requested permissions determine its capabilities in network traffic manipulation, cookie accessibility, and web page modification. Thus, the requested permissions serve as a critical feature to detect malicious extensions in our approach.

Programmatic Features. The logic of an extension is detailed in its content scripts and the background page source code. Content scripts play a key role in interacting with the web pages that the browser navigates to. They can read the details of the webpage or modify its DOM. Complementing the content scripts, extensions can also run scripts in the context of the background page which can be used to maintain the state and control the behavior logic of the extension without being visible to the user. Considering the distinct execution logics and the resulting behaviors between the malicious and benign extensions, these programmatic patterns have been utilized to benchmark the differences between them. They have shown effectiveness in practice [87].

2.3 Cryptocurrency-themed Malicious Extensions

In this work, we consider two types of threats that are relevant to cryptocurrencies in the context of browser extensions, i.e., *involving cytocurrencies for illicit payment* and *involving crytocurrencies as disguises or lures*. Due to the anonymous nature of transactions, cryptocurrencies are often used as the payment method by malware and hidden services that provide *illicit services* such as gambling and drug trading [38, 78]. Therefore, we examine extensions that may contain such behaviors.

Due to their investment nature, cryptocurrencies have also been abused as baits to attract users to click links containing malicious contents or install malicious applications, as shown by previous studies [90–92]. Malicious behaviors covered up by cryptocurrencies may include *phishing*, *scamming*, *mining* and *advertising*.

- ***Phishing extensions*** typically craft visually identical interfaces as the official extensions or web pages to trick victims into entering their sensitive information unwittingly, such as authentication credentials for cryptocurrency exchanges, private keys and seed phrases of cryptocurrency wallets. Using such information, attackers can log into the victim's account and initiate unauthorized transactions.
- ***mining extensions*** mine cryptocurrencies with victim's computational power, through fetching tasks from mining pools and in-browser mining in the background.
- ***Scam extensions*** trick victims into the "honeypot" traps with fake attractions or deals. They commonly utilize fake or irresistible advertisements to lure the victims into transferring digital coins to attacker-controlled wallet addresses.

Table 1. Summary of Preliminary Filtering

Stores	Raw No.	Neg Review/Rating	Downloads < 100	Total	Stores	Raw No.	Neg Review/Rating	Downloads < 100	Total
Chrome Web Store	1,430	413	609	651	Whale Store	7	7	7	7
Add-ons for Firefox	1,532	782	1047	1075	Crx4Chrome	427	427	427	427
Opera Add-ons	54	4	0	4	Guge	93	93	93	93
Microsoft Edge Add-ons	26	26	26	26	Haoyong	14	14	14	14
360 Extreme Explorer Store	16	16	16	16					

- ***Adware extensions*** pretend to be cryptocurrency-related services but pop up advertisement upon execution.

3 DATA COLLECTION

Since no dataset could be reused for our study, we start with building one. We mainly address two challenges in this phase: 1) to construct *a comprehensive dataset* that includes relevant extensions for mainstream web browsers from their official and alternative (i.e., third-party) extension stores, and 2) to employ a real-time monitoring approach such that our study does not miss the new samples that are taken down by the store operators within a short time.

3.1 Data Sources

Browser types. We target the top 10 most downloaded browsers [11], as listed in Table 8 (marked as *Global* in their regions) in Appendix A.1. In addition, we also include the regional browsers, considering that cryptocurrency exchanges are often localized along with the regional restrictions on fiat currencies. We investigate the regional browsers in the top 10 countries that have the most cryptocurrency adoption according to Statista [72] and have identified 18 popular regional browsers from six of them, as listed in Table 8 (marked with country codes in their regions).

Extension sources. We resort to two sources for extension collection. The first source includes the official extension stores of the target browsers. We have developed crawlers for *Chrome*, *Firefox*, *Opera*, and *Edge* due to their popularity and high coverage. Our crawlers built for these four manage to cover 20 browsers because they are based on a handful of browser engines and share the same stores. As for the remaining browsers, the *360 Explorer* and *Whale* enforce strict anti-crawling mechanisms, so our crawlers only monitor the updates on their stores and we download the extensions manually. *IE* supports a limited number of proprietary extensions and its extension store is not open to third-party developers. *Safari* combines its store with the Apple app store. Others have a limited number of cryptocurrency-themed extensions available in their stores.

Our second source includes alternative extension stores. They are often intensively targeted by the attackers, due to the lack of strict vetting and monitoring mechanisms (e.g., the malware detection system implemented by Google [58]). We include three popular ones: *Crx4Chrome* [26], *Haoyong* [49], and *Guge* [47]. All in all, our crawlers cover browsers that account for approximately 90% of the market share in total (see Table 8).

3.2 Collection Methodology

By reviewing the names and descriptions of cryptocurrency-themed extensions, we find that most of them function as the portals to access various cryptocurrency services or serve as lightweight alternatives to existing web-based services. Based on this finding, our crawlers search the extension stores using a keyword corpus. The corpus contains the top 600 keywords listed by CoinMarketCap [23] and another 200 keywords used in a recent related study [92]. The keywords include the names and abbreviation of the cryptocurrencies (e.g., “Bitcoin”, “Ethereum”, “Litecoin” and “Zcash”), exchanges (e.g., “Binance”, “Coinbase”, “OKEx” and “Coindeal”), cryptocurrency-related vocabulary (e.g., “Wallet”, “Ledger” and “Crypto”). Considering that attackers may use anagrams (such as “cion” derived from “coin”) to mimic benign extensions, our crawlers also search the anagrams of

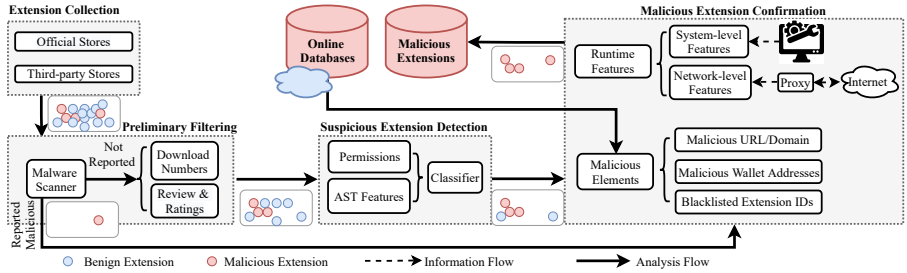


Fig. 1. Detection Approach Overview

the keywords. To cover the extensions in languages other than English, we use Google Translate to translate the keywords into Chinese and Korean from English, and into the local languages when crawling the regional extension stores. Our crawlers are developed based on the web application testing tool Selenium [81] to automate the data collection process.

The malicious extension population is relatively unstable. For example, an attacker may only make its extension available during a particular event and immediately take it down after the campaign. An extension could also be taken down by the store operator shortly after it is uploaded, due to policy violations or complaint reports filed by users. Therefore, we conduct the crawling process every eight hours. According to a recent study [69] which does so every 24 hours, the samples we miss are much less than 0.5%. For each relevant extension, our crawlers download its entire code base. We then check whether it exists in our database with its hash value, and keep only those unseen ones. This also allows us to capture the updated versions of every relevant extension.

We deploy our crawlers on Windows 10 virtual machines hosted by a server in our university. Each virtual machine has 8 CPUs, 16GB RAM, and 160GB storage. We first tested and refined our collection method from May to July 2020. We manually reviewed each extension returned by the search engines of the stores (over 30,000) and excluded those irrelevant to cryptocurrency. Then, we continuously crawled from December 2020 to June 2022. We gather a dataset containing 3,599 cryptocurrency-themed extensions (4.5GB data), distributed in 9 stores as listed in Table 1.

4 DETECTION OF MALICIOUS EXTENSIONS

The fast evolving nature of cryptocurrency-themed malicious extensions renders it challenging to identify them based on pre-built signatures. We thus propose a detection approach leveraging multi-stage analysis and multi-dimensional criteria. Figure 1 shows its pipeline. We first flag suspicious extensions through a coarse-grained filtering and a classification-based detection. Then we reach a verdict through the confirmation based on their string characteristics and run-time behaviors.

4.1 Preliminary Filtering

To narrow down the search space for the later analyses, we conduct coarse-grained filtering. We first resort to existing anti-virus tools (i.e., VirusTotal [84] online scan engines) to check the crawled extensions, and keep all samples that are flagged as suspicious by them. Nonetheless, this helps us identify a limited number of malicious extensions (see Section 5.1 for details), as they are too new for those anti-virus tools to generate signatures. As a complement, we further leverage the following two types of data as the criteria for filtering.

User Reviews. Users' reviews and feedback reflect their attitude towards an extension after they install and use it. First, we mark the extensions with an average rating lower than 2 stars (out of 5) as suspicious for further checks. Second, we conduct a semantic and sentiment analysis [63] on user reviews to identify extensions with any negative reviews which indicate their possible malicious

Table 2. The Full List of Suspicious Extension Detection Features in our Classifier

Detection Feature Types		Detailed Features
Permissions		cookie (H[#]), webRequest (H) ,< *all_urls* > (H), file:///* (H), tabs (M), http://*/* (M), https://*/* (M) storage (M), webNavigation (M), webRequestBlocking (L), activeTab (L)
AST Features	Variable Type Frequencies	String, Punctuator, Keyword, Identifier, Numeric, Boolean, RegularExpression, Null and Template
	Function Type Frequencies	setTimeout, clearTimeout, parseInt, parseFloat, isNaN, define, clear, setInterval decodeURIComponent, encodeURIComponent, isFinite, Object, Function

[#] H, M and L represent high-risk, medium-risk and low-risk permissions, listed by *ExtAnalysis* [39].

behaviors. Following a recent study [31], our analysis is based on 41 negative-toned keywords (e.g., "bad", "malicious", "scam", "cheat", "fraud", and "risk") adopted by it. Third, we monitor the changes in review sentiment and rating scores over time. Inspired by Pantelaios et al. [69], those extensions with significantly deteriorated feedback and scores (i.e., over 1 point drop out of 5 on a week-to-week basis) are marked as suspicious.

Number of Downloads. The number of downloads reflects the extension's popularity. A small download number could be linked to the short existence period, which may suggest the maliciousness of the extension. We thus keep those with low downloads (we select 100 as the threshold as 80% of samples reported by VirusTotal have a download number lower than that). Changes in the download numbers also reflect the variation of an extension's popularity, possibly indicating the abnormality associated with it. We thus log the download numbers over time and select extensions with drastic number changes (i.e., over 50% increase/decrease on a week-to-week basis).

Filtering Results. Our filtering remains coarse-grained to keep the actual malicious extensions in the dataset and remove some "noise". We exclude 1286 extensions from 3,599 extensions, as listed in Table 1.

4.2 Suspicious Extensions Detection: A Lightweight Classification-based Approach

After filtering, we design a lightweight classification-based approach to detect suspicious extensions. We note that the purpose of our classification at this stage is to obtain as many malicious samples as possible, so the classifiers are trained with high false positive (detailed in Section 4.2.2) and confirmation is introduced (detailed in Section 4.3). After a dataset with confirmed samples is constructed, accurate features can be extracted and advanced detection methods can be used, as explored in our experiments (Section 5.4).

4.2.1 Classification Features. Following the literature [43, 52, 87], we use programmatic features extracted from extensions for the classification, including requested permissions and AST features. They have shown the capability to capture the subtle differences between benign and malicious extensions. From the *.crx* and *.xpi* archives, we extract the following two types of features.

Requested Permissions. Our feature list includes the requests of 11 permissions listed in Table 2. These permissions are commonly used by detectors and are labeled with certain risk levels by the open-source extension analyzer *ExtAnalysis* [39].

AST Features. Most malicious behaviors in an extension can be traced back to its JavaScript code, so we extract features from the extension code bases and incorporate them into our detection. Inspired by Wang et al. [87], we construct the feature set based on the source code statistics including 9 variables and 13 function frequencies, as listed in Table 2. They can be extracted from the ASTs (Abstracted Syntax Trees). In our work, we construct ASTs using *AST Explorer* [5] and *Esprima* [36].

4.2.2 The Classification. With the feature set, we proceed with training classifiers to detect malicious extensions. We adopt the one-vs-all strategy [68] for the classification task and have trained five classifiers to detect the malicious extensions exhibiting the five categories of malicious capabilities explained in Section 2.3, i.e., *phishing*, *scam*, *mining*, *adware* and *illicit services*.

Table 3. The Precision and Recall Rate of our Classification Models

Type	Algo	Precision (Mal)	Recall (Mal)	Precision(Benign)	Recall(Benign)	Type	Algo	Precision (Mal)	Recall (Mal)	Precision(Benign)	Recall(Benign)
Phishing	DT	0.67	**1.00**	1.00	0.95	Scam	NB	0.17	**1.00**	1.00	0.50
Mining	SVM	0.31	**1.00**	1.00	0.38	Gambling/Porn	NB	0.25	**1.00**	1.00	0.86
Adware	NB	0.17	**1.00**	1.00	0.76						

Training Data Labeling. First, we construct a labeled dataset for training and benchmarking our classifiers. We derive the labeled malicious extensions from those reported by VirusTotal and those identified by our manual search. For the latter, two of the authors manually inspect the behaviors and the source code of the extensions with low ratings (less than 2 stars), negative reviews (more than 10), and small numbers of downloads (less than 100). We randomly select a sample and both of us analyze it independently. The sample is kept only if it is confirmed as malicious by both of us. Followed by this, we discuss with a third-coauthor and reach a consensus on the category of each malicious extension. This selection process is continued till we have obtained 55 malicious extensions, 27 from VirusTotal and 28 from manual search. We select 10 extensions for phishing, scam and mining categories, and 5 for adware and illicit services due to their low prevalence during our labelling process.

We then include another 70 benign extensions into our dataset, so that each malicious category and the remaining categories maintain a 1:10 or 1:20 ratio, simulating the unbalanced distribution in the wild. These benign extensions are randomly sampled from our cryptocurrency-themed extension dataset, where we select those with high ratings (over 4 stars), frequent positive reviews (over 20) and large numbers of downloads (over 50k). We further manually inspect them in the way we select malicious ones, to ensure they are truly benign.

Training and Testing. With the labeled dataset, we train five classifiers, each of which targets one malware category. We extract a fixed-length feature vector containing all permission and AST features listed in Table 2. For permission features, we represent the existence and absence of certain permission with 1 and 0 respectively. For AST features, we calculate their frequencies and use the normalized values as the feature inputs. When training a classifier, we only label the target category of malicious extensions as foreground (i.e., labeled as 1) and the rest as background (i.e., labeled as 0). For example, when training the phishing classifier, the 10 phishing extensions have the label 1, and the remaining 100 extensions have the label 0. The rationale behind this setting is to maximize the classifier sensitivity on the target malware category (i.e., the target malware category against all other categories).

We split the five folds of the labeled data into three for training and two for testing. For each classifier, we implement four classification algorithms including SVM, logistic regression, decision tree and Naive Bayes, and adopt the algorithm with the highest recall. As shown in Table 3, all five classifiers achieve an average recall of 1.0 for the malicious extensions, indicating that our classifiers can detect nearly all of them in practice. The average precision is relatively low (near 0.35), causing false positives that require further confirmation (to be discussed soon in Section 4.3).

Detection Results. We use the five classifiers to examine all the collected extensions and mark those malicious-by-prediction if they are reported by any of the classifiers as suspicious. In this way, we identify 691 suspicious extensions, including 97 involving phishing, 400 scam, 68 mining, 94 adware and 32 illicit services.

4.3 Malicious Extension Confirmation

We conduct a confirmation step to remove false positives from those reported by our classifiers. To ensure the accuracy of our confirmation, we rely on two types of confirmative characteristics.

Confirmation with Malicious Elements. The existence or references to malicious cryptocurrency-specific elements including malicious web domains and cryptocurrency wallet addresses can serve

as a key indicator of the malicious nature. We extract the domain and address elements from the suspicious extensions using *ExtAnalysis*, and scan them against online databases that include 5,838 mining-related URLs [41, 53, 89], online abuse databases [9, 28], and the blacklist of 49 chrome extension IDs [50]. Extensions with matching malicious elements are confirmed as malicious.

Confirmation with Runtime Behavioral Features. We deploy each suspicious extension in a sandboxed testbed deployed on a virtual machine and interact with it for around five minutes using our test account. We aim to trigger its behaviors as completely as possible, by testing functions such as log-in, transferring cryptocurrency and clicking links. The testbed monitors their system-level and network-level behaviors, and confirm an extension as malicious if the followings are observed:

- ***System-level Behaviors.*** We monitor and log the system status every 10 seconds, including CPU usage, memory usage and file system changes. We check if the extension quickly depletes the resource of the machine. For example, a malicious mining extension would quickly occupy the vast majority of CPU resources (over 90%).
- ***Network-level Behaviors.*** We intercept and inspect the network traffic between the extension and the server through a man-in-the-middle proxy built with the *mitmproxy* [62]. We check if users' sensitive information, such as login credentials or cryptocurrency wallet addresses are sent to malicious or blocked URLs.

Results. After the confirmation, we have obtained overall 186 malicious extensions, including 65 in the phishing category, 22 mining, 75 scam, 16 adware, and 8 illicit services. As further validation of the results in the confirmation step, we adopt the similar extension labeling detailed in Section 4.2.2. The vast majority of labels (i.e., over 90%) are assigned without disagreement, and only very few labels (less than 10) went through the discussion and consensus-reaching process.

5 CHARACTERIZING CRYPTOCURRENCY-THEMED MALICIOUS EXTENSIONS

After collecting those cryptocurrency-themed malicious extensions, we characterize them in this section. Our investigation aims to explore the following four research questions (RQs).

RQ1. ***What is the status quo of cryptocurrency-themed malicious extensions in the wild?*** This research question aims to understand the overall ecosystem of existing cryptocurrency-themed malicious extensions. We focus on the malicious extensions themselves and their developers. For the extensions, we investigate **RQ1-1**): *how are they created and circulated, and what are their targeted browsers, cryptocurrencies, and services?* We reveal their distribution channels and their lifespan on these channels. Considering the great variety of browsers, cryptocurrencies, and services, we identify and characterize the top targets of the malicious extensions. For the developers, we explore **RQ1-2**): *who developed these malicious extensions?* As it is always a challenge to identify cybercriminals, we strive to profile the cryptocurrency-specific malicious developers based on our collected information.

RQ2. ***What are the hostile behaviors and the defining techniques associated with each category of the cryptocurrency-themed malicious extensions?*** This research question aims to find out the commonly-seen hostile behaviors of cryptocurrency-themed malicious extensions. We reveal the distinct deceptive features belonging to each malicious category and how they are leveraged to lure the victims into their traps.

RQ3. ***What are the financial impacts of cryptocurrency-themed malicious extensions?*** This research question aims to estimate the financial loss related to the identified cryptocurrency-themed malicious extensions, and demystify the money flow characteristics of the illegal profit.

RQ4. ***What features can be used by anti-malware countermeasures to effectively distinguish cryptocurrency-themed malicious extensions?*** The cryptocurrency-themed malicious extensions are domain-specific. They commonly exhibit features that are atypical and difficult to

be effectively captured by existing general-purpose malware detectors. This research question thus aims to identify a set of features to facilitate their detection.

5.1 RQ1: Status Quo of Malicious Extensions

We first investigate the *status quo* of cryptocurrency-themed malicious extensions in the wild. We focus on the extensions themselves (Section 5.1.1) and their developers (Section 5.1.2).

5.1.1 Measurement of Malicious Extensions. For the malicious extensions, we are interested in their *distributions*, *lifespans over time*, *targets*, and *abused services*.

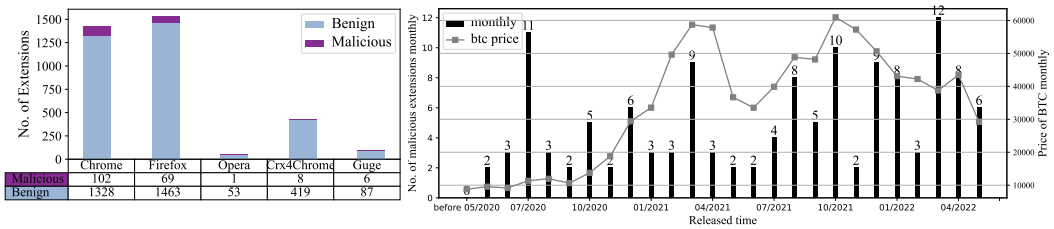
Target Browsers and Distribution Channels. The distribution of browsers targeted by malicious extensions is quite unbalanced. Chrome and Chrome-based browsers are the main targets, in line with their popularity. They account for 62.4% (116 out of 186) of all identified malicious extensions, while Firefox accounts for 37.1% (69 out of 186) and Opera 0.5% (1 out of 186).

The malicious extensions are distributed across five stores, as shown in Figure 2(a). They are the top five with the largest numbers of cryptocurrency-themed extensions (see Table 1). No malicious extensions have been identified from the remaining four stores, partly due to their limited number of actively maintained extensions. The *Chrome Web Store* has the highest prevalence rate of malicious extensions (7.1%), even though it has applied a strict vetting process [32]. This may be attributed to Google's policy that makes installing unknown-source extensions on Chrome a difficult procedure [4]. Due to this, the attackers have to distribute their malware through Chrome Web Store to infect Chrome users. The *Guge* extension store, which a store for Chrome-based browsers, is intensively targeted too (6.5%).

Lifespan. We estimate the lifespan of the malicious extensions based on the duration they remain available in the stores. Our crawlers record the time points of an extension's initial and final appearance. For extensions created before December 2020 (when our automatic collection started), we use the *last update time* as the starting point, since the stores do not make the *first upload time* available. Meanwhile, we also record the number of updates within each extension's lifespan.

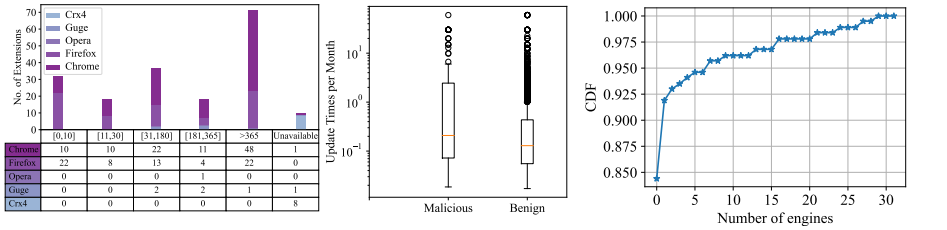
The number of newly emerging malicious extensions roughly follows the fluctuations of cryptocurrency market capital, with more identified when the crypto-assets value more and vice versa. For example, the number of monthly identified malicious extensions coincides with the Bitcoin price changes, as shown in Figure 2(b). The more detailed time distribution versus malicious category is presented in Appendix A.2. The lifespan distribution of the malicious extensions is shown in Figure 3(a). 56.5% of (105 out of 186) malicious extensions are removed eventually by the stores, compared with 12.5% (428 out of 3413) removed among the benign ones. Over 73% (136 out of 186) of them manage to exist in the store for more than one month, and more than half (71) even remain available over a year. The official stores do not perform significantly better than alternative stores in terms of detecting and removing malicious extensions, with only 19.6% (20 out of 102) and 43.5% (30 out of 69) removed within a month for Chrome Web Store and Firefox Add-ons respectively. The malicious extensions tend to update more frequently compared to the benign ones, with a median value 0.21 times versus 0.13 times per month, as shown in Figure 3 (b).

These findings are to our surprise, given that the stores have deployed strict vetting mechanisms [2, 32]. We speculate that they may rely on generic malicious extension detection techniques. However, these techniques have shown lower effectiveness for detecting cryptocurrency-themed malicious extensions that usually lack typical malicious attributes such as malicious code injection or utilization of malicious libraries. We further analyze the performance of existing anti-virus engines in VirusTotal on all identified malicious extensions. As shown in Figure 3(c), only 15.6% of them can be reported by at least one anti-virus tool, at the time point of their detection by our study.



(a) Platform Distribution of Malicious Extension (b) Timeline Distribution of Malicious Extension

Fig. 2. Malicious Extension Distribution Platforms and Timeline



(a) Lifespan of Malicious Extension (b) Update Times of Extensions (c) CDF of VirusTotal Engines Detection Results

Fig. 3. Malicious Extension Lifespan and Detection

This urges the necessity of developing detection techniques specific to cryptocurrency-themed malicious extensions. Our effort on this will be discussed in Section 5.4.

Target Cryptocurrencies and Services. To extract the cryptocurrencies and services targeted by the malicious extensions, we search for their names among the strings extracted from their *crx*/*xpi* packages and their execution logs (see Section 4.3), based on the full list of cryptocurrencies, exchanges, and wallets we obtain from a few relevant ranking websites [24, 25]. We find that 166 malicious extensions target at least one cryptocurrency, 72 target at least one cryptocurrency wallet, and 28 target at least one exchange.

We list the top 5 targeted cryptocurrencies and services in Table 4. Those popular cryptocurrencies and services are the primary targets given their large number of potential victims and high-level trust from them. Those less popular and short-term trending ones are also on the horizon due to the high potential profit for deceiving and luring the opportunists during an ephemeral craze. In particular, 88.0% (or 146) out of the 166 extensions that are involved with cryptocurrencies target the top 30 cryptocurrencies, measured by their trading volume on CoinMarketCap [23], such as BTC and ETH. Similarly, 64.3% (or 18) of the 28 exchange-target extensions target the top 30 exchanges in terms of their trading volume, including *Bittrex*, *Binance*, *Poloniex*, *Kraken*, *Hitbtc*, *Bitfinex* and *Coinbase*.

For the cryptocurrency wallets, as there is a lack of a ranking on their popularity, we calculate the cumulative numbers of reviews from mainstream application distribution platforms including Apple App Store and Google Play Store, and mark the wallets with 10,000 reviews as top popular ones. We find that 47.9% of the extensions target top popular wallets, including *Exodus*, *Trust Wallet*, *Metamask*, *Safepal*, *Atomic Wallet*, and *Coinbase Wallet*.

Domains and Registration Information. We list the top-level domains (TLDs), autonomous system number (ASN) information, domain registrars and registrant emails of the most frequently used domains in the malicious extensions, as shown in Table 5. In total, we have identified 34 TLDs, 28 unique network operators, 22 domain registrars. Apart from the common generic TLDs such as .com, .net and .org which take up the majority proportion (total of 61.35%), new generic top-level domains (e.g., .xyz) and country code TLDs (e.g., .io and .cn) are also becoming prevalent

Table 4. Top 5 Targeted Exchanges, Wallets and Cryptocurrencies

Targeted Exchanges			Targeted Wallets			Targeted Cryptocurrencies		
Exchange	#Extension	Rate	Wallet	#Extension	Rate	Cryptocurrency	#Extension	Rate
Bittrex	4	14.29%	Exodus	16	22.22%	BTC	119	71.69%
Binance	4	14.29%	TrustWallet	7	9.72%	ETH	88	53.01%
Poloniex	2	7.14%	MetaMask	6	8.33%	XMR	86	51.81%
Kraken	2	7.14%	Safepal	4	5.56%	BSV	78	46.99%
Hitbtc	2	7.14%	Ledger Nano	3	4.17%	SOL	77	46.39%

Table 5. Top 5 Domain Registration Information

Top 10 TLDs				Top 10 ASNs				Top 10 Registrars	
hlineTLD	Category	TLD Manager	Percentage	ASN	Description	Region	Percentage	Registar	Percentage
.com	gTLD	VeriSign Global Registry Services	48.45%	13335	Cloudflare, Inc.	US	33.33%	NameCheap, Inc.	29.10%
.org	gTLD	Public Interest Registry (PIR)	7.22%	25751	Conversant, Inc.	US	10.64%	MarkMonitor, Inc.	23.13%
.net	gTLD	VeriSign Global Registry Services	6.19%	22612	Namecheap, Inc.	US	10.64%	GoDaddy.com, LLC	14.93%
.io	ccTLD	Internet Computer Bureau Ltd.	5.67%	16509	Amazon.com, Inc.	US	7.09%	Dynadot, LLC	4.48%
.in	ccTLD	National Internet Exchange of India	2.45%	15169	Google LLC	US	4.96%	GANDI SAS	3.73%

due to their lower price and more relaxed regulation [34]. Due to a similar reason, *NameCheap* and *MarkMonitor* are more popular than *GoDaddy* although they have much lower global market shares (i.e., 9.4% and 0.8% according to DomainState [33]) than the latter (i.e., 52.6%).

Abused Third-party Services. We further seek to analyze the third-party services abused by the malicious extensions, as summarized by Table 9 in Appendix A.3. We first extract the domain names from 186 extensions. From them, we have identified 95 different third-party services. We further investigate them by manually visiting them and also looking them up in search engines. We find that most of the abused services can be categorized into two types: *development services* (41 out of 95, e.g., `fonts.googleapis.com`) and *cryptocurrency information/toolbox* (54 out of 95, e.g., `www.tradingview.com` and `connect.trezor.io`). Such findings reveal that the third-party services place no restrictions on extensions utilizing them, which could pose security threats if high-risk development services are abused.

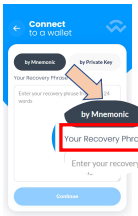
Answers to RQ1-1): We find a high prevalence of cryptocurrency-themed malicious extensions. They mainly target those popular and less-restrictive browsers, so Chrome accounts for the vast majority of malicious extensions. They mostly appear in official stores, but their distribution between official stores and alternative stores is balanced in terms of percentage. The cryptocurrency-themed malicious extensions stay available in the stores for a surprisingly long duration, partially because they can evade detection from those state-of-the-art anti-virus tools. This urges the necessity of domain-specific countermeasures.
The well-known services and cryptocurrencies remain the top targets of the malicious extensions while less-popular ones also attract a significant amount of attention from the attackers. Third-party services are at risk of being abused to facilitate the distribution of malicious extensions and to compromise user security.

5.1.2 Linking Developers of Malicious Extensions. Considering that the malicious developers may collude with each other to launch malicious campaigns targeting cryptocurrency-themed extensions, we are interested to identify the underlying connections among them, based on information from code bases (i.e., code base structures), registration information and transaction records.

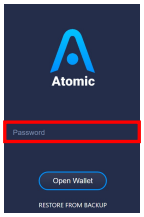
First, we correlate the extensions using the file structure and content similarity, as the near-duplicate extensions suggest the same developer [65]. To this end, we search for duplicates of highly individualized private libraries. Second, for extensions containing malicious domains, we link them if they have the same registrants or send credentials to the same domain. Third, we link the developers if the malicious wallet addresses embedded in the extensions are controlled by the same

Table 6. Top 6 Developers with the Most Linked Accounts

Author ID	Author Account	Extension ID	Linking Metrics File	Dom	Trans	Author ID	Author Account	Extension ID	Linking Metrics File	Dom	Trans
#1	exodus houss	e-xo-du-s-crypto-btc-wallet	✓	✓		#3	LINK DEV	apcmoigdfhnpdefifchnjapedkaceiob	✓	✓	
	Cryptoleadinc	e-xo-du-s-crypto-btc	✓	✓			Terra	cdgadjhfmbokfflmgjpiieifghkmpipc	✓	✓	
	Exodus Case	e-xo-dus-crypto-wallet	✓	✓			solana	dnnfplhmimbdhkomfncfdeijimdmlgfj	✓	✓	
	TradeCryptoNow	exodus-bitcoin-crypto-wallet	✓				Polkawallet	ffpbldifhhejjmjpcibcecggemkobkcf	✓	✓	
	Exodus LTD	exodus-btc-crypto	✓				Carnado Developer	kmfbhobieckelghhfhdndbfookcdhfje	✓	✓	
	Trust Coin	trust-wallet-coin	✓			#4	tpidev	aihogeigcnkcklfaljfimkefkmbmlomi	✓	✓	✓
	Trust Wallet	trust-wallet-nft	✓	✓			tpidev	jjdbklmemcpdklojpniabhfhclngpppe	✓	✓	✓
	trust view	trust-wallet-qr-code		✓			tpidev	oheacmjjkbcbpgmdljkbcaopcmpjfloj	✓	✓	✓
#2	atomicwallet.io	atomic-wallet-io	✓	✓			tpidev	caopgikafahfcgbfaagibfelkoaehjjp	✓	✓	✓
	atomicwallet.io	atomic-wallet-exchange	✓	✓		#5	coinbase, SSLD	scoinbase-wallet-crypto-wallet		✓	
	Ledger Live Extension	ledger-nano	✓	✓			safepal wallet, LLS	safepal-crypto-wallet		✓	
	Ledger Nano	live-ledger-nano	✓	✓			safepal wallet, Ltd	safepal-wallet-crypto-wallet	✓	✓	
	Ledger	nano-ledger-wallet-live	✓	✓			safepal wallet, Ltd	safepal-wallet-crypto-wallet	✓	✓	
	Coinbase Wallet	Coinbase Wallet	✓			#6	Exodus Movement, Inc.	exodus-cryptoss-bitcoin-wallet	✓	✓	
	Trust Wallet	trust-wallet-s	✓				Exodus Wallet	exodus-crypto-wallet-btc	✓	✓	
							Exodus Team	exodus-wallet-extension	✓		
							tebi	exodusrwinawallet	✓		

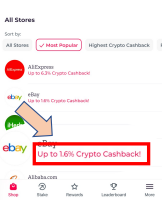


(a) Phishing Extension Stealing Wallet Account

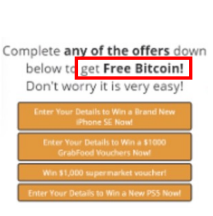


(b) Phishing Extension Stealing Password

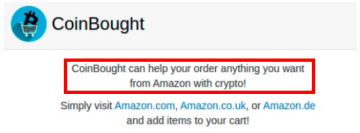
(c) Malicious Miner



(d) Cashback Scam



(e) Bitcoin Giveaway Scam



(f) Fake Transaction Proxy Scam

(g) Adware Triggering A Pop-up Window

(h) Disguised Gambling Service

Fig. 4. Examples of Phishing, Mining and Scam Extensions

attacker. For example, we track the transactions among the addresses, and link the change addresses and addresses involved in multi-input transactions [56]. Among the 186 malicious extensions, we have linked 56 of them to 17 developers, each of which accounts for at least two extensions. The relationship graph is shown in Figure 8 in Appendix A.4. We list the top six developers with the largest numbers of extensions in Table 6. For example, one developer creates seven phishing extensions from six accounts, targeting four wallets including *Ledger Nano Wallet* (3), *Atomic Wallet* (2), *Coinbase Wallet* (1), *Trust Wallet* (1).

Answer to RQ1-2): Based on the code structure and content similarity, shared registrant/registrar information, and transaction-based connections, we can link 56 malicious extensions to 17 adversarial entities.

5.2 RQ2: Malicious Extension Characterization by Category

Our analysis in RQ1 has suggested the prevalence of cryptocurrency-themed malicious extensions. We further investigate their behaviors to understand how they trick the victims. We install the confirmed 186 malicious extensions in our confined testbed (see Section 4.3), interact with them, and inspect their behaviors.

5.2.1 Phishing Extensions (65). We list the full list of the identified phishing extensions in Table 10 in Appendix A.5. The vast majority (61/65) of the phishing extensions impersonate legitimate extensions, while the rest four forge web pages. These phishing extensions appear only in the official stores of Chrome and Firefox. The Firefox browser is their main target, accounting for 43 malicious extensions.

Impersonated Services. Phishing extensions tend to impersonate wallet services. Out of the 65 phishing extensions, most (59) target wallets, a few (4) target exchanges and the rest two are exceptions (they aim to collect user-specific information and their wallet addresses). The phishing extensions target well-known cryptocurrency wallets with large numbers of users, including *Exodus Wallet* (16), *Trust Wallet* (7), *Metamask Wallet* (6), *SafePal Wallet* (4), *Atomic Wallet* (3), hardware wallets (e.g., 3 on *Ledger Nano Wallet*).
Malicious Behaviors. The phishing extensions impersonate legitimate ones to steal *passwords* or *wallet accounts* of the victims. Either of them will lead to full control of the wallet/user account.

- *Wallet Account.* 57 extensions mimic a wallet loading page to prompt users to key in the backup phrases, as shown in Figure 4(a).
- *Password.* 6 extensions mimic a wallet login page to prompt users to key in the login credentials, as shown in Figure 4(b).

5.2.2 Mining Extensions (22). We list the identified mining extensions in Table 11 in Appendix A.5. Despite the ban enforced by Chrome, Firefox, and Opera official stores, over half (12/22) of the mining extensions still circumvent the restriction and appear in them: Chrome (10), Firefox (1), and Opera (1). The other half (10/22) are from the third-party stores: *Crx4Chrome* (8) and *Guge* (2).
Mined Cryptocurrencies and Mining Pools. The mining extensions mostly (11/22) mine the Monero (i.e., XMR). This is highly likely due to its *RandomX* mining algorithm which optimizes CPU mining and penalizes GPU and AISC (application-specific integrated circuit) mining. Despite a lower efficiency compared to Monero, Bitcoin remains popular as the target of four extensions. The mining extensions fetch tasks from popular mining pools, including *Coinhive* (6), *CryptoLoot* (3), *CoinImp* (2), *Mineralt* (1), *MoneroOcean* (1), *CCGMining* (1), and *XMR Miners Club* (1).
Malicious Behaviors. At runtime, most mining extensions discreetly drain the computational resources. Specifically, they could quickly occupy most of the CPU resource (over 90%). We have also observed their frequent communication with the mining pools in the network traffic. The malicious behaviors can be divided into three categories:

- *Mining Unlocking* (14 out of 22). As the official stores have banned mining extensions, they bypass the vetting process and provide the users with the in-browser mining functionality.
- *Mining Plundering* (3 out of 22). They abuse the victim's computational resources to mine cryptocurrencies for the attacker. An example is KMine, as shown in Figure 4(c).
- *Invalid Mining Blocking* (5 out of 22). These extensions claim to be capable of preventing in-browser mining, but fail to do so.

5.2.3 Scam Extensions (75). This category of extensions is the most prevalent among all. We list the identified scam extensions in Table 12 in Appendix A.5. In general, the scam extensions target popular platforms and cryptocurrencies to maximize their illicit income. The vast majority (54/75) are developed for Chrome (50 on *Chrome Web Store* and 4 on *Guge*), and the rest (21/75) are for Firefox. All of these extensions target BTC (56) or ETH (30), with 11 exceptions.
Malicious Behaviors. The scam extensions exhibit diversified malicious behaviors. Based on the scam techniques, we further summarize them into the following 8 subcategories.

- *Account Manager Scam* (22 out of 75). These extensions promote themselves as the account management tools and trick victims into creating insecure wallets with compromised credentials including the private key and backup phrases.
- *Cashback Scam* (10 out of 75). These extensions pretend to be cashback providers for shopping on multiple well-known merchants such as eBay, iHerb, and Ali-express, as shown in Figure 4(d). They typically advertise reasonable cashback up to several percent, but they never fulfill the money payback.

- *Shopping Proxy Scam* (9 out of 75). This type of extension redirects victims to websites that are disguised as shopping agents. They promise to purchase goods on behalf of the user after receiving payments in cryptocurrency, but never fulfill their promise afterward. An example of such a scam is shown in Figure 4(f).
- *Giveaway Scam* (9 out of 75). These extensions redirect victims to websites that advertise fake generous rewards, such as cash rewards, smartphones, and cryptocurrencies. They require the victims to complete a series of insecure tasks, such as visiting compromised websites or providing sensitive personal information. An example of such a scam is shown in Figure 4(e).
- *Integrated Service Portal Scam* (9 out of 75). These extensions pretend to be portals to access multiple cryptocurrency services. The user will be redirected to the malicious websites upon clicking on the buttons from the extensions.
- *False Information Scam* (6 out of 75) These extensions mimic cryptocurrency information providers and provide fake information to the victims, such as fake news or incorrect prices.
- *Investment Scam* (7 out of 75). These extensions redirect victims to websites that lure them with promising investment opportunities, such as the extremely high interest in the cryptocurrency deposit and invest in "promising" cryptocurrencies for capital gain.
- *Address Manipulation Scam* (3 out of 75). These extensions embed an adversary-controlled wallet address as the fund recipient. Whenever the victim initiates a transfer, the cryptocurrency will be deposited into the attacker's account.

5.2.4 Adware Extensions (16). We list the identified adware extensions in Table 13 in Appendix A.5. Among the 16 adware extensions, 13 are identified from *Chrome Web Store* and the rest 3 are from *Firefox Add-ons*. Various services are used as undercover to conceal their malicious intentions, including crypto-news platforms (7), coin price trackers (5), coin rewards providers (3), and blockchain forums (1).

Malicious Behavior. When using adware extensions, the victim users will be presented with various types of target advertisements, such as shopping sites (7), games (6), and job markets (1). There are two ways of presenting the unconsented advertisements:

- *Redirected Windows* (10 out of 16). The advertisement windows are launched as redirection pages only when the victim clicks on the buttons in the extensions.
- *Pop-up Windows* (6 out of 16). The advertisement windows will be automatically triggered when the user opens the extensions. An example is shown in Figure 4(g), the extension launches a pop-up window of advertisement sites upon the user initiates the extension.

5.2.5 Illicit Services (8). The identified extensions of illicit services mainly involve gambling and pornography. They are listed in Table 14. Most (5 out of 8) of them pretend to be benign cryptocurrency exchanges with fake interfaces, as shown by the online casino extension in Figure 4(h). Only three extensions in this category directly market themselves as online casinos. The users will be redirected to the online casinos or will be presented with pornographic content, triggered after clicking a certain button such as login.

Answer to RQ2: We characterize the malicious extension on the fine-grain level, according to the 5 categories: phishing malware (deceiving the users into revealing their sensitive information), mining malware (abusing computation resources for illicit gains), scam malware (deceiving the users into transferring to adversary-controlled wallet addresses), adware (throwing advertisements and click frauds) and gambling/porn (covert illegal services). Among them, phishing and scam are the major forms of illicit activities.

5.3 RQ3. Financial Impacts of Malicious Extensions

In this section, we investigate the financial losses caused by cryptocurrency-themed malicious extensions. Due to unavailability of the attack data, e.g., the amount of mined coins by the mining extensions and the illicit incomes from adware, porn, etc., we focus on traceable transactions involving wallet addresses controlled by malware developers. We identify wallet addresses from the malicious extensions and study their characteristics (i.e., transaction amounts and money flows).

5.3.1 Malicious Addresses Identification. We adopt a two-step approach to identify and further expand our list of malicious wallet addresses.

Extracting Malicious Seed Addresses. We first search the code bases of all identified malicious extensions for strings that match the format of cryptocurrency wallet addresses. We scan for BTC and ETH wallet addresses as they are the top targets. To match BTC addresses, we use two regular expressions to represent the patterns including *(1|3)[0-9a-km-zA-HJ-NP-Z]{24,33}* and *(bc1)[0-9a-zA-HJ-NP-Z]{39}*. To match ETH addresses, we use *(0x)[0-9a-fA-F]{40}*.

From the obtained strings, we first filter out invalid ones by verifying with online address checking tools (e.g., AddressChecker [3]). To further narrow down our search space, we remove addresses associated with well-known services (e.g., exchanges) and benign purposes (e.g., donation), and dead addresses that have no transaction records. Then, we confirm a set of malicious addresses, denoted as *seed addresses* hereafter, by checking with online blacklists (e.g., CryptoScamDB [28], BitcoinAbuse [9], and EtherScan[37]). To pin down the financial losses onto the relevant extensions, we focus on transactions from and to each address within the lifecycle of the embedding extension.

Identifying Colluding Addresses. Starting from each seed address, we expand our address list by monitoring those controlled by the same entity, known as the *malicious-by-association* [90]. For example, if a seed address transfers coins to another address immediately after receiving incoming payments from victims, we treat the two addresses as colluding addresses and consider that they belong to the same attacker. A typical example of this kind is shown in Figure 9(a) where outgoing transactions almost overlap with the incoming ones. Similarly, we mark all the identifiable outgoing fund transfer addresses, change addresses, and addresses involved in multi-input transactions [56] with the seed address as malicious. In particular, for the outgoing fund transfer addresses, we track the next address using online tools (e.g., WalletExplorer [85] and OXT [86]) until some known services (e.g., exchanges or cryptocurrency mixing services) are reached or no other outgoing transactions are recorded. Considering a large number of relevant transactions as we continue tracking the outgoing fund transfer addresses in depth, we restrict the maximum search depth to 5 (5 transactions away from a seed address). We refer to the set of addresses expanded from a seed address as the *colluding addresses* hereafter.

Overall, we identify 10 malicious BTC seed addresses with 38 colluding addresses, and 12 ETH seed addresses with 29 colluding addresses. Most (18/22) of the addresses are embedded in distinct extensions from different developers, with four exceptions embedded in two extensions. Almost all (20/22) seed addresses are found among the most prevalent malware categories, i.e., scam (15) and phishing (5). No seed address is shared by different extensions, and no developer can be linked through the usage of the same address. We list the full BTC and ETH addresses in Appendix A.6.

5.3.2 Characterizing Financial Impacts. With the identified wallet addresses, we characterize the financial impacts from the perspectives of financial loss estimation and money flow analysis.

Financial Loss Estimation. To estimate the total financial losses, we first calculate the relevant incoming transactions to the seed addresses. As the seed addresses are embedded inside the malicious extensions, these transactions directly account for the incurred losses, referred to as *primary losses* hereafter. To reflect the impacts of the malicious extensions more accurately, we

particularly focus on the periods overlapped with their lifespans (i.e., from the release date till the removal date), noting that many malicious addresses exist before the release of the malicious extensions. In addition to the primary losses, we also calculate the cumulative incoming transactions into the colluding addresses over the same period, as an indicator to characterize the potential impacts relevant to the malicious extensions. Such losses are referred to as *secondary losses* hereafter.

Based on the transaction records retrieved from BlockCypher [10], we have tracked a total of 1070 transactions into the seed addresses and 456 into the colluding addresses. Most of the addresses have been involved in attack campaigns since 2013, and have accumulated 32.40 BTC and 26.28 ETH primary losses, equivalent to $1,006,610 as per the exchange rate in June 2022. The secondary losses are accumulated to include 18.32 BTC and 24.46 ETH, valued at $583,576. Considering that we are unable to retrieve all extensions and wallet addresses, as well as background attack activities, the estimated financial losses are merely the lower bound of the damage caused by the malicious cryptocurrency-themed extensions.

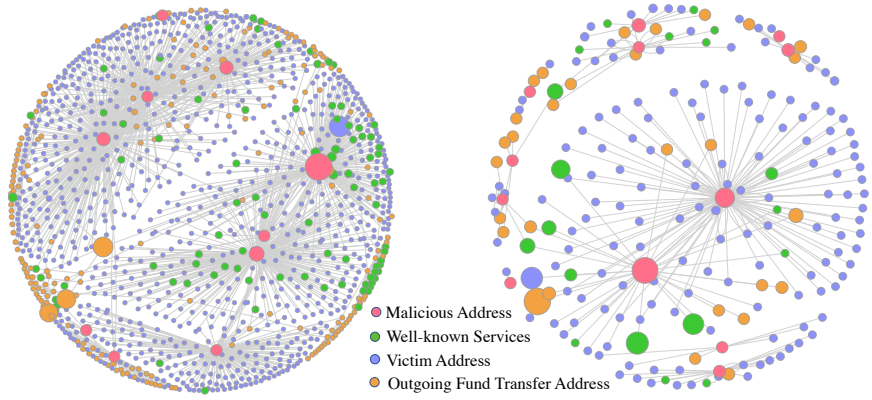
We observe a huge deviation in the amount of cryptocurrencies per transaction, ranging from 0.00000003 to 21.39 BTC (median value 0.00012 BTC), and from 0.001 to 19.55 ETH (median value 0.1 ETH). In general, there is a trend of the declining amount per transaction over time, plausibly due to the rapid appreciation of digital coins. For each address, it is a common trend that the transaction frequency decreases over time, indicating the loss of active users or the removal of the extension from the stores. We present a case study of the most profitable address in Appendix A.7.

Money Flow Analysis. Given the estimated amount of transactions through the malicious wallet addresses, we further aim to demystify the dynamics of the involved illegal activities associated with the malicious extensions by answering: (1) Who are depositing into the malicious addresses? (2) Where is the money going? (3) How are the transactions/addresses connected?

Impacted Victim Estimation. We estimate the number of victims based on the number of unique wallet addresses that deposit into the seed addresses. To better reflect the impacts from the extensions, we adopt the similar time frames used in financial loss estimation. In total, we identified 989 victims, which is an upper bound considering that a single user might own multiple accounts and wallet addresses. However, due to the limited time of our evaluation (around a year), we merely reveal the tip of an iceberg, suggesting the significant impact on the cryptocurrency stakeholders in reality. Among the identified victims, we have observed that the majority transfer to only one malicious address, and only one (BTC wallet owner) of them transfers to two addresses, showing that almost all victims tend to be more cautious after experiencing financial losses.

Money Flow Tracking. To understand the money flow patterns, we focus on the chains of transactions that originate from malicious addresses. They further flow into different outgoing fund transfer addresses until reaching the terminating node (i.e., well-known services or non-outgoing wallet) or the maximum search depth. From the transaction records, we identified 134 exchanges/cryptocurrency mixing services (105 for BTC and 29 for ETH). At the same time, we find that carefully designed plans are adopted to purposely obscure the money flows. One strategy is to utilize multiple chains of transactions to avoid being tracked. Another strategy is that adversaries use separate addresses to collect the illicit income and assemble them into their main address afterward via 2 to 3 layers of manipulated transactions (i.e., 2 to 3 intermediate transactions). This has been found common among seed addresses embedded inside the malicious extensions. For example, the address *36456e4vXkJsqNJoAYGT3jaziGRCboe4ca* uses 4 different routes and 2-layer transactions to assemble their illicit income to their main account at *3CrDUGkhPREv8XEjQMTtMiYnsXQcXL2qq1*.

Address Clustering. Utilizing the derived information regarding the victims and the money flows, we further attempt to establish the relationships among the victims, attackers, and the terminating services from a broader point of view. As shown in Figure 5, we plot nodes representing the four types of addresses. The node sizes represent the relative cryptocurrency amounts. The



(a) BTC Transaction Clusters (b) ETH Transaction Clusters

Fig. 5. Clustering of BTC and ETH Transactions with Malicious Addresses

transactions among them are represented as edges. We have observed that each seed address forms a transaction cluster, leading to 22 clusters in total (10 for BTC and 12 for ETH). For malicious addresses with large numbers of outgoing fund transfers, we believe they are among the colluding accounts controlled by an adversarial developer since they heavily rely on benign untraceable services to "launder" their illicit income and assemble it into their accounts afterward. For the malicious addresses without outgoing transfers, they are considered owned by the adversary.

Answer to RQ3: We have identified 22 distinct malicious seed addresses and their 67 colluding addresses. The identified extensions account for an accumulated financial loss of $1,006,610. By further tracking the money flows associated with the addresses, we link them with 989 unique upstream victims and 134 unique downstream well-known services, forming 10 and 12 transaction clusters for BTC and ETH separately.

5.4 RQ4: Feature Relevance

In this RQ, we seek to interpret the relevance and distinguishability of the features we used in each stage of malicious extension detection in Section 4, to facilitate the differentiation of the emerging malicious extensions by the users, and the detection by anti-malware mechanisms.

5.4.1 Features in Preliminary Filtering. We include user reviews, ratings, and download numbers.

User Reviews. Reviews with negative sentiment turn out to be indicative of the maliciousness among the extensions. We find that 17% of the malicious extensions have at least one review with negative sentiment, and that 42% of extensions with negative-sentiment reviews are malicious. Furthermore, we also find that the words strongly suggesting illegal activities (e.g., "*theft*", "*cheat*", "*steal*") is at least two times more prevalent among malicious extensions, in comparison to generically negative words (e.g., "*bad*", "*horrible*").

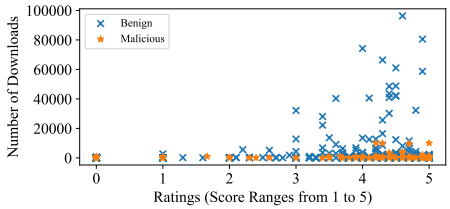


Fig. 6. Distribution of Ratings and Downloads

Ratings and Download Numbers. We further examine the ratings and download numbers of both benign and malicious samples, as shown in Figure 6 where we include randomly selected 1000 benign extensions and all the 186 confirmed malicious extensions. We present the following two findings that the users may consider before they download and install a cryptocurrency-themed

Table 7. Odds Ratio for Selected Top Relevant Features between Malicious and Benign Extensions

Extension Types	Permission					Function Types					Variable Types					Browser API Types				
	P1	P2	P3	P4	P5	F1	F2	F3	F4	F5	V1	V2	V3	V4	V5	B1	B2	B3	B4	B5
Phishing	9.51	0.26	0.18	0.20	0.35	0.62	1.81	2.95	2.79	2.01	0.21	0.98	0.55	0.89	1.42	2.84	0.00	0.00	1.13	0.00
Mining	9.05	**2.55**	**3.90**	**1.85**	**2.47**	1.79	0.45	1.60	1.42	2.67	1.53	3.29	1.03	0.54	1.29	6.62	0.00	21.95	6.00	6.62
Scam	2.52	0.83	2.72	0.98	0.73	0.50	4.24	1.14	1.00	1.51	0.55	1.35	0.65	1.00	0.42	0.00	2.21	0.00	1.33	2.21
Adware	12.79	0.85	0.72	0.76	0.76	2.53	0.64	2.81	2.48	0.38	1.02	3.49	1.26	0.27	1.45	19.86	12.64	0.00	7.11	0.00
Gambling/Porn	**33.73**	0.21	1.90	0.25	0.88	6.67	1.69	5.62	4.95	0.45	0.55	2.32	1.88	0.40	1.29	0.00	0.00	0.00	0.00	0.00
Malicious Overall	**3.26**	0.63	1.52	0.69	0.75	0.21	**2.30**	1.92	1.74	1.62	0.55	**1.41**	0.71	0.80	0.89	4.11	2.44	2.44	2.36	1.62
Benign	0.31	1.58	0.66	1.45	1.34	4.67	0.43	0.52	0.57	0.62	1.83	0.71	1.40	1.25	1.12	0.24	0.41	0.41	0.42	0.62

Permissions: P1: file://*; P2: storage; P3: http://*/*; P4: tabs; P5: < *all_urls* > **Function Types**: F1: decodeURIComponent(); F2: parseFloat(); F3: setTimeout(); F4: clearTimeout(); F5: clearInterval(); **Variable Types**: V1: Template; V2: Punctuator; V3: RegularExpression; V4: Numeric; V5: String; **Browser API Types**: B1: identity; B2: app.runtime; B3: system.cpu; B4: webRequest; B5: permissions;

extension. First, the malicious extensions tend to have low download numbers: the majority have fewer than 500 downloads while the benign ones could easily have 50,000 and above. Second, there is a huge discrepancy in the rating scores among malicious extensions. Some have very low ratings (0 to 1 star), which means the victims have complained about the extensions. Others have abnormally high ratings (4 stars and above), which can be attributed to a large number of fake rating scores. As a consequence of such manipulation, the proportion of malicious extensions rated 4 stars and above is 45% which is comparable to that of benign extensions at 40%. Therefore, the user should avoid relying merely on the rating scores.

5.4.2 Programmatic Features for Detection. We employ a total of 33 programmatic features in our classifier (see Section 4.2). To measure the relevance of each feature to cryptocurrency-themed malicious extensions, we calculate the Odds Ratio [76] between our malicious extension set (186 extensions) and the benchmark benign extension set (186 randomly sampled extensions). By ranking the absolute differences in the Odds Ratios between the two sets of extensions, we have identified the most (positively or negatively) relevant five permissions, function types, and variable types, as shown in Table 7. Note that the Odds Ratio implies positive relevance (larger than 1), negative relevance (closer to 0 and smaller than 1), and no relevance (near 1) between the features and the malicious/benign property of an extension. Overall, most programmatic features (9 out of 15) are negatively relevant to the malicious extensions, and positively relevant to the benign ones.

Permissions. The file access permission (P1) shows high positive relevance among all malicious extension categories, indicating their general interest to gain access to the user's files. In contrast, they are less engaged in web communication (P2-P5), given their primary goal of executing carefully designed malicious behaviors. One exception is the mining extension that constantly visits mining pools, and thus this category intensively utilizes the web communication permissions.

AST Features. Four function types (F2-F4) and one variable type (V2) show positive relevance. This indicates that malicious extensions tend to leverage a particular set of functions to implement their malicious logic, rather than other diversified features such as web communication (e.g., F1).

5.4.3 Features for Confirmation. Our malware confirmation relies on three categories of features. In this section, we discuss their relevance.

Malicious Elements. Nearly half of the identified malicious extensions are embedded with malicious URLs or wallet addresses. More specifically, for scam extensions, the malicious wallet addresses are embedded as the recipient of the transactions from the victims. For phishing extensions, the malicious URLs are embedded to intercept the victim's credentials. For mining extensions, the malicious pool addresses are embedded for mining task retrieval, and the attacker's wallet addresses are included to harvest the mined cryptocurrencies. For adware/porn/gambling extensions, malicious URLs are embedded to redirect the victim to illegal services.

Network-level Features. The behavior of communicating with malicious domains is prevalent among phishing and mining extensions. We find that each of them communicates with only one or

two malicious domains though, which are much fewer than the benign domains they connect to, to hide their malicious activities. For example, the phishing extension *Coinbase Wallet* connects to only one malicious domain among 45 domains it connects to, and the mining extension *KMine* connects to two among 27 domains.

System-level Features. The high consumption of system resources is obviously exhibited among mining extensions, and is less typical among other categories. We find that 42% of the mining extensions show high usage of system resources with over 90% CPU utilization rate at runtime. For example, *Monero Browser Crypto Miner* and *earnsurfing* use up to 90% CPU on average during execution while the phishing extension *Atomic Wallet* uses up to 30% and the benign extension *MetaMask* uses merely 17% on average.

Besides the features used in our work, we notice that the invoked browser APIs are also taken as features for malicious extension detection [73]. Therefore, we study their effectiveness and relevance based on our dataset. Our study is presented in Appendix A.8, and the Odds Ratio values are listed in the last five columns in Table 7.

Answers to RQ4: First, 15 programmatic features are identified, significantly differentiating cryptocurrency-themed malicious extensions from benign ones. The behavioral features exhibit defining characteristics in confirming malicious extensions. All these features can be utilized by the countermeasures against cryptocurrency-themed malware. Second, the metadata features, especially the rating scores, are evidenced to be subject to the manipulation of attackers. This should raise the awareness of the users who rely on such features to distinguish malware.

6 DISCUSSIONS

Implications. Our findings reveal that cryptocurrency-themed extensions are exposed to the threats targeting both the cryptocurrency community and the browser extension ecosystem.

Towards Efficient Detection and Warnings. First, it is necessary to construct and maintain a comprehensive and up-to-date dataset, containing the distinctive features specific to cryptocurrency-themed extensions as demonstrated in Table 7, to empower their real-time detection. Second, the significant financial losses should alert the extension users, store operators, and regulators. Efficient channels (i.e., platform-level warning and feedback mechanisms) should be deployed to inform the users of attack campaigns.

Towards Secure Payments. Cryptocurrency payment services are abused for financing illegal services including gambling and pornography. We call for stricter regulations on the "in-extension payment", similar to that of the in-app payment in the mobile app ecosystem.

Limitations. To the best of our knowledge, this is the first work that systematically investigates cryptocurrency-themed malicious extensions. However, it carries several limitations that should be targeted in future work. First, despite the usage of a large number of cryptocurrency-related keywords and their anagrams to discover the cryptocurrency-themed extensions, it is possible that we still miss some extensions that attempt to evade detection by omitting all the relevant keywords. Given their low profile and the negligible consequent impacts, our study retains the fidelity in characterizing the majority of the cryptocurrency-themed extensions. Second, our work focuses on investigating the *status quo* of the cryptocurrency-themed malicious extensions, and we have not fully automated our detection approach yet. Although we reuse existing applicable techniques/tools, interaction from analysts is sometimes required. For example, the confirmation of malicious extensions requires the analysts to interact with them (e.g., registration, log-in, and transferring coins) to trigger their behaviors. For future work, especially in practice, a fully automated detection approach should be developed.

7 RELATED WORK

In this section, we first review the existing works studying the malicious browser extensions. Then we briefly introduce the cryptocurrencies and discuss the common attacks targeting them.

Analysis of Malicious Browser Extensions. There is rich literature for detecting malicious extensions [7, 8, 67, 71, 80], leveraging various techniques including static, dynamic, and hybrid analysis. Pantelaios et al. [69] proposed a static detection system that targets the delta of the extensions. It monitored nearly one million extensions and identified 143 malicious ones. Somé et al. [73] constructed a static analyzer and have identified 197 vulnerable extensions which allow the web applications to abuse their privileges including accessing APIs and sensitive user data. Prior to this work, the misuse of excessive permissions has raised attention from the research community [30, 48, 57, 75]. Various techniques have been proposed to detect such vulnerabilities [7].

Dynamic analysis has shown effectiveness for identifying malicious extensions through monitoring extension behaviors. Hulk [52] triggers and detects malicious behaviors through carefully crafted web pages. It discovered 130 malicious extensions. Thomas et al. [82] proposed a multi-staged pipeline to capture the malicious activities and characterize the revenue chain associated with the advertisement-injection extensions. Xing et al. [93] propose a framework named Expector to facilitate the detection of advertisement injection among extensions.

Jagpal et al. [65] designed and implemented a malicious extension detection system, leveraging hybrid analysis on extensive dimensions through static and dynamic analysis. In comparison, our proposed approach targets the malicious behaviors specific to the cryptocurrency-themed malicious extensions. Additionally, we cover a wider evaluation and filtering dimensions including dynamics of user reviews, number of downloads, online times, etc.

Cryptocurrencies and Relevant Attacks. There is a rich literature on cryptocurrency-themed crimes, including Ponzi schemes [16, 17, 59], market manipulation [15, 66, 83], phishing [70, 88, 91, 92] and cryptojacking [12, 29, 79]. In addition, given their dependency on the blockchain, most cryptocurrencies suffer from vulnerabilities and attacks originating from it [6, 13, 14, 44]. To the best of our knowledge, we are the first to systematically characterize the crimes related to cryptocurrency-themed extensions.

8 CONCLUSION

In this work, we characterize the cryptocurrency-themed malicious extensions. Specifically, we continuously monitor various extension stores for 18 months and collect cryptocurrency-themed extensions. Leveraging a lightweight detection approach, we identify 186 malicious extensions. We then reveal their distributions and development ecosystem, categories, financial implications, and defining features. To the best of our knowledge, this is the first systematic study of the *status quo* of cryptocurrency-themed malicious extensions. Our work should raise an alert to the extension users, and would encourage the extension store operators to enact dedicated countermeasures.

ACKNOWLEDGMENTS

We thank the shepherd Prof. Emiliano De Cristofaro and anonymous reviewers for improving this manuscript. This research is supported by Singapore Ministry of Education Academic Research Fund Tier 3 under MOE's official grant number MOE2017-T3-1-007. This research is also supported by the University of Queensland under Global Strategy and Partnerships Seed Funding and the NSRSG grant 4018264-617225, National Key R&D Program of China (2021YFB2701000), the National Natural Science Foundation of China (grant No.62072046), and the Fundamental Research Funds for the Central Universities (HUST 3004129109).

REFERENCES

[1] AdBlock. 2009. https://getadblock.com. (2009).
[2] Add-on Policies. Visited in July 2022. https://extensionworkshop.com/documentation/publish/add-on-policies. (Visited in July 2022).
[3] Address Checker. Visited in July 2022. http://addresschecker.eu. (Visited in July 2022).
[4] Alternative Extension Distribution Options. Visited in July 2022. https://developer.chrome.com/docs/extensions/mv3/external_extensions. (Visited in July 2022).
[5] AST Explorer. Visited in July 2022. https://astexplorer.net. (Visited in July 2022).
[6] Atzei, Nicola and Bartoletti, Massimo and Cimoli, Tiziana. 2017. A Survey of Attacks on Ethereum Smart Contracts SoK. In *POST*. 164–186.
[7] Sruthi Bandhakavi, Nandit Tiku, Wyatt Pittman, Samuel T. King, P. Madhusudan, and Marianne Winslett. 2011. Vetting Browser Extensions for Security Vulnerabilities with VEX. *Commun. ACM* 54, 9 (2011), 91–99.
[8] Barrera, David and Kayacik, H. Güneş and van Oorschot, Paul C. and Somayaji, Anil. 2010. A Methodology for Empirical Analysis of Permission-Based Security Models and Its Application to Android. In *CCS*. 73–84.
[9] Bitcoin Abuse Database. Visited in July 2022. https://www.bitcoinabuse.com. (Visited in July 2022).
[10] BlockCypher. Visited in July 2022. https://www.blockcypher.com. (Visited in July 2022).
[11] Browser Market Share Worldwide. Visited in July 2022. https://gs.statcounter.com/browser-market-share. (Visited in July 2022).
[12] Maurantonio Caprolu, Simone Raponi, Gabriele Oligeri, and Roberto Di Pietro. 2021. Cryptomining makes noise: Detecting cryptojacking via Machine Learning. *Computer Communications* 171 (2021), 126–139.
[13] Chen, Ting and Li, Zihao and Zhu, Yuxiao and Chen, Jiachi and Luo, Xiapu and Lui, John Chi-Shing and Lin, Xiaodong and Zhang, Xiaosong. 2020. Understanding Ethereum via Graph Analysis. *ACM Trans. Internet Technol.* 20 (2020).
[14] Chen, Ting and Zhu, Yuxiao and Li, Zihao and Chen, Jiachi and Li, Xiaoqi and Luo, Xiapu and Lin, Xiaodong and Zhange, Xiaosong. 2018. Understanding Ethereum via Graph Analysis. In *IEEE INFOCOM*. 1484–1492.
[15] Chen, Weili and Wu, Jun and Zheng, Zibin and Chen, Chuan and Zhou, Yuren. 2019. Market Manipulation of Bitcoin: Evidence from Mining the Mt. Gox Transaction Network. In *IEEE INFOCOM*. 964–972.
[16] Chen, Weili and Xu, YueJin and Zheng, Zibin and Zhou, Yuren and Yang, Jianxun Eileen and Bian, Jing. 2019. Detecting "Pump Dump Schemes" on Cryptocurrency Market Using An Improved Apriori Algorithm. In *SOSE*. 293–2935.
[17] Chen, Weili and Zheng, Zibin and Cui, Jiahui and Ngai, Edith and Zheng, Peilin and Zhou, Yuren. 2018. Detecting Ponzi Schemes on Ethereum: Towards Healthier Blockchain Technology. In *WWW*. 1409–1418.
[18] CipherTrace. 2020. Cryptocurrency Crime and Anti-Money Laundering Report. https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report. (2020).
[19] Coin98 Wallet. Visited in July 2022. https://chrome.google.com/webstore/detail/coin98-wallet/aeachknmefphepccionboohckonoeemg. (Visited in July 2022).
[20] Coinbase. 2021. Coinbase Wallet introduces new browser extension. https://blog.coinbase.com/coinbase-wallet-introduces-new-browser-extension-dd067403b86. (2021).
[21] Coinbase Exchange Extension. Visited in July 2022. https://chrome.google.com/webstore/detail/coinbase-wallet-extension/hnfanknocfeofbddgcijnmhnfnkdnaad. (Visited in July 2022).
[22] Coinbase Wallet extension. Visited in July 2022. https://chrome.google.com/webstore/detail/coinbase-wallet-extension/hnfanknocfeofbddgcijnmhnfnkdnaad. (Visited in July 2022).
[23] CoinMarketCap. Visited in July 2022. https://coinmarketcap.com/rankings/exchanges. (Visited in July 2022).
[24] CoinMarketCap. Visited in July 2022. https://coinmarketcap.com. (Visited in July 2022).
[25] Compare cryptocurrency wallets. Visited in July 2022. https://www.finder.com.au/view-cryptocurrency-wallets. (Visited in July 2022).
[26] Crx4Chrome. Visited in July 2022. https://www.crx4chrome.com. (Visited in July 2022).
[27] Crypto Price Tracker. Visited in July 2022. https://chrome.google.com/webstore/detail/crypto-price-tracker/fpkhlnacfhciopipcjpcjmkpldbogaeo. (Visited in July 2022).
[28] CryptoScamDB. Visited in July 2022. https://cryptoscamdb.org. (Visited in July 2022).
[29] Hamid Darabian, Sajad Homayounoot, Ali Dehghantanha, Sattar Hashemi, Hadis Karimipour, Reza M Parizi, and Kim-Kwang Raymond Choo. 2020. Detecting cryptomining malware: a deep learning approach for static and dynamic analysis. *Journal of Grid Computing* 18, 2 (2020), 293–303.
[30] Louis F. DeKoven, Stefan Savage, Geoffrey M. Voelker, and Nektarios Leontiadis. 2017. Malicious Browser Extensions at Scale: Bridging the Observability Gap between Web Site and Browser. In *CSET*.
[31] Alberto Falk Delgado, Gregory Garretson, and Anna Falk Delgado. 2019. The language of peer review reports on articles published in the BMJ, 2014-2017: an observational study. *Scientometrics* (2019), 1225–1235.
[32] Developer Program Policies. Visited in July 2022. https://developer.chrome.com/docs/webstore/program_policies. (Visited in July 2022).

[33] Domain State. Visited in July 2022. https://www.domainstate.com. (Visited in July 2022).
[34] Kun Du, Hao Yang, Zhou Li, Haixin Duan, and Kehuan Zhang. 2016. The Ever-Changing Labyrinth: A Large-Scale Analysis of Wildcard DNS Powered Blackhat SEO. In *USENIX Security*. 245–262.
[35] EQUAL Wallet. Visited in July 2022. https://chrome.google.com/webstore/detail/equal-wallet/blnieiiffboillknjnepogjhkgnoapac. (Visited in July 2022).
[36] Esprima. Visited in July 2022. https://esprima.org. (Visited in July 2022).
[37] Etherscan. Visited in July 2022. https://etherscan.io. (Visited in July 2022).
[38] Europol Spotlight - Cryptocurrencies - Tracing the evolution of criminal finances. 2021. https://www.europol.europa.eu/media-press/newsroom/news/digital-gold-rush-debunking-common-myths-criminal-use-of-cryptocurrencies. (2021).
[39] ExtAnalysis. 2019. https://github.com/Tuhinshubhra/ExtAnalysis. (2019).
[40] Extension Dataset. Visited in July 2022. https://github.com/browserExtension057/Cryptocurrency-extensions. (Visited in July 2022).
[41] Extension Deltas. Visited in July 2022. https://github.com/wspr-ncsu/extensiondeltas. (Visited in July 2022).
[42] Fake Ledger Chrome Extension Crypto Scam May Have Stolen Up to $2.5M. 2020. https://www.financemagnates.com/cryptocurrency/news/fake-ledger-chrome-extension-crypto-scam-may-have-stolen-up-to-2-5m. (2020).
[43] Adrienne Porter Felt, Kate Greenwood, and David Wagner. 2011. The Effectiveness of Application Permissions. In *USENIX WebApps*. 7.
[44] George Bissias and Brian Neil Levine and A. Pinar Ozisik and Gavin Andresen and Amir Houmansadr. 2016. An Analysis of Attacks on Blockchain Consensus. *CoRR* (2016).
[45] Google is banning all cryptomining extensions from its Chrome Web Store. 2020. https://techcrunch.com/2018/04/02/google-is-banning-all-cryptomining-extensions-from-its-chrome-web-store. (2020).
[46] Google Removes 49 Phishing Extensions That Steal Cryptocurrency Data. 2020. https://cointelegraph.com/news/google-removes-49-phishing-extensions-that-steal-cryptocurrency-data. (2020).
[47] Guge App. Visited in July 2022. https://www.gugeapps.net. (Visited in July 2022).
[48] Guha, Arjun and Fredrikson, Matthew and Livshits, Benjamin and Swamy, Nikhil. 2011. Verified Security for Browser Extensions. In *IEEE S&P*. 115–130.
[49] Haoyong. Visited in July 2022. https://www.chrome666.com. (Visited in July 2022).
[50] Harry. Visited in July 2022. https://medium.com/mycrypto/discovering-fake-browser-extensions-that-target-users-of-ledger-trezor-mew-metamask-and-more-e281a2b80ff9. (Visited in July 2022).
[51] Huobi Market. Visited in July 2022. https://chrome.google.com/webstore/detail/lgeilhhjnhcjlmlohhlpedhgddddgebh. (Visited in July 2022).
[52] Alexandros Kapravelos, Chris Grier, Neha Chachra, Christopher Kruegel, Giovanni Vigna, and Vern Paxson. 2014. Hulk: Eliciting Malicious Behavior in Browser Extensions. In *USENIX Security 14*. 641–654.
[53] keraf. Visited in July 2022. :https://github.com/keraf/NoCoin/blob/master/src/blacklist.txt. (Visited in July 2022).
[54] KuCoin:Bitcoin,Dogecoin Price Market. Visited in July 2022. https://chrome.google.com/webstore/detail/kucoinbitcoindogecoin-pri/nalaeminfbmmidadoaegigajbapfajgi. (Visited in July 2022).
[55] LastPass. 2008. https://www.lastpass.com. (2008).
[56] Seunghyeon Lee, Changhoon Yoon, Heedo Kang, Yeonkeun Kim, Yongdae Kim, Dongsu Han, Sooel Son, and Seungwon Shin. 2019. Cybercriminal minds: an investigative study of cryptocurrency abuses in the dark web. In *NDSS*. 1–15.
[57] Yuxi Ling, Kailong Wang, Guangdong Bai, Haoyu Wang, and Jin Song Dong. 2022. Are They Toeing the Line? Diagnosing Privacy Compliance Violations among Browser Extensions. In *ASE*.
[58] Malware and unwanted software. Visited in July 2022. https://developers.google.com/search/docs/advanced/security/malware. (Visited in July 2022).
[59] Massimo Bartoletti and Barbara Pes and Sergio Serusi. 2018. Data mining for detecting Bitcoin Ponzi schemes. *CVCBT* (2018).
[60] Metamask. Visited in July 2022. https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn. (Visited in July 2022).
[61] minerBlock. Visited in July 2022. https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl. (Visited in July 2022).
[62] mitmproxy. Visited in July 2022. https://mitmproxy.org. (Visited in July 2022).
[63] MonkeyLearn. Visited in July 2022. https://monkeylearn.com/sentiment-analysis. (Visited in July 2022).
[64] Nami Wallet. Visited in July 2022. https://chrome.google.com/webstore/detail/nami-wallet/lpfcbjknijpeeillifnkikgncikgfhdo. (Visited in July 2022).
[65] Nav Jagpal and Eric Dingle and Jean-Philippe Gravel and Panayiotis Mavrommatis and Niels Provos and Moheeb Abu Rajab and Kurt Thomas. 2015. Trends and Lessons from Three Years Fighting Malicious Extensions. In *USENIX Security*. 579–593.

[66] Neil Gandal and JT Hamrick and Tyler Moore and Tali Oberman. 2018. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics* 95 (2018), 86–96.
[67] Kaan Onarlioglu, Mustafa Battal, William Robertson, and Engin Kirda. 2013. Securing Legacy Firefox Extensions with SENTINEL *(DIMVA)*. 122–138.
[68] One-vs-the-rest (OvR) Multiclass Strategy. Visited in July 2022. https://scikit-learn.org/stable/modules/generated/sklearn.multiclass.OneVsRestClassifier.html. (Visited in July 2022).
[69] Nikolaos Pantelaios, Nick Nikiforakis, and Alexandros Kapravelos. 2020. You've Changed: Detecting Malicious Browser Extensions through Their Update Deltas. In *CCS*. 477–491.
[70] Ross Phillips and Heidi Wilder. 2020. Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites. *CoRR* (2020).
[71] Shahriar, Hossain and Weldemariam, Komminist and Zulkernine, Mohammad and Lutellier, Thibaud. 2014. Effective Detection of Vulnerable and Malicious Browser Extensions. *Comput. Secur.* 47 (2014), 66–84.
[72] Share of respondents who indicated they either owned or used cryptocurrencies in 55 countries worldwide in 2020. Visited in July 2022. https://www.statista.com/statistics/1202468/global-cryptocurrency-ownership. (Visited in July 2022).
[73] Dolière Francis Somé. 2019. EmPoWeb: Empowering Web Applications with Browser Extensions. In *IEEE S&P*. 227–245.
[74] Stargazer Wallet. Visited in July 2022. https://chrome.google.com/webstore/detail/stargazer-wallet/pgiaagfkgcbnmiiolekcfmljdagdhlcm. (Visited in July 2022).
[75] Stefan Heule and Devon Rifkin and Alejandro Russo and Deian Stefan. 2015. The Most Dangerous Code in the Browser. In *HotOS XV*. USENIX Association.
[76] Magdalena Szumilas. 2010. Explaining odds ratios. *Journal of the Canadian academy of child and adolescent psychiatry* 19, 3 (2010), 227.
[77] Tab Wrangler. 2010. https://github.com/tabwrangler/tabwrangler. (2010).
[78] Ted Knutson. 2022. Crypto Increasingly Used In Human/Drug Trafficking Says GAO. https://www.forbes.com/sites/tedknutson/2022/01/10/crypto-increasingly-used-in-humandrug-trafficking-says-gao/?sh=7043c1c4637e. (2022).
[79] Ege Tekiner, Abbas Acar, A. Selcuk Uluagac, Engin Kirda, and Ali Aydin Selcuk. 2021. SoK: Cryptojacking Malware. In *2021 IEEE EuroS&P)*. 120–139.
[80] Mike Ter Louw, Jin Soon Lim, and V. N. Venkatakrishnan. 2007. Extensible Web Browser Security *(DIMVA)*. 1–19.
[81] The Selenium Project. Visited in July 2022. https://www.selenium.dev. (Visited in July 2022).
[82] Kurt Thomas, Elie Bursztein, Chris Grier, Grant Ho, Nav Jagpal, Alexandros Kapravelos, Damon Mccoy, Antonio Nappa, Vern Paxson, Paul Pearce, Niels Provos, and Moheeb Abu Rajab. 2015. Ad Injection at Scale: Assessing Deceptive Advertisement Modifications. In *IEEE S&P*. 151–167.
[83] Victor, Friedhelm and Weintraud, Andrea Marie. 2021. Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges. In *WWW*. 23–32.
[84] VirusTotal. Visited in July 2022. https://www.virustotal.com/gui/home. (Visited in July 2022).
[85] WalletExplorer. Visited in July 2022. https://www.walletexplorer.com. (Visited in July 2022).
[86] WalletExplorer. Visited in July 2022. https://oxt.me. (Visited in July 2022).
[87] Yao Wang, Wandong Cai, Pin Lyu, and Wei Shao. 2018. A combined static and dynamic analysis approach to detect malicious browser extensions. *Security and Communication Networks* (2018).
[88] Wu, Jiajing and Yuan, Qi and Lin, Dan and You, Wei and Chen, Weili and Chen, Chuan and Zheng, Zibin. 2020. Who Are the Phishers? Phishing Scam Detection on Ethereum via Network Embedding. *IEEE SMC* (2020), 1–11.
[89] xd4rker. Visited in July 2022. https://github.com/xd4rker/MinerBlock/blob/master/assets/filters.txt. (Visited in July 2022).
[90] Pengcheng Xia, Haoyu Wang, Bingyu Gao, Weihang Su, Zhou Yu, Xiapu Luo, Chao Zhang, Xusheng Xiao, and Guoai Xu. 2021. Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange. *Proc. ACM Meas. Anal. Comput. Syst.* 5, 3 (2021), 26.
[91] Pengcheng Xia, Haoyu Wang, Xiapu Luo, Lei Wu, Yajin Zhou, Guangdong Bai, Guoai Xu, Gang Huang, and Xuanzhe Liu. 2020. Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams. In *Symposium on Electronic Crime Research*. 1–14.
[92] Pengcheng Xia, Haoyu Wang, Bowen Zhang, Ru Ji, Bingyu Gao, Lei Wu, Xiapu Luo, and Guoai Xu. 2020. Characterizing cryptocurrency exchange scams. *Computers & Security* 98 (2020), 101993.
[93] Xinyu Xing, Wei Meng, Byoungyoung Lee, Udi Weinsberg, Anmol Sheth, Roberto Perdisci, and Wenke Lee. 2015. Understanding Malvertising Through Ad-Injecting Browser Extensions. In *WWW*. 1286–1295.

A SUPPLEMENTARY DOCUMENTS

A.1 Full List of Global and Regional Browsers Covered In Our Data Collection

In this work, we target the top 10 most downloaded browsers (those with Global in their regions) and the 18 popular regional browsers (those with country codes in their regions), which are listed as *covered* in Table 8.

Table 8. Global and Regional Browsers Covered by our Data Collection

Name	Region	Global Market Share	Extension Store	Covered?	Name	Region	Global Market Share	Extension Store	Covered?
Chrome	Global	69.52%	Chrome Web Store	✓	Silk	US	<0.1%	Chrome Web Store	✓
Edge	Global	9.71%	Microsoft Edge Add-ons	✓	360 Explorer	CN	<0.1%	https://ext.se.360.cn/webstore	✓
Firefox	Global	7.14%	Add-ons for Firefox	✓	Cheetah	CN	<0.1%	http://store.liebao.cn	✗
IE	Global	4.93%	IE Add-ons	✗	Maxthon	CN	<0.1%	https://webstore.maxthon.cn	✗
Safari	Global	3.52%	Apple App Store	✗	TheWorld	CN	<0.1%	Chrome Web Store	✓
QQ Browser	Global	1.43%	https://appcenter.browser.qq.com	✓	CoolNovo	CN	<0.1%	Chrome Web Store	✓
Sogo	Global	1.35%	http://ie.sogou.com/app	✓	Cent	CN	<0.1%	Chrome Web Store	✓
Opera	Global	0.90%	Opera add-ons	✓	2345	CN	<0.1%	https://extensionie.2345.com	✗
Yandex	Global	0.84%	Chrome Web Store	✓	Whale	KR	<0.1%	https://store.whale.naver.com	✓
UC Browser	Global	0.29%	UC Web Store	✗	Swing	KR	<0.1%	Chrome Web Store	✓
Netscape	US	<0.1%	Chrome Web Store	✓	Coc Coc	VT	<0.1%	Chrome Web Store	✓
Vivaldi	US	<0.1%	Chrome Web Store	✓	JioPages	IN	<0.1%	Chrome Web Store	✓
Brave	US	<0.1%	Chrome Web Store	✓	Epic	IN	<0.1%	https://epicbrowser.com/webstore2	✗
Pale Moon	US	<0.1%	https://addons.palemoon.org	✗	Sleipnir Browser	JP	<0.1%	Chrome Web Store	✓

A.2 Time Distribution of Malicious Extensions by Category in RQ1

Following the overall time distribution of malicious extensions presented in Figure 2(b), we further break down the distribution information according to the malicious categories, as shown in Figure 7. Note that we only present the time distribution for extensions found in official stores, as the release date is unavailable in third-party stores (i.e., 14 out of 186 malicious extensions are found in Guge and Crx4chrome). This leads to the less accurate time distribution especially for mining extensions, as a large proportion of them come from the third-party stores.

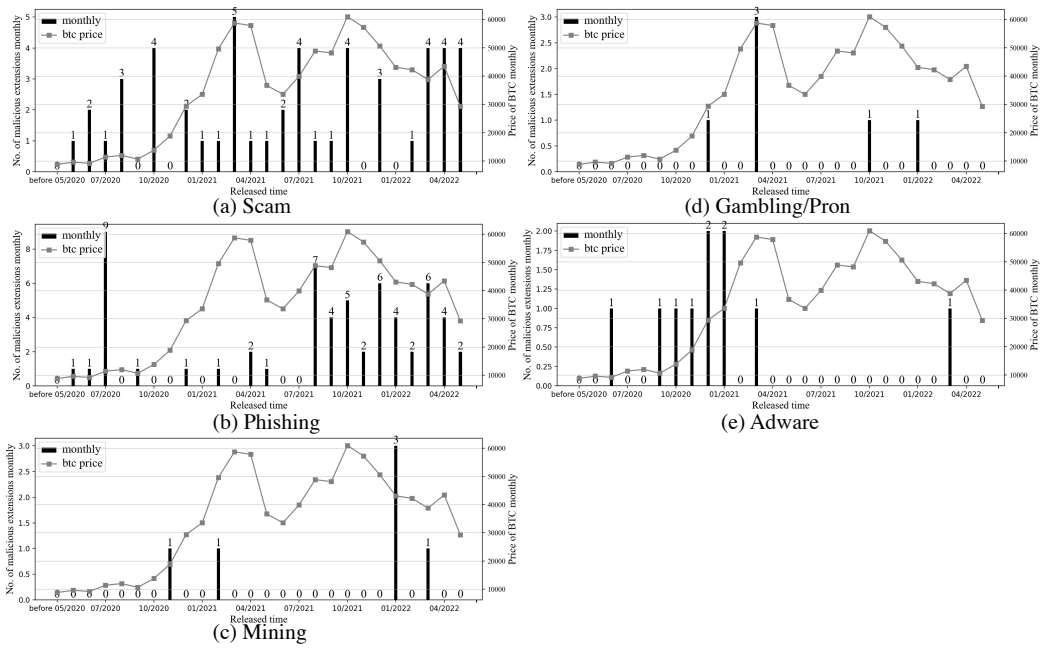


Fig. 7. Time Distribution of Malicious Extensions in 5 Types

Table 9. Top 10 Abused Third-party Domains/Libraries

#	Third-party Domains	No. Ext	#	Third-party Domains	No. Ext	#	Third-party Domains	No. Ext
1	fonts.googleapis.com	35	5	unpkg.com	9	9	www.bitcoinrewards.com	4
2	www.w3.org	20	6	twitter.com	9	10	www.portal.network	4
3	cdnjs.cloudflare.com	17	7	maxcdn.bootstrapcdn.com	9			
4	github.com	16	8	connect.trezor.io	9			

A.3 Top 10 Abused Third-Party Domains and Libraries in RQ1

To analyze the third-party services abused by the malicious extensions, we first extract the domain names from 186 extensions. From them, we have identified 95 different third-party services. We further investigate them by manually visiting them and also looking them up in search engines. The top 10 abused third-party domains and libraries are listed in Table 9.

A.4 Relationship Graph of Developers and Their Linked Extensions in RQ1

Based on our developer linking criteria including similar file structure and contents, and same malicious registration information/domain/wallet addresses, we manage to link 56 out of 186 malicious extensions to 17 developers, each of the developers account for at least two extensions.

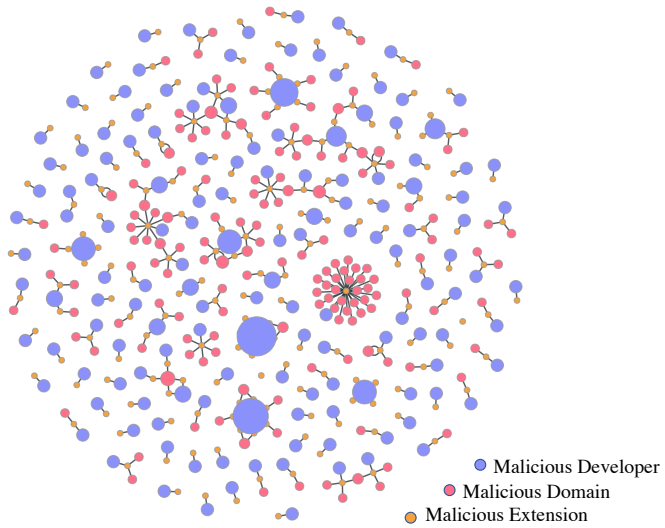


Fig. 8. Relationship Graph for Developers and Malicious Extensions

A.5 Full Lists of Identified Malicious Extensions in RQ2

Phishing Extensions. Phishing extensions construct visually identical user interfaces as the official extensions or web pages to trick victims into entering their sensitive information unwittingly, including authentication credentials at cryptocurrency exchanges, private keys and seed phrases of cryptocurrency wallets. Out of the 186 malicious extensions, we have identified 65 phishing extensions. Their full list is as shown in Table 10.

Table 10. The Complete List of Identified Phishing Extensions

Extension Name	Platform	Impersonated		Target Crypto	Stealing
		Exchange	Wallet		
atomic-wallet-io	Firefox	-	Atomic	ANY[3]	Password[1]
oigbaldgchoafpjakdmmjednlaflfmgn	Chrome	-	NCP Wallet	RBD, NCP	Wallet account[2]
atomic-wallet-exchange	Firefox	-	Atomic	ANY	Password

onfhpipacphcihanjjnkhcpkfnkaofje	Chrome	-	Wickret Wallet	BTC, ETH, BNB	Wallet account
ledger-nano	Firefox	-	Ledger Nano	ANY	Password
jmdgapllicgldgelcpedkfmdgeeoimbm	Firefox	-	ANY	ETH	Wallet account
live-ledger-nano	Firefox	-	Ledger Nano	ANY	Password
dubaicoin-dbix-price-ticker	Firefox	Livecoin	-	DBIX	Wallet account
nano-ledger-wallet-live	Firefox	-	Ledger Nano	ANY	Password
metaio-wallet	Firefox	-	MetaMask	ANY	Wallet account
Coinbase Wallet	Firefox	-	Coinbase Wallet	ANY	Wallet account
etherflyer-exchange	Firefox	EtherFlyer	-	ANY	Wallet account
trust-wallet-s	Firefox	-	Trust Wallet	ANY	Wallet account
scoinbase-wallet-crypto-wallet	Firefox	-	Coinbase Wallet	ANY	Wallet account
etherflyer-exchange	Firefox	EtherFlyer	-	ANY	Wallet account
safemoon-wallet-swap-dex	Firefox	-	Safepal	ANY	Wallet account
atomic_wallet	Firefox	-	Atomic	ANY	Password
safepal-crypto-wallet	Firefox	-	Safepal	ANY	Wallet account
exodus-wallet	Firefox	-	Exodus	ANY	Wallet account
safepal-wallet-crypto-wallet	Firefox	-	Safepal	ANY	Wallet account
adfnjoodbdcoikkhallnfejjokefkkbd	Chrome	-	VSYS Wallet	VSYS	Wallet account
safepal-wallet	Firefox	-	Safepal	ANY	Wallet account
aehoaajegaoakamklmcbgefibhnilbip	Chrome	-	VES Wallet	ETH	Wallet account
hive-keychain	Firefox	-	Hive Wallet	ANY	Wallet account
aihogeigcnkcklfaljfimkefkmbmlomi	Chrome	-	Brain Wallet	BTC	Wallet account
steemkeychain	Firefox	-	Steam Keychain	ANY	Wallet account
metamask-buy-send	Firefox	-	MetaMask	ANY	Wallet account
exodus-bitcoin-ethereum-wallet	Firefox	-	Exodus	ANY	Wallet account
metamask-wallet-buyswap-crypto	Firefox	-	MetaMask	ANY	Wallet account
exodus-cryptoss-bitcoin-wallet	Firefox	-	Exodus	ANY	Wallet account
coinbase-wallet-app	Firefox	-	Coinbase Wallet	ANY	Wallet account
exodus-wallet-device	Firefox	-	Exodus	ANY	Wallet account
trust-crypto-bitcoin-wallet	Firefox	-	Trust Wallet	ANY	Wallet account
trust-crypto-btc-wallet	Firefox	-	Trust Wallet	ANY	Wallet account
partisia-wallet	Firefox	-	Partisia w]Wallet	ANY	Wallet account
cgkifhiihlpcglfifjiklemcppbejdpf	Chrome	-	MetaMask	ETH	Wallet account
exodus-crypto-wallet-btc	Firefox	-	Exodus	ANY	Wallet account
binance-chain	Firefox	Binance	-	ANY	Wallet account
gcfbekmogelpbhgcepghlkdbmhpbaaig	Chrome	-	Goat Wallet	ANY	Gathering user info
kmkmhgjamoppdmaafcmfmojhhbcklfdd	Chrome	-	Goat Wallet	DGB	Wallet account
bitcoin-balance-viewer	Firefox	-	-	BTC	Gathering wallet address
e-xo-du-s-crypto-btc-wallet	Firefox	-	Exodus	ANY	Wallet account
e-xo-du-s-crypto-btc	Firefox	-	Exodus	ANY	Wallet account
e-xo-dus-crypto-wallet	Firefox	-	Exodus	ANY	Wallet account
exodus-bitcoin-crypto-wallet	Firefox	-	Exodus	ANY	Wallet account
exodus-btc-crypto	Firefox	-	Exodus	ANY	Wallet account
exodus-nfts-wallet-1-2	Firefox	-	Exodus	ANY	Wallet account
exodus-wallet-extension	Firefox	-	Exodus	ANY	Wallet account
exodusrwinawallet	Firefox	-	Exodus	ANY	Wallet account
trust-wallet-coin	Firefox	-	Trust Wallet	ANY	Wallet account
trust-wallet-nft	Firefox	-	Trust Wallet	ANY	Wallet account
trust-wallet-qr-code	Firefox	-	Trust Wallet	ANY	Wallet account
apcmoigdfhnpdefifchnjapedkaceiob	Chrome	-	ChainLink	ANY	Wallet account
cdgadjhfmbokfflmgjpiieifghkmpipc	Chrome	-	Terra Wallet	LUNA	Wallet account
dnnfplhmimbdhkomfncfdeijimdmlgfj	Chrome	-	Solana	ANY	Wallet account
ffpbldifhhejjmjpcibcecggemkobkcf	Chrome	-	Polkadot	DOT	Wallet account
gbncpgegfhmhfaicgojejjgehgclhlcn	Chrome	-	Exodus	ANY	Wallet account
hhgnnfacfifahmdaomokgjklcjjciknc	Chrome	-	MetaMask	ANY	Wallet account
kmfbhobieckelghhfhdndbfookcdhfje	Chrome	-	Cardano	ANY	Wallet account
leekelfhedhhbehcgoidhenildifedae	Chrome	-	Ravine	ANY	Wallet account
pnfppegmgdomhndfgocelcpjajmfhijm	Chrome	-	Avax	ANY	Wallet account
djlnfokielnkgcaalhjflappbcjlaobj	Chrome	-	Trust Wallet	ANY	Wallet account
mdfmdejjpacdlljplloanggaickcpccf	Chrome	-	MetaMask	ANY	Wallet account
kabhkmhfcgdekaaeabdlmknlnmklienl	Chrome	-	Exodus	BTC	Wallet account
pmpjkkicnikmldkombdlfgmdnnodgpkc	Chrome	-	Exodus	BTC	Wallet account

[1] Password: The extension forges a login window to steal the input password. An example is shown in Figure 4.(b)
[2] Wallet account: The extension forges a keychain loading window to trick the victims into loading their existing wallets. An example is shown in Figure 4(a). The password, backup phrase and private key would be leaked to the attacker.

[3] ANY: The impersonated wallet or exchange supports more than three cryptocurrencies, so we omit details here.

Mining Extensions. The mining extensions mine cryptocurrencies with victim's computation power, through fetching tasks from mining pools and in-browser mining in the background. Out of the 186 malicious extensions, we have identified 22 mining extensions. Their full list is as shown in Table 11.

Table 11. The Complete List of Identified Mining Extensions

Extension Name	Platform	Mining Targets		Mining Behavior
		Crypto	Pool	
Litecoin Miner	Crx4Chrome	BTC	Coinhive	Mining plundering
Ethereum Miner	Crx4Chrome	BTC	Coinhive	Mining plundering
bitcoin-monero-miner	Opera	BTC, XMR	Mineralt	Mining unlocking
KMine	Crx4Chrome	XMR	Coinhive	Mining unlocking
Monero Browser Crypto Miner	Crx4Chrome	XMR	MoneroOcean	Mining unlocking
Monero Mining	Crx4Chrome	XMR	Coinlmp	Mining unlocking
DFP Cryptocurrency Miner	Chrome	XMR	CryptoLoot	Mining unlocking
weMiner	Crx4Chrome	XMR	CryptoLoot	Mining unlocking
JustMineIt	Crx4Chrome	XMR	XMR Miners Club	Mining plundering
Pickaxe: Coinhive Monero Miner	Crx4Chrome	XMR	Coinhive	Mining unlocking
ccagdbjcbhmcdcbbknfebhhdbolnfimo	Chrome	-	-	Invalid mining blocking
notmining-org	Firefox	-	-	Invalid mining blocking
egnfmleidkolminhjlkaomjefheafbbb	Chrome	DFP	CryptoLoot	Mining unlocking
eigblbgjknlfbajkfhopmcojidlgcehm	Chrome	XMR	Coinhive	Mining unlocking
lekkmokmojahmfgdkfeldeoijmmeodod	Chrome	-	-	Invalid mining blocking
minecontrol	Guge	-	-	Invalid mining blocking
earnsurfing	Guge	XMR	CoinImp	Mining unlocking
emikbbbebcdfohonlaifafnoanocnebl	Chrome	-	-	Invalid mining blocking
iefilmjnfffjnbdmofcgkfnnkbldckmo	Chrome	BTC	CCGMining	Mining unlocking
aimhjeaphadcaibpmidbcjgpokpkhfpa	Chrome	XMR	Coinhive	Mining unlocking
bnbmlmjhaohpobnjfifeghjmamjfolnb	Chrome	BTC	RPC	Mining unlocking
mnlfoooikhmcaomegmfopecjngldnmmn	Chrome	ETH	Ethermine	Mining unlocking

Scam Extensions. The scam extensions commonly trick victims into the "honeypot" traps with fake attractions or deals. This category of extensions are the most prevalent among all malicious extensions, accounting for 75 of the 186 identified malicious extensions. Their full list is as shown in Table 12.

Table 12. The Complete List of Identified Scam Extensions

Extension Name	Platform	Scam Crypto	Scam Location	Scam Sub-Category
1-click Amazon Bitcoin checkout	Chrome	BTC	Redirect to website	Shopping proxy
aejmoogjdllanidlpfjmmmmimfaficio	Chrome	ANY	In extension	Account manager
afommmnmohdebmgabmbglefkbholcobb	Chrome	ANY	Redirect to website	Investment
afpfjkgccddomghmkalpoefodphfpefm	Chrome	BTC	In extension	False information
aopdfjgkaphbpmhemeadmlcbfeddfeme	Chrome	ANY	Redirect to website	Integrated service portal
BurnerX	Chrome	DAI, ETH	In extension	Address manipulation
cggcgkjaddjjcgjlpkmneklfamidgdma	Chrome	ANY	Redirect to website	Shopping proxy
cgmhechlnfbnfcnomkmcillkgnipocfh	Chrome	TRUE	In extension	Account manager
cjehbpdobheocpjadjpmomolgogaeajn	Chrome	ANY	Redirect to website	Giveaway
coin2-shop-extension	Firefox	ANY	Redirect to website	Shopping proxy
coincorner	Chrome	BTC	Redirect to website	Giveaway
coinjay_caofapkfjgdhaphoohhgnajilfgcccnf	Chrome	BTC	Redirect to website	Shopping proxy
coinstats-crypto-tracker	Firefox	ANY	In extension	False information
CryptoRewards	Guge	BTC	Redirect to website	Giveaway
CryptoRewards	Chrome	BTC	Redirect to website	Giveaway
epfkdlghgcjdonodehdakmmidlklindn	Chrome	ANY	Redirected to website	Integrated service portal
epfkdlghgcjdonodehdakmmidlklindn	Chrome	BTC	Redirect to website	Giveaway
ETH Ticker | Ethereum Ticker | Token Ticker	Chrome	ETH	In extension	False information
fbi-free-bitcoin	Firefox	BTC	Redirect to website	Giveaway
fpabdmjmldajnkijknogckkhlmbnfiog	Chrome	ANY	In extension	Account manager
free_bitcoin	Guge	BTC	Redirect to website	Investment
free_bitcoin	Chrome	BTC	Redirect to website	Investment
goldmint-lite-wallet	Firefox	MNT, GOLD	In extension	Account manager
halmgkimboipdmlbhmfpaagfkpjecklm	Chrome	ANY	In extension	Account manager
idkijaagnjnpbicdifhpkogkkcdffhge	Chrome	BTC	Redirect to website	Giveaway
idoockghidhkajjcomifcbcneopnbkph,Bitlo.com	Chrome	ANY	In extension	False information
jjdbklmemcpdklojpniabhfhclngpppe	Chrome	BTC	In extension	Address manipulation
justLiquidityWallet	Firefox	ETH	Redirect to website	Giveaway

llcndhdbiiocjfhggkagdbinbpoebbmh	Chrome	BTC	Redirect to website	Shopping proxy
LTC Ticker | Litecoin Ticker	Chrome	LTC	In extension	False information
Maskbook	Firefox	ANY	In extension	Account manager
microbitcoin-wallet-extension	Firefox	BTC	In extension	Account manager
Moon: Shoop online with Bitcoin	Guge	BTC	Redirect to website	Shopping proxy
Moon: Shoop online with Bitcoin	Chrome	BTC	Redirect to website	Shopping proxy
Oxygen-Atomic Crypto Wallet	Chrome	ANY	In extension	Account manager
ocfgfhicacgipgpiapepehhpidbhijkl	Chrome	ETH, TOMO	Redirect to website	Investment
Purse: Shop with Bitcoin	Guge	BTC	Redirect to website	Shopping proxy
Purse: Shop with Bitcoin	Chrome	BTC	Redirect to website	Shopping proxy
sugarchain-wallet-extension	Firefox	SUGAR	In extension	Account manager
TezBox	Firefox	ANY	In extension	Account manager
thanos-wallet	Firefox	ANY	In extension	Account manager
twetch-wallet	Firefox	BSV	In extension	Account manager
oheacmjjkbcbpgmdljkbcaopcmpjfloj	Chrome	BTC	In extension	Account manager
ndclmokbpeggeoahfjjkjfifhpjnbkho	Chrome	BTC	In extension	Address manipulation
iejeonlbmfggijedgafmelbabpacldac	Chrome	BTC	In extension	Account manager
jaooiolkmfcmloonphpiiogkfckgciom	Chrome	BSV	In extension	Account manager
bitcoinrewards	Firefox	BTC	Redirect to website	Cashback
stormX	Chrome	BTC	In extension	Cashback
jmclmpncoehnbcpfjkdddopnpdockkih	Chrome	GCR	In extension	Account manager
mmeojdpadjnmjnlfjmbbeocnoknafmpn	Chrome	BTC	Redirect to website	Cashback
iaafbpabegfpdebjplhgcglanbgennmm	Chrome	ANY	Redirected to website	Integrated service portal
top-10-bitcoin-faucets	Firefox	ANY	Redirected to website	Integrated service portal
hdpjhoafkepknmfjjkhajghegemjcanl	Chrome	BTC	Redirected to website	Integrated service portal
givingassistant-button	Firefox	ANY	Redirected to website	Integrated service portal
dommpfbbddejhlmnoeilamlncnedcjfi	Chrome	CELO	In extension	Account manager
ihifemcnankeeeaicfaeifhmmaefhapp	Chrome	ETH	In extension	Account manager
jkefllnpggoehndkogpdjndhfidgnchk	Chrome	ETH	Redirect to website	Investment
bitpay-decoder-anti-bitpay-com	Firefox	ANY	In extension	Integrated service portal
crypto-airdrop-tools	Firefox	BTC	In extension	Integrated service portal
dgfhnpfofgalhnmamhlgbphnegkcgcic	Chrome	ANY	In extension	Integrated service portal
walletpeak-rs	Firefox	ANY	In extension	False information
stekking-earn-bitcoin-rewards	Firefox	BTC	Redirect to website	Cashback
lolli-earn-bitcoin	Firefox	BTC	Redirect to website	Cashback
rewardsbunny	Firefox	ANY	Redirect to website	Cashback
satsback-earn-bitcoin-rewards	Firefox	BTC	Redirect to website	Cashback
bamhkeeolhfjabljjoajbfcebhjbkoaa	Chrome	BTC	Redirect to website	Cashback
bdhomkmlcfplpamlpnimlmmgmnbmhamo	Chrome	BTC	Redirect to website	Cashback
aafjjocpcjgbdkcfblcaejddeemlfjej	Chrome	BTC	Redirect to website	Cashback
agkfnefiabmfpanochlcakggnkdfmmjd	Chrome	ICP	In extension	Account manager
iompmkajdofndagijpjmknmnmhkapbhj	Chrome	ETH	In extension	Account manager
lpklidjhgjhpoakmhpgjpgdckhgiggki	Chrome	SOLANA	In extension	Account manager
pjpaehngacdnemhiokleffbaohinhioi	Chrome	BTC	Redirect to website	Investment
cokgnjencngigmhgphpkmmbcmebekkdp	Chrome	ANY	Redirect to website	Giveaway
ojnkijohnecihlkfbmplngdfldkcgelh	Chrome	BTC, ETH, LTC	Redirect to website	Investment
iifeegfcfhlhhnilhfoeihllenamcfgc	Chrome	ADA	In extension	Account manager

Adware Extensions. This category of extensions intend to inject unwanted advertisement without the consent of the user, alongside the cryptocurrency-related services provided by them. Out of the 186 malicious extensions, we have identified 16 adware extensions. Their full list is as shown in Table 13.

Gambling/Porn Extensions. Most (5/8) of the gambling/pornography extensions pretend to be benign cryptocurrency exchanges with fake interfaces. Two exceptions in this category directly market themselves as online casinos. Out of the 186 malicious extensions, we have identified 8 gambling/pornography extensions. Their full list is as shown in Table 14.

A.6 The Identified Malicious Seed Addresses in RQ3

In total, we have identified 10 malicious BTC seed addresses with 38 colluding addresses, and 12 ETH seed addresses with 29 colluding addresses, as listed in Table 15. Out of the 22 seed addresses, most (15) belong to *Scam* extensions, a few (5) belong to *Phishing*. The only 2 exceptions

Table 13. The Complete List of Identified Adware Extensions

Extension Name	Platform	Disguised Service	Target Advertisement	Ad Presenting Method
eachlnokbkckmbhglohpcmhllebcdbme	Chrome	Price tracker	Shopping sites	Redirect to website
edlhfnhkegagbfhppecphocjmloaodbm	Chrome	Blockchain usage forum	Others	Pop-up windows
emnbgnmkmndoebdjfmammpamenknhfmj	Chrome	Price tracker	Shopping sites	Redirect to website
folodlanokmgajkjngaablakgdonghlm	Chrome	Crypto news	Games	Pop-up windows
aeefckiopejmogjdfmhlbmbdlifkjpho	Chrome	Price tracker	Others	Pop-up windows
jmilgfebahjgmcnhiiemhbebehfmljld	Chrome	Crypto news	Shopping sites	Redirect to website
kkagambidfkjokpcplknnffejlppkijb	Chrome	Crypto news	Job market	Redirect to website
acfodajggdfhmkgalgjijpbnpgnhpdeo	Chrome	Price tracker	Others	Pop-up windows
hdmfmeoikfkhkbilebheebjejomkkjjk	Chrome	Price tracker	Games	Redirect to website
hppfhaphpjlonbhdnhhhlicceeadefah	Chrome	Coin reward provider	Games	Redirect to website
lbdhflfllhpalbgpihfaihgboehmegap	Chrome	Crypto news	Shopping sites, games	Pop-up windows
gametop-free-games	Firefox	Coin reward provider	Games	Redirect to website
dlgphafbolodmjgcibcijhioabpplnim	Chrome	Coin reward provider	Games	Redirect to website
bb-auction-assistant	Firefox	Crypto news	Shopping sites	Redirect to website
Cashweb BB	Firefox	Crypto news	Shopping sites	Redirect to website
idepgkijkcpdjfjodklngiepdgncaoek	Chrome	Crypto news	Shopping sites	Pop-up windows

Table 14. The Complete List of Identified gambling/Porn Extensions

Extension Name	Platform	Disguised Service	Actual Content
cpdoomofobgidgcfaeiffcnakimkgclp	Chrome	Online casino	Online casino
ndhhpfjiakijfojhdhjhjoboelhngjhc	Chrome	Crypto exchange	Porn
kbkfhfkoiflhigkmgalpojgkdfeamiod	Chrome	Crypto exchange	Porn
dgfmkfjdpeeamlboiccabbeekienlcmo	Chrome	Crypto exchange	Porn
hddhfbmnobjkpefjbkdihnjpejfkcfop	Chrome	Online casino	Online casino
bitdice	Firefox	Crypto exchange	Online casino
1inch-exchange	Firefox	Crypto exchange	Porn
jopilafbmdbhmplganabmfbmjfgbgbab	Chrome	Online casino	Online casino

Table 15. Seed Wallet Addresses Extracted from Malicious Extensions

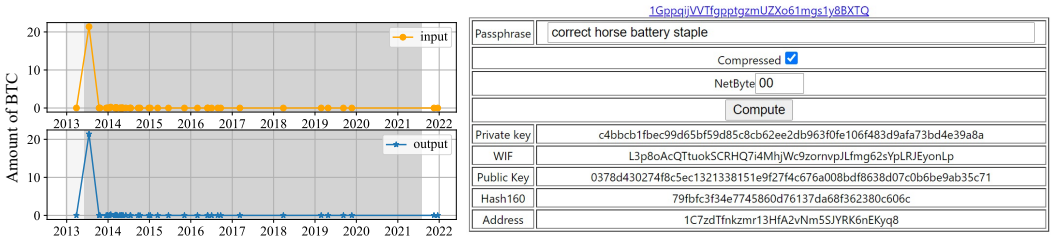
Seed Address (BTC)	Type	Amt(BTC)	ITN#	VAN#	CAN#	Seed Address (ETH)	Type	Amt(ETH)	ITN#	VAN#	CAN#
1C7zdTfnkzmr13HfA2vNm5SJYRK6nEKyq8	Scam	21.89	131	124	1	0xF6791CB4A2037Ddb58221b84678a6ba992cda11d	Scam	19.95	2	2	9
3BMEX91ZhhKoWtsH9QRb5dNXnmnGpiEetA	Phishing	3.99	220	220	0	0x76A004b8b94df5120708158c47295C8b63D72a96	Phishing	2.17	7	6	2
1E1QFEYncL9gXLoiNZyGLGq23orYW1UvcD	Scam	3.24	33	29	1	0x434863a764770985e0b71425e7d108cc6b3beb65	Phishing	1.49	26	16	7
36456e4vXkJsqNJoAYGT3jaziGRCboe4ca	Scam	2.73	191	191	0	0x3057b2648d905912ef511674aa3ffe9fcf5140db	Mining	0.89	20	20	4
1DwGvcw7e9oT1PdVs93bLBkERupLueBFt7	Scam	0.24	4	4	32	0x2bC471eF0E259aB41f578A540a45f8f64c598882	Scam	0.71	18	18	1
1EiK8BgSbMsSuBKafee8DwSQwshVhnBYgP	Scam	0.17	3	3	0	0xf1b26cb6cab29d171187703118cfef6c38b31bea	Scam	0.53	52	52	1
1DqG5P9nDmbHbg41622oPno6P1s1TuJJTy	Gam/Porn	0.12	24	24	0	0xf720f7fa4033B07915Ab37Bc9Eb9d3e99B78D4df	Scam	0.24	5	5	1
1C52TCmbaUmyBa1RmbVRdUuG6346uuJR9z	Scam	0.015	117	73	0	0x32585BE48b9f45D107A933F992225a8606F6967a	Phishing	0.20	1	1	0
17dEg1hFMZcemSEePP87rdfDEc1EppiD1m	Scam	0.013	101	101	4	0x8db97C7cEcE249c2b98bDC0226Cc4C2A57BF52FC	Scam	0.063	3	1	0
3CDJNfdWX8m2NwuGUV3nhXHXEeLygMXoAj	Scam	0.00048	8	8	0	0x89205A3A3b2A69De6Dbf7f01ED13B2108B2c43e7	Scam	0.021	90	90	0
						0x88a5C2d9919e46F883EB62F7b8Dd9d0CC45bc290	Phishing	0.015	13	9	4
						0x765DE816845861e75A25fCA122bb6898B8B1282a	Scam	0.010	1	1	0

ITN is the incoming transaction number, VAN is the victim address number and CAN is the colluding address number

are from *Gambling/Porn* and *Mining* extensions. According to the distinct malicious behavior of *Scam* and *Phishing* extensions as discussed in Section 5.2, such as alluring victims to transfer the cryptocurrency into illicit address and substituting users' receiving address with illicit address, these two types of malicious extension typically embed malicious addresses that can be detected by our approach. In particular, we also check the two addresses related to *Gambling/Porn* and *Mining*. The address *1DqG5P9nDmbHbg41622oPno6P1s1TuJJTy* is the payee address for selling gambling chips, and the address *0x3057b2648d905912ef511674aa3ffe9fcf5140db* is embedded inside an invalid mining blocking extension, linked by a redirection button for collecting malicious donation.

For the source of 22 seed address, most (18) exist in individual extensions, a few (4) belong to 2 extensions. Specifically, the address *17dEg1hFMZcemSEePP87rdfDEc1EppiD1m* and *0xf720f7fa4033B0791-5Ab37Bc9Eb9d3e99B78D4df* are from the same scam extension, *top-10-bitcoin-faucets*. And the address *0xF6791CB4A2037Ddb58221b84678a6ba992cda11d* and *0x2bC471eF0E259aB41f578A540a45f8f64c-598882* are from another scam extension, *ihifemcnankeeeaicfaeifhmmaefhapp*. No seed address is shared by different extensions, and no developer can be linked through the usage of the same address.

A.7 The Most Profitable Address in RQ3



(a) Incoming and Outgoing Transactions

(b) User Interface of the Address Embedding Extension

Fig. 9. Transaction History of Address *1C7zdTfnkzmr13HfA2vNm5SJYRK6nEKyq8* and its Embedding Extension.

As a case study, we further look into the wallet address *1C7zdTfnkzmr13HfA2vNm5SJYRK6nEKyq8* that incurred most loss (21.89 BTC) in our study. We check its embedding extension named *TP' Brainwallet*, whose interface is shown in Figure 9(b). This scam extension advertises to facilitate the wallet creation in an easy and hassle-free manner, while actually tricking the victims into reusing the adversary-controlled credentials and user secrets. The affected victims would end up topping up to this compromised wallet address. To avoid being tracked to its actual owner, this extension stealthily utilize cryptocurrency mixing services to anonymize the outgoing transactions. Due to the lack of typical malicious features that existing malware detection tools rely on, extensions of this type can be challenging to identify and filter out in the wild. This could explain its prolonged existence period from 2013 till 2021.

A.8 API Features of Cryptocurrency-themed Malicious Extensions

Besides the features used in this work, we notice that the invoked browser APIs are also taken as features for malicious extension detection [73]. Therefore, we study their effectiveness and relevance based on our dataset. The Odds Ratio values are listed in the last five columns in Table 7. In general, malicious extensions invoke more API calls at runtime, compared to the benign ones. Most of the API calls are in line with the categorical malicious behavior. For example, the mining extensions show high relevance to *system.cpu* API (i.e., to query CPU status during mining) and *permissions* API (i.e., to manipulate resources for mining) . The adware extensions are related to the *webRequest* and *app.runtime* to load/redirect users to the desired pages. In addition, the API calls for each category also exhibit new features. For example, the *identity* is heavily invoked in mining and adware extensions to manipulate user authentication and steal private information, besides the expected phishing extensions.

Received August 2022; revised October 2022; accepted November 2022