Understanding the Utilization of Cryptocurrency in the Metaverse and Security Implications

Ayodeji Adeniran, Mohammed Alkinoon, and David Mohaisen

University of Central Florida, Orlando. USA

Abstract. We present our results on analyzing and understanding the behavior and security of various metaverse platforms incorporating cryptocurrencies. We obtained the top metaverse coins with a capitalization of at least 25 million US dollars and the top metaverse domains for the coins, and augmented our data with name registration information (via whois), including the hosting DNS IP addresses, registrant location, registrar URL, DNS service provider, expiry date and check each metaverse website for information on fiat currency for cryptocurrency. The result from virustotal.com includes the communication files, passive DNS, referrer files, and malicious detections for each metaverse domain. Among other insights, we discovered various incidents of malicious detection associated with metaverse websites. Our analysis highlights indicators of (in)security, in the correlation sense, with the files and other attributes that are potentially responsible for the malicious activities.

Keywords: Metaverse, security, cryptocurrencies, data analysis.

1 Introduction

Metaverse is a technology of the future with much anticipation and hype about its capabilities to alter the life of humans through online model values [4]. Several companies are energetically working on building the metaverse, including technology giants like Facebook and Microsoft, among others. The metaverse is still in its development phase, and the full realization of an interconnected virtual world is yet to be a reality. The metaverse holds the potential for various applications, such as entertainment, gaming, education, virtual commerce, virtual meetings, and more, and is expected to revolutionize how we socialize, work, learn, and interact with digital contents [2].

Although the metaverse is still developing, metaverse coins already amount to trillions of USD in value, and this trend is expected to persist as the technology reaches maturity [13]. However, as with any digital platform or online community [1], the possibility of malicious activities occurring in the metaverse cannot be ignored. As the metaverse concept evolves, it is essential to address potential security concerns, including detecting malicious activities within this virtual space. While the metaverse presents new opportunities for collaboration, interaction, and entertainment, it can also attract malicious actors who seek to exploit vulnerabilities or engage in harmful activities. The intent and motivation for carrying out the malicious activity could be to steal vital information or assets that can be translated into money. Since the metaverse represents

the digital world, which involves buying and selling with either cryptocurrency or fiat currency, malicious activities cannot be uncommon.

This paper focuses on understanding malicious activities in the metaverse represented by various platforms and domains. The attackers are sophisticated and experienced with reported attacks on other online platforms, e.g., cryptocurrencies and social media platforms. One of the ways the cyber attackers operate is by sending malicious files to the intended targets to corrupt the system and enable them to access it. The cyber-attacks can be malware [12], denial-of-service (DOS) attacks [22], phishing [21], or code injections [11]. Security analysis of the metaverse domains is the central focus of this paper, and we intend to analyze the files interacting with the domains to gain insight. We will discuss the possible security challenges and malicious activities in the metaverse.

Organization. In section 2, we present the related work, including the research gap. In section 3, we introduce the problem statement, including the research questions. In section 4 we introduce our approach. In section 5, we discussed the results. We discuss various aspects of our studies in section 6 and conclude our work in section 7.

2   Related Work

Several papers explored the security of the metaverse. Di Pietro and Cresci [6] explored the security and privacy concerns surrounding the metaverse by focusing on the security risks that metaverse users may face and how it could affect their privacy. Zhao *et al.* [25] also conducted a study on security in the metaverse, discussing the common security issues and how they can impact the metaverse. Choi *et al.* [5] examined the future of the metaverse, tackled similar security issues as the previous ones, and discussed the technology and structural frameworks associated with the realization of solutions.

Kurtunluoglu *et al.* [10] explored authentication in virtual reality and the metaverse, focusing on security and privacy concerns related to authentication methods. Aks *et al.* [3] also conducted a study on metaverse security, covering metaverse infrastructure, human interactions, and other interconnected virtual worlds aspects [8].

Tariq *et al.* [20] explored the security implications of deepfakes in the metaverse, the security challenges, authentication issues, and impersonation problems. Oosthoek *et al.* [14] researched the security threats to cryptocurrencies, particularly to Bitcoin exchanges—Bitcoin is one of the major cryptocurrencies used in the metaverse. Zaghloul *et al.* [24] also examined the security and privacy issues with Bitcoin and blockchain relevant to the metaverse. Giechaskiel *et al.* [7] examined Bitcoin security challenges and their impact when there is a security breach or exposure.

Rosenberg *et al.* [15] conducted a study on marketing in the metaverse and consumer protection. Rosenberg *et al.* [16] also studied marketing in the metaverse and the associated risks. Kshetri *et al.* [9] studied the economics of the metaverse and its impact on the global economy. Other works that explored the security of cryptocurrencies in general include those in [18,17,19]

The Research Gap. Our study is significantly different from other existing related studies. Our study examines the sources of security vulnerability in the metaverse and relates the findings to market capitalization. Unlike the prior work, our study conducts a

thorough direct analysis of each metaverse token rather than focusing on general security concerns (e.g., human error, authentication issues, and other vulnerabilities). Our approach involves analyzing the top metaverse tokens, obtaining their domains and relevant information, and conducting a vulnerability scan to identify potential security issues that may lead to recommendations for this emerging application domain.

We note that our work is the first of its type in this space, as there is prior work that directly studied or measured the overlap between metaverse technologies and cryptocurrencies and how these cryptocurrencies are utilized within the metaverse.

3 Problem Statement and Research Questions

Both legal and illegal activities and transactions are expected in the metaverse. Metaverse is expected to become the digital center for gaming, entertainment, education, etc. Traffic to the metaverse will likely increase with millions of dollars in daily transactions. Security of assets, non-fungible tokens, cryptocurrency, and other technologies has become a challenge due to illegal activities associated with them in the metaverse.

To this end, this paper aims to tackle three crucial research questions related to identifying harmful behavior in the metaverse, particularly those associated with virtual tokens. Our analysis will be guided by these questions to ensure we provide accurate and self-contained answers. By scrutinizing various domains in the metaverse, we will obtain valuable insights that will aid our examination.

1. **RQ1: What are the prevalence of digital coins in the metaverse, and what are their associated threats?** We thoroughly scrutinize the correlation between the popularity and market capitalization of the metaverse and the plausible malicious threats. We analyzed the top forty metaverse coins with the highest market capitalization to accomplish this objective.
2. **RQ2: How significant are metaverse domain artifacts such as communication and referring files in determining the maliciousness of such domains?** To effectively identify malicious incursions in Metaverse domains, conducting a thorough analysis of critical artifacts is imperative. This includes communication files, referrer files, and Passive DNS artifacts, which all directly impact Metaverse domains. Therefore, a comprehensive assessment of their contribution is essential.
3. **RQ3: Is there any correlation between fiat currency to cryptocurrency and vice versa, and the maliciousness of metaverse applications?** It is imperative to recognize the imminent threat posed by cyber attackers who aim to steal money and assets, especially in the metaverse, where cryptocurrency reigns supreme. Our investigation will determine whether domains incorporating fiat currency are more susceptible to malicious activities than those solely relying on cryptocurrency.

4 Technical Approach

This study explored the level of malicious activities in the top metaverse tokens. We analyzed 44 metaverse tokens with a market capitalization of at least 25 million USD. We hypothesize that cybercriminals are likelier to target tokens with a high market

capitalization. To test this, we first divided the metaverse tokens into their respective domains and mapped them to their IP addresses. Then, we used the "whois" tool to gather information about the DNS service provider, registrar location and URL, hosting DNS IP addresses, and content delivery network (CDN). We manually inspected all the metaverse websites we studied for transactions from fiat to cryptocurrency.

We thoroughly scanned the metaverse domains and associated IP addresses using virustotal.com. During the scan, we gathered *passive DNS*, communication files, and referrer files and identified malicious detections. We then analyzed the communication and referrer files to detect any malicious activities and identified the file types to locate the source of the malicious activities. We then cross-referenced the metaverse domains with the malicious detections in the communication and referrer files to verify their presence. Additionally, we compared domains with fiat currency and cryptocurrency to domains with malicious activity. Lastly, we examined the metaverse tokens to identify patterns between the top and low tokens based on their market capitalizations.

4.1   Dataset and Preprocessing

Websites and Their Attributes. For this study, we collected data on metaverse coins, their corresponding domains, and their IP addresses. Our first step was to manually select metaverse coins with a market capitalization of at least 25 million USD and then map them to their respective domains. For the initial set of domains, we utilized https://coinmarketcap.com, a website that specializes in tracking coins, their market caps, and associated domains of application. To extract infrastructure information and address the first research question we posed in section 3, we used domain query tools to extract information such as the IP addresses and CDN providers and *manually* checked each webpage for the presence of fiat currency.

Security Data Attributes. We then scanned each metaverse domain and its associated IPs with virustotal.com. This scan provided information on Passive DNS, communication files, referrer files, and malicious detections. We further analyzed the communication files and referrer files to identify those with malicious detection and their types. The malicious detection was also categorized into different types with the number of occurrences for each type. Our primary focus was collecting data with malicious detection to explore the correlation between the different metaverse platforms, cryptocurrencies, artifacts, and associated malicious detection.

To gain a deeper understanding of file connections, especially those related to malicious activities, we thoroughly examined the interlinking between infected communication and referrer files and malware detections. Moreover, we meticulously tallied the frequency of each file type and its association with infected communication and referrer files. Our efforts to uncover malicious behavior were further amplified by our detailed analysis of every scan result and its correlation with malware detection in the scanned files and hosting metaverse platforms.

4.2   Analysis Dimensions

Our study explores the relationship between the metaverse domains and malicious activity and detection. We aim to identify the source and prevalence of such activity within

the metaverse space. To do so, we analyzed various dimensions and provided answers to research questions. In the next section, we will focus on specific dimensions to uncover answers to our research questions in section 3. Namely, the dimensions we cover with our analysis are (1) communication files and referrer files activities in the metaverse domain, (2) metaverse coins market capitalization, (3) malicious activities in Metaverse coins, and (4) metaverse coins with fiat currency to cryptocurrency.

5   Results and Findings

Our main results, which analyze and map the relationship between malicious detections in metaverse domains and other artifacts, will be presented in this section.

5.1   Communication and Referrer Files in the Metaverse Domain

The popularity of online platforms is determined by the number of visitors, transactions, and overall traffic. Facebook, for instance, boasts billions of registered users and experiences a significant amount of communication and transactions. These interactions are facilitated through manual website exploration, file exchanges, and website database access. However, it is important to exercise caution as autonomous programs such as bots can also interact with these systems. They can inject messages or code, store data in databases, and even remotely manipulate and hijack systems. Therefore, it is crucial to implement proper security measures to prevent unauthorized access and protect sensitive information. In the metaverse, communication files play a significant role. We have collected communication files from all domains and are studying their relationship with malicious activities. Our analysis aims to determine if the number of communication files is linked to malicious detections and identify the types of files responsible for such detections. This information will be crucial in developing preventive policies against malicious threats in the metaverse.

Observations. The heatmap in Fig 1 displays the frequency of malicious detections in different file types across various domains in the metaverse. The Win32 EXE file type had the highest frequency of malicious detection, with 14 domains recording it. Android came in second, with 11 domains showing a malicious presence. The axieinfinity.com domain had the highest number of malicious detections at 483. Other file types with malicious activity included PDF, Javascript, Android, and MS Excel Spreadsheet. These file types were responsible for most malicious detections in the study. Additionally, Fig 2 shows the frequency of referrer files with no detection. The figure displays a heatmap indicating the frequency of infected referrer file types in the metaverse domain. The number of occurrences for each file type is indicated.

The heatmap in Fig 3 displays a significant number of communication files with malicious detections. It was discovered that metaverse domains that had malicious detections also had communication files with malicious detections. The Win32 EXE and Android file types were more commonly found than others. The Win32 EXE file type had more detections and was present in approximately 25 out of 31 metaverse domains with malicious detections. Fig 3 provides a visualization of the total occurrences of
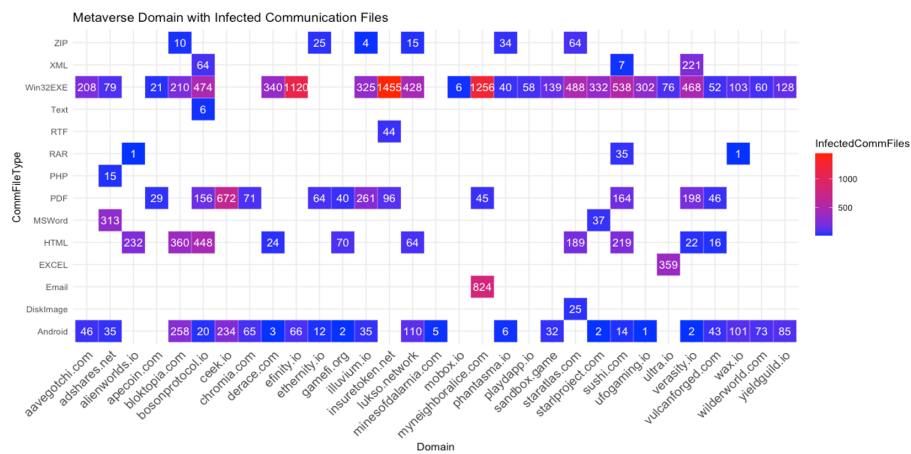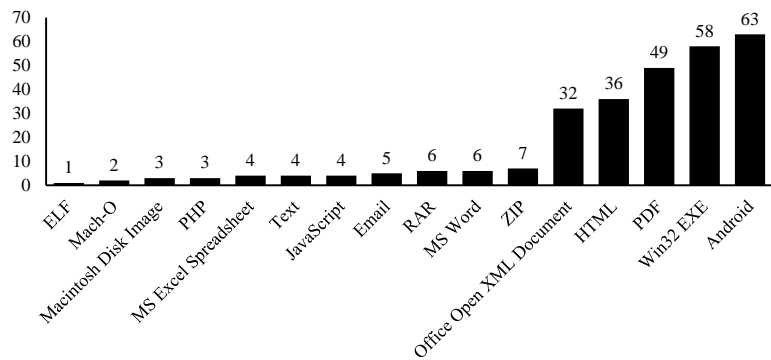
Fig. 1: Metaverse Domain with Infected Referrer Files

Fig. 2: Number of Referrer File Types

each file type in the metaverse domains, with Android and Win32 EXE file types following the same pattern as previously observed. These two file types are dominant and contribute significantly to the detections recorded in the metaverse domains.

5.2   Metaverse Coins Market Capitalization

The market capitalization of each metaverse token is obtained from crypto.com[1]. It is important to note that this value is subject to fluctuations, as with other markets. The data provided in this paper reflects the value at a specific point in time and may have since changed. Despite being a futuristic technology, the metaverse already boasts a

---

[1] https://crypto.com/price/categories/metaverse

Fig. 3: Infected Communication File

Fig. 4: Infected Communication File

trillion-dollar market capitalization. The highest-valued token is worth over a billion USD, while the lowest is approximately one thousand USD.

Table 1 shows the list of metaverse tokens in descending order based on market capitalization for the domains with at least 25 million USD capitalization.

Observations. We analyzed the top metaverse token with at least a market capitalization of about 25 million USD for vulnerability and malicious activities by performing a scan with third-party software. The scan result reveals various malicious detections in 31 out of the 44 metaverse domains, representing about 70% of the domains under consideration as shown in Figure 1 and Figure 3. The malicious detections reported are those obtained from the scan of the metaverse domains, IP addresses, communication files, and referrer files associated with the domains.

5.3   Malicious Activities in Metaverse Coins

Using Virustotal.com, we conduct thorough scans of files, IP addresses, and domains using many security engines, each utilizing unique algorithms to detect any sign of malicious activity. It is important to note that these engines may classify results differently, which is why we meticulously scrutinize associated components such as passive DNS, communication files, and referrer files to determine the presence of any malicious activity accurately.

Table 2. displays the domains of the metaverse, their corresponding security engines, and the types of malicious detections they can identify. These findings are a result of scanning IP addresses that have been linked to their respective domains.

Domain	Security Engines	Type	# Files
playdapp.io	Abusix	Malicious	79
playdapp.io	Xcitium Verdict Cloud	Malicious	58
playdapp.io	CMC Threat Intelligence	Malware	46
bloktopia.com	CMC Threat Intelligence	Malware	210
illuvium.io	CMC Threat Intelligence	Malware	261
bloktopia.com	CMC Threat Intelligence	Malware	360
step.app	Xcitium Verdict Cloud	Malware	544
sushi.com	CMC Threat Intelligence	Malware	588
sushi.com	CMC Threat Intelligence	Malware	655
sushi.com	Criminal IP	Malicious	124
efinity.io	Xcitium Verdict Cloud	Malware	680
myneighboralice.com	Xcitium Verdict Cloud	Malware	822
myneighboralice.com	CMC Threat Intelligence	Malware	824
myneighboralice.com	Xcitium Verdict Cloud	Phishing	248
myneighboralice.com	Xcitium Verdict Cloud	Phishing	840
bosonprotocol.io	CMC Threat Intelligence	Malware	1220

Table 1: Malicious detection and types

Observations. We found eight domains to have malicious infections when the domain IP addresses were scanned. Some domains reported more than one type of malicious detection through different security engines used by virustotal.com. The malicious types in the results are shown in Table 2. Malware, malicious, and phishing are types of files found. The CMC Threat Intelligence security engine was more prevalent, appearing eight times. The table shows the relationship between the metaverse domain and communication files. Every domain that has malicious detection records corresponding communication files. The communications files have shown to have some files with malicious detection, and these files will invariably infect the host domain with malware, phishing, and other maliciousness.

5.4   Metaverse coins with fiat currency to cryptocurrency

Fiat currency in the metaverse refers to using government-issued currencies, such as traditional national currencies (e.g., USD, EUR, JPY) or digital representations of those currencies within virtual worlds or virtual reality environments.

Security Engines	Malicious Type	Count of Malware
CMC Threat Intelligence	Malware	7
Xcitium Verdict Cloud	Malware	3
Xcitium Verdict Cloud	Phishing	2
Xcitium Verdict Cloud	Malicious	1
Abusix	Malicious	1
CMC Threat Intelligence	Malware	1
Total		15

Table 2: Security engines and Malicious types

While virtual worlds primarily operate with their virtual currencies or tokens, some platforms or virtual marketplaces may support the integration of fiat currency as a means of exchange. This integration lets users purchase virtual assets or participate in economic activities using real-world currencies.

Cryptocurrency in the metaverse refers to using digital currencies, typically using blockchain technology, within virtual worlds or immersive virtual environments value [23]. Cryptocurrencies offer a decentralized and secure means of conducting transactions and can play a role in facilitating economic activities within the metaverse.

Categorizing metaverse domains into two groups is crucial for identifying which currency type is more susceptible to malicious activity. These groups include those using fiat currency and those using cryptocurrency. It is important to understand the vulnerabilities associated with each type of currency within these domains.

Observations. After analyzing 44 domains, it was found that 21 of them (48.84%) use fiat currency. Both classifications of domains showed evidence of malicious activity. It was observed that domains using fiat currency did not exhibit any distinct behavior from those using cryptocurrency, nor did it impact market capitalization. The exchange of fiat currency and cryptocurrency in the metaverse domain is considered a potential factor contributing to malicious activity, but the analysis revealed otherwise.

6   Discussion

Our analysis revealed several instances of malicious activity within metaverse domains. Interestingly, the location of the domains and the DNS and CDN service providers did not contribute to detecting these malicious activities. Our investigation revealed numerous communication and referrer files within the domains, many containing malware. This discovery was unsurprising, as communication and information exchange are common on metaverse web pages. Unfortunately, cyber infections within domains are quite common. Cyber criminals often select their targets based on reconnaissance activities or random selection. With ongoing cyber attacks on cryptocurrency domains and pools, we anticipate similar threats to emerge within metaverse tokens.

We have gathered communication files from 44 domains and found malicious activity in 31 of them. However, when we directly scanned the domains and their IP addresses, only 8 out of the 44 domains showed signs of malicious activity, as shown in Fig 5. This means that the number of domains with malicious activity after a direct scan using virustotal.com is much smaller than reported from the communication files and referrer files. It's possible that the large number of communication files with malicious

Domain	Fiat Currency	Domain	Fiat Currency
apecoin.com	No	minesofdalarnia.com	Yes
decentraland.org	No	myneighboralice.com	Yes
axieinfinity.com	No	efinity.io	Yes
sandbox.game	No	insuretoken.net	Yes
enjin.io	No	bloktopia.com	Yes
wemixnetwork.com	No	yieldguild.io	Yes
sushi.com	No	staratlas.com	Yes
ont.io	No	virtua.com	Yes
illuvium.io	No	aavegotchi.com	Yes
wax.io	No	ufogaming.io	Yes
lukso.network	No	adshares.net	Yes
playdapp.io	No	gamefi.org	Yes
highstreet.market	No	starlproject.com	Yes
chromia.com	No	play.staratlas.com	Yes
vulcanforged.com	No	wilderworld.com	Yes
decentral.games	No	step.app	Yes
ceek.io	No	ethernity.io	Yes
mobox.io	No	bosonprotocol.io	Yes
raca3.com	No	derace.com	Yes
ultra.io	No	metahero.io	Yes
verasity.io	No	phantasma.io	Yes
alienworlds.io	No		

Table 3: Metaverse Fiat to Cryptocurrency

detection does not necessarily translate to domain infections. This could be due to various reasons, such as the domains having security checkpoints, anti-malware, firewalls, or policies that prevent infections from corrupt communication files. While our study doesn't dive deeply into communication files, we can conclude that the eight domains we identified also had communication files with malicious activity.

The website Virustotal.com has its own passive DNS service. We have noticed that the passive DNS results show many malicious detections. Passive DNS stores DNS queries for future analysis, which can help detect malicious networks or infrastructure. However, we cannot confirm if the malicious detections in passive DNS are directly linked to the malicious activities in the eight domains mentioned in Fig 5. It is worth noting that these eight domains are also present in the passive DNS malicious results, as seen in communication files.

The body of the analysis is based on several scan results from virutotal.com.

7   Conclusion and Future Work

Our research analyzes the top metaverse tokens with a market capitalization of at least 25 million USD. We examined the corresponding domains and IP addresses and scanned them for malicious activity using virustotal.com. We found that while many associated files had malicious activity, only 18.6% of the domains showed signs of maliciousness. Although our analysis confirms the presence of malicious activity in metaverse domains, we were unable to determine the contributing factors. Further research is nec-
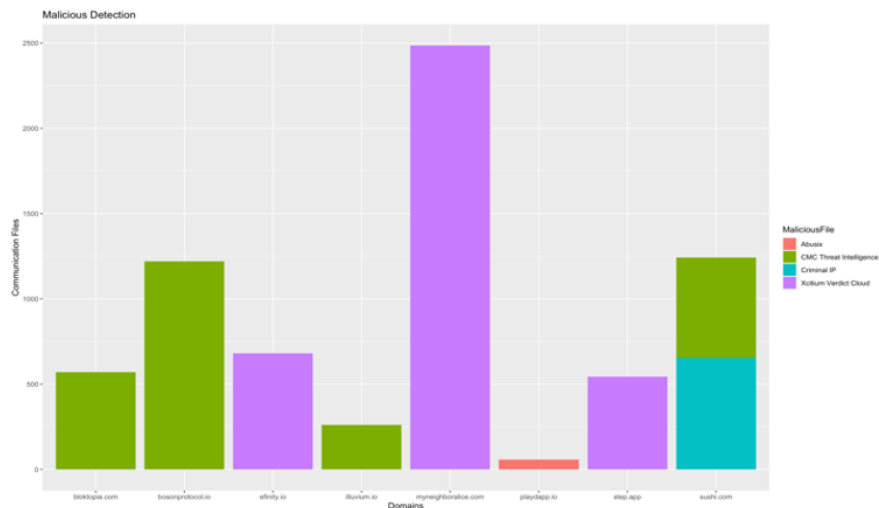
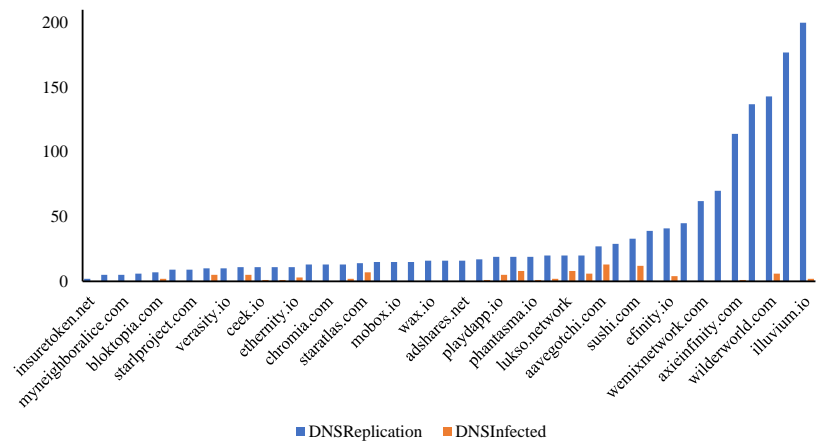Fig. 5: Metaverse Domains with Malicious Detection Types

Fig. 6: Metaverse Domains with Malicious Detection Types

essary to identify the sources and factors that contribute to potential malicious activities in the metaverse.

The confirmation of malicious activities in metaverse domains is undeniable, according to the study. It should be noted that a high market capitalization of tokens does not necessarily indicate a lack of maliciousness. The study has identified various forms of maliciousness that must be taken seriously. In the future, we will expand the number and range of metaverse domains for our analysis, expand the study into fiat currencies and association with the security of the metaverse, and further look into the payload (files) in the metaverse platform and their contribution to the security of such systems.

References

1. Adeniran, A., Mohaisen, D.: Measuring cryptocurrency mining in public cloud services: A security perspective. In: CSoNet. pp. 128–140. Springer-Verlag, Berlin, Heidelberg (2023)
2. Akkus, H.T., Gursoy, S., Dogan, M., Demir, A.B.: Metaverse and metaverse cryptocurrencies (meta coins): Bubbles or future? J. Economics Finance and Accounting **9**(1), 22–29 (2022)
3. Aks, S.M.Y., Karmila, M., Givan, B., Hendratna, G., Setiawan, H.S., Putra, A.S., Winarno, S.H., Kurniawan, T.A., Simorangkir, Y.N., Taufiq, R., et al.: A review of blockchain for security data privacy with metaverse. In: 2022 International Conference on ICT for Smart Society (ICISS). pp. 1–5. IEEE (2022)
4. Buhalis, D., Leung, D., Lin, M.: Metaverse as a disruptive technology revolutionising tourism management and marketing. Tourism Management **97**, 104724 (2023)
5. Choi, M., Azzaoui, A., Singh, S.K., Salim, M.M., Jeremiah, S.R., Park, J.H.: The future of metaverse: Security issues, requirements, and solutions. Human-Centric Computing and Information Sciences **12** (2022)
6. Di Pietro, R., Cresci, S.: Metaverse: Security and privacy issues. In: 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). pp. 281–288 (2021)
7. Giechaskiel, I., Cremers, C., Rasmussen, K.B.: When the crypto in cryptocurrencies breaks: Bitcoin security under broken primitives. IEEE Secur. Priv. **16**(4), 46–56 (2018)
8. Jaber, T.A.: Security risks of the metaverse world. International Journal of Interactive Mobile Technologies **16**(13) (2022)
9. Kshetri, N.: The economics of the industrial metaverse. IT Prof. **25**(1), 84–88 (2023)
10. Kürtünlüoğlu, P., Akdik, B., Karaarslan, E.: Security of virtual reality authentication methods in metaverse: An overview. arXiv preprint arXiv:2209.06447 (2022)
11. Mohaisen, A.: Towards automatic and lightweight detection and classification of malicious web contents. In: Third IEEE Workshop on Hot Topics in Web Systems and Technologies, HotWeb. pp. 67–72. IEEE Computer Society (2015). https://doi.org/10.1109/HOTWEB.2015.20, https://doi.org/10.1109/HotWeb.2015.20
12. Mohaisen, A., Alrawi, O., Mohaisen, M.: AMAL: high-fidelity, behavior-based automated malware analysis and classification. Comput. Secur. **52**, 251–266 (2015)
13. Momtaz, P.P.: Some very simple economics of web3 and the metaverse. FinTech **1**(3), 225–234 (2022)
14. Oosthoek, K., Doerr, C.: Cyber security threats to bitcoin exchanges: Adversary exploitation and laundering techniques. IEEE Trans. Netw. Serv. Manag. **18**(2), 1616–1628 (2021)
15. Rosenberg, L.: Marketing in the metaverse and the need for consumer protections. In: 13th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, UEMCON. pp. 35–39. IEEE (2022)
16. Rosenberg, L.: Marketing in the metaverse: Emerging risks. In: Arai, K. (ed.) FICC. LNCS, vol. 651, pp. 41–51. Springer (2023)
17. Saad, M., Chen, S., Mohaisen, D.: Syncattack: Double-spending in bitcoin without mining power. In: ACM CCS. pp. 1668–1685. ACM (2021)
18. Saad, M., Khormali, A., Mohaisen, A.: Dine and dash: Static, dynamic, and economic analysis of in-browser cryptojacking. In: APWG eCrime. pp. 1–12 (2019)
19. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., Mohaisen, D.: Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials **22**(3), 1977–2008 (2020)
20. Tariq, S., Abuadbba, A., Moore, K.: Deepfake in the metaverse: Security implications for virtual gaming, meetings, and offices. CoRR **abs/2303.14612** (2023)

21. Thomas, M., Mohaisen, A.: Kindred domains: detecting and clustering botnet domains using DNS traffic. In: 23rd International World Wide Web Conference, WWW. pp. 707–712. ACM (2014). https://doi.org/10.1145/2567948.2579359, https://doi.org/10.1145/2567948.2579359

22. Wang, A., Mohaisen, A., Chang, W., Chen, S.: Delving into internet ddos attacks by botnets: Characterization and analysis. In: 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2015, Rio de Janeiro, Brazil, June 22-25, 2015. pp. 379–390. IEEE Computer Society (2015). https://doi.org/10.1109/DSN.2015.47, https://doi.org/10.1109/DSN.2015.47

23. Xu, H., Li, Z., Li, Z., Zhang, X., Sun, Y., Zhang, L.: Metaverse native communication: A blockchain and spectrum prospective. In: IEEE ICC Workshops. pp. 7–12. IEEE (2022)

24. Zaghloul, E., Li, T., Mutka, M.W., Ren, J.: Bitcoin and blockchain: Security and privacy. IEEE Internet Things J. **7**(10), 10288–10313 (2020)

25. Zhao, R., Zhang, Y., Zhu, Y., Lan, R., Hua, Z.: Metaverse: Security and privacy concerns. Journal of Metaverse **3**(2), 93–99 (may 2023)

A   Appendix

Table 1 shows the list of metaverse tokens with at least 25 million USD capitalization.

Metaverse Token	Metaverse Domain	Metaverse Token	Metaverse Domain
Apecoin	apecoin.com	Phantasma SOUL	phantasma.io
Decentraland MANA	decentraland.org	Metahero	metahero.io
Axie Infinity AXS	axieinfinity.com	DeRace DERC	derace.com
The Sandbox	sandbox.game	Boson Protocol	bosonprotocol.io
Enjin Coin ENJ	enjin.io	Ethernity Chain ERN	ethernity.io
WEMIX	wemixnetwork.com	Step App FITFI	step.app
SushiSwap SUSHI	sushi.com	Wilder World WILD	wilderworld.com
Ontology ONT	ont.io	Star Atlas	play.staratlas.com
Illuvium ILV	illuvium.io	Starlink	starlproject.com
WAXP	wax.io	GameFi GAFI	gamefi.org
LUKSO LYXe	lukso.network	Adshares	adshares.net
PlayDapp PLA	playdapp.io	UFO Gaming	ufogaming.io
Highstreet HIGH	highstreet.market	Aavegotchi GHST	aavegotchi.com
Chromia CHR	chromia.com	Terra Virtua Kolect TVK	virtua.com
Vulcan Forged PYR	vulcanforged.com	Star Atlas DAO POLIS	staratlas.com
Decentral Games DG	decentral.games	Yield Guild Games YGG	yieldguild.io
CEEK VR	ceek.io	Bloktopia BLOK	bloktopia.com
MOBOX MBOX	mobox.io	inSure DeFi SURE	insuretoken.net
Radio Caca RACA	raca3.com	Efinity Token EFI	efinity.io
Ultra UOS	ultra.io	MyNeighborAlice	myneighboralice.com
Verasity VRA	verasity.io	Mines of Dalarnia DAR	minesofdalarnia.com
Alien Worlds TLM	alienworlds.io		

Table 4: Metaverse Tokens