Helium-based IoT Devices: Threat Analysis and Internet-scale Exploitations

Conference Paper · May 2023

DOI: 10.1109/WiMob58348.2023.10187762

5 authors, including:

Joseph Khoury
University of Texas at San Antonio
11 PUBLICATIONS **57** CITATIONS
SEE PROFILE

Đorđe Klisura
Louisiana State University
5 PUBLICATIONS **2** CITATIONS
SEE PROFILE

Claude Fachkha
University of Dubai
40 PUBLICATIONS **682** CITATIONS
SEE PROFILE

Elias Bou-Harb
Louisiana State University
160 PUBLICATIONS **3,000** CITATIONS
SEE PROFILE

Helium-based IoT Devices: Threat Analysis and Internet-scale Exploitations

Veronica Rammouz*, Joseph Khoury*, Đorđe Klisura*, Morteza Safaei Pour†, Mostafa Safaei Pour†, Claude Fachkha‡, Elias Bou-Harb*
*The Cyber Center for Security and Analytics, The University of Texas at San Antonio, TX, USA
†San Diego State University, CA, USA
‡College of Engineering and Information Technology, University of Dubai, Dubai, UAE

***Abstract*—With the explosive growth of resource-constrained smart devices and the widespread deployment of Internet-of-Things (IoT) devices, there is an ever-increasing demand for low-energy and cost-effective wireless communication solutions to serve a wide variety of systems and processes. To this end, blockchain-enabled `Helium` devices were conceived to enable Internet services and to support third-party IoT devices. This decentralized paradigm allows individuals and entities to freely engage, monetize and deploy wireless `Helium` hotspots, offering Internet coverage through piggy-backing packets via their existing network and Internet infrastructure (e.g., fiber optics at home). Currently, there are close to 1M operational `Helium` devices deployed in 189 countries, which are owned by 425K accounts. Given this evolving paradigm, in this paper, we take a first step to explore the plausible attack vectors which could potentially impact the confidentiality, integrity, and availability of such `Helium` hotspots. Along this vein, we then scrutinize 2.9 TB of one-way unsolicited Internet traffic arriving at 0.5M monitored dark IP addresses to identify 869,822 darknet events pertained to 6K `Helium` hotspots (as infected devices and DoS victims). By further leveraging active and passive methodologies coupled with public exploitation databases, we uncover medium to critical severity vulnerabilities attributed to 62K online `Helium` hotspots.**

***Index Terms*—`Helium`, IoT devices, Security analysis, Network telescope, Vulnerabilities.**

I. Introduction

The Internet-of-Things (IoT) paradigm extends network connectivity and computing capabilities to electronics, sensors, and systems to generate, share and consume data with minimal human intervention. In the past few years, IoT devices have significantly increased in terms of deployability, heterogeneity and functionality. Indeed, it is estimated that by the end of 2027, 41B devices will be interconnected [1], demanding more agile and modular solutions. Nowadays, the majority of IoT devices depend on long-adopted wireless communications, such as cellular, WiFi, and Bluetooth, which are either power-intensive, expensive or only provide limited coverage, which may not be suitable for mobile and wearable devices; or those that typically demand long-range connectivity, or those in rural areas with stringent mobile requirements, or those with limited power (i.e., battery) resources.

By adopting the "sharing economy" business model, the `Helium` network [2] enables individuals and entities to share their Internet connectivity infrastructure with IoT devices by deploying Long Range Wide Area Network (LoRaWAN) hotspots to enable low-energy Internet access while addressing global coverage challenges. LoRaWAN is a data-link layer protocol supporting long-range, low-power (i.e., devices can run for years on a small battery), and low bit rate, designed specifically for IoT and wireless sensor networks, where end-devices use LoRa to communicate with gateways via a single hop. To achieve this, they use the blockchain infrastructure to build trust by validating every transaction on the public ledger, having hotspot owners witness others, and rewarding and incentivizing them with tokens for validating others or for transporting packets [3]. In contrast to cellular ISPs which deploy a large number of base stations, millions of entities continue to deploy a distributed network of hotspots to generate revenue by utilizing the available infrastructure's capacity. Thus, in brief, `Helium` addresses the high-demand for both static and dynamic clients by providing low-power and long-range Internet connectivity.

Since `Helium` hotspots are widely distributed, playing a critical role in providing Internet connectivity to a broad range of end-devices, they inevitably become susceptible to a plethora of attack vectors. Such misdemeanours could possibly impact their confidentiality, availability, and integrity. According to the `Helium` foundation, most of such hotspot devices are being deployed in consumer realms and critical infrastructure such as manufacturing setups, transportation networks, and telecommunication services [3]. Given that IoT mobile and wearable devices endeavor to continuously connect to several tens and hundreds of these `Helium` hotspots, which are typically operated by enthusiasts who are motivated by blockchain-related income rewards while lacking the skills to secure such systems, security concerns arise not only related to vulnerabilities and exploitations towards such `Helium` hotspots but more importantly, towards their connected (critical) infrastructure and related interconnected components. Hence, for a broader, more trustworthy adoption of such `Helium` infrastructure, related security issues ought to be explored, prioritized and promptly addressed.

Towards this end, this paper takes a first step to investigate the security of the `Helium` infrastructure. More specifically, we focus on the (in)security of the deployed hotspots by initially characterizing their related threat vectors and subsequently by providing unique empirical evidence of their Internet-wide exploitations and existing vulnerabilities. Herein, we frame the contributions of the paper as follows:

- Characterizing and analysing the security posture of `Helium` hotspots via the systematic exploration of their

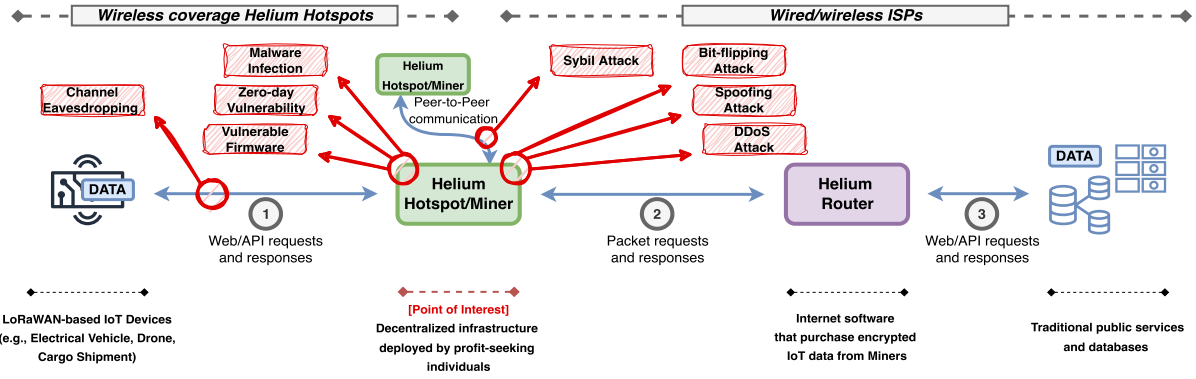

Figure 1. A simplified Helium infrastructure and related attack vectors: The depiction of the Helium decentralized network infrastructure comprising the Helium hotspot/miner and the Helium router. The data transmission between the IoT devices and traditional public services traversing through the Helium infrastructure, along with their plausible threat vectors, are also illustrated.

related plausible attack vectors.

- Drawing-upon more than 2TB of real, one-way Internet-scale empirical data while devising techniques rooted in passive measurements to shed the light on the global exploitations of Helium hotpots while performing an in-depth investigation of such devices.
- Leveraging device search engines which index active devices, coupled with devising and employing methods rooted in application (and banner) grabbing and static analysis to attribute the fingerprinted hotspots to critical and high severity vulnerabilities, while revealing their exact Common Vulnerabilities and Exposures (CVEs).

The paper is organized as follows. In the next section, we discuss plausible attack vectors related to the Helium infrastructure. In Section III, we elaborate on the empirically-driven proposed methodology to infer exploitations and vulnerabilities pertaining to Helium hotspots. In Section IV, we present the generated results and discuss their inferences and insights. Then, in Section V, we briefly present some related work to demonstrate the uniqueness of the proposed work, while in Section VI, we provide some concluding remarks and pinpoint a few endeavors for future work.

II. Attack Vectors threatening Helium hotspots

The rationale behind this work stems from the need to analyse the security posture of Helium hotspots; given that they render major components of the infrastructure. Due to their crucial role in connecting various IoT devices to the Internet, and their high-stake risks related to connected IoT devices, the network and even the blockchain, herein we initially explore their plausible attack vectors. Figure 1 depicts a simplified version of the infrastructure coupled with a number of relevant attack vectors. In the sequel, following the de-facto approach for threat analysis, we structure our narrative by adopting the Confidentiality, Integrity, Availability (CIA) security triad model.

A. Confidentiality attacks

Confidentiality involves measures to restrict unauthorized access to sensitive information. Typically, such measures mitigate cyber (and cyber-physical) attacks that intend to intercept (and disclose) information between (two) communicating entities.

Eavesdropping Attacks. Since Helium hotspots tend to communicate with each other, IoT devices and routers over LoRaWAN using a counter-mode AES encrypted channel could indeed be susceptible to such attacks. In fact, it is possible for eavesdropping to take place through key reuse since the packet counter is not set as a one-time numeric [4], leaving room for communication monitoring and observation of plaintexts, which can be highly problematic by allowing sensitive data to flow towards a malicious actor.

Malware Attacks. Malware is also a common scenario wherein confidentiality can be bypassed, enabling a variety of other attacks that expose sensitive information, including for instance, personally identifying information for identity monitoring. The eminent IoT Mirai botnet [5] is known to compromise smart devices, which is a major deterrent to privacy. Other malware variants [6] collect private keys, seed phrases and credentials, which may also extend to the blockchain and compromise cryptocurrencies and/or digital assets. Moreover, if a hotspot runs vulnerable software, it becomes a gateway to further attacks by exposing the owner's sensitive information. By gaining unauthorized access through theft of credentials, malware via DNS hijacking can move laterally [7] in a network to compromise critical systems. It is possible for such attacks to occur by employing weak and/or default credentials or via scanning for Helium-specific open ports, such as port 44158, which operates the consensus protocol between hotspots.

Zero-day Attacks. Further, if the hotspot management portal was found to host a zero-day vulnerability, new attacks would be introduced, rendering hotspots within a specific ISP, region, vendor, or even the entire autonomous system vulnerable. The consequences of the above-noted attacks can in fact be exorbitant given the distributed nature of Helium hotspots and their capabilities in connecting various end-devices and related infrastructure.

B. Integrity attacks

Integrity involves verifying (and eventually defending against) improper information modifications and destruction. Helium hotspots could indeed be affected by such attacks.

Bit-flipping Attacks. Although communication channels between IoT devices and the cloud servers are typically end-to-

end encrypted, some modifications are still possible. Through the usage of LoRaWAN, an attacker can employ bit-flipping attacks [4] by modifying the bits in a ciphertext, thus allowing the modifications of sensor readings. This often occurs when the integrity check mechanism in LoRaWAN is terminated too early.

Data-Manipulation Attacks. Additionally, a compromised link or a malware-infected hotspot can expedite the alteration of information originating from critical end-devices. Such threats occur through various network attacks or large-scale worm propagations which tend to infect these systems with malignant payloads. For instance, a series of malware-infected `Helium` hotspots within a geographic proximity can collectively induce data alteration and/or falsification associated with cargo shipments or utility meter systems to mislead legitimate parties, hence vandalizing key processes while causing physical and financial impacts.

Blockchain Attacks. Some vulnerabilities may also lead to blockchain attacks, including 51% attacks through consensus mechanisms [8], allowing transaction modifications and double-spending tokens.

Sybil Attacks. Disruptions of the consensus processes, as well as the P2P network can occur by operating many Sybil identities. The ultimate goal of this attack is the initiation of a double-spending incident for what is referred to as "selfish mining". This can occur when a certain amount of nodes in the network are controlled by means of fraud.

Spoofing Attacks. Tampering with the consensus mechanism associated with port 44158 can also take place via spoofing attacks to modify the parameters that characterize the hotspots. Often, some ports are mismanaged and stay open. This could lead to severe persistent threats on the targeted `Helium` network, related blockchain and autonomous systems.

Other Integrity Attacks. Adversarial access to a hotspot may lead to false data injection within the communication directed towards connected IoT devices. For instance, if a zero-day vulnerability is found in a specific vendor's hotspot (or a malicious firmware is injected by an update/patch mechanism), there would be a risk of modifications in the configuration file or via malware installation, posing a complimentary threat to the communication between the hotspot and the designated autonomous system, leading up to data breaches and imminent threats to services and critical infrastructure. The implications of such integrity attacks on various sectors and systems can be indeed debilitating. Just as an example, in the context of electric vehicles piggy-backing on the `Helium` network, an attacker can manipulate electric vehicle charging stations, which could result in the electric vehicle's battery becoming overloaded, or causing crucial instabilities in the grid, damaging the car while broadly affecting the entire ecosystem.

C. Availability attacks

Availability encompasses timely and reliable access to information. Systems' availability is mainly affected by cyber attacks that aim to overwhelm services and/or communication links with illicit requests to disrupt legitimate ones. Intuitively,

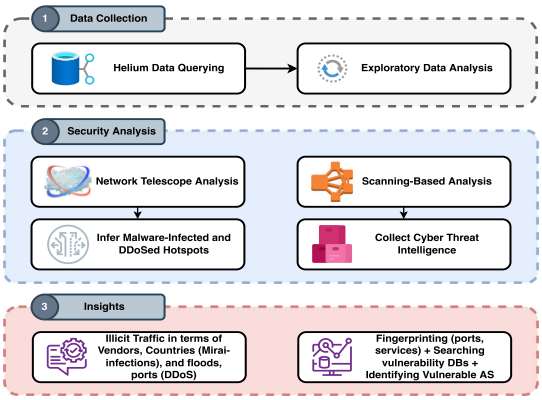

Figure 2. A multi-layer framework used to perform Internet-scale exploration and security analysis of `Helium` hotspot devices.

`Helium` hotspots are susceptible to various attacks that could impact their availability.

Distributed Denial of Service (DDoS) Attacks. Such threats include, but are not limited to, flooding, reflection attempts and buffer overflow exploits. Vulnerable `Helium` hotspots can negatively impact the availability of the entire infrastructure, inducing serious of ramifications that potentially might impact millions of end-devices. For example, DDoS attacks targeting a large subspace of `Helium` hotspots may lead to wide-scale Internet disruptions for numerous end-devices which can have adverse impacts on their associated services within their deployed sectors.

Replay Attacks. Through LoRaWAN, the availability of a hotspot can be rendered offline through message replay or battery exhaustion. A replay attack can jeopardize the availability of the hotspot and/or network in an undetectable fashion, as it does not consist of traditional flooding methods. Through one customized packet, the connection can be taken offline for an extended period of time.

Other Availability Attacks. In the case of IoT botnets, DDoS attacks are a common ultimate goal. As these malware variants infect more and more devices within a network, more hosts are impacted leading up to availability issues. In the event that a zero-day vulnerability is found in any hotspot subpart (e.g., management portals), it may lead to targeted attacks on a given hotspot vendor, via software-based exploitation. Furthermore, DDoS attacks may lead to the disruption of the connected infrastructure by preventing packets from arriving at designated routers, which in turn might induce a significant impact on hotspots utilizing the same ISP infrastructure. As noted in this section, these overarching attack vectors threatening the CIA triad in the `Helium` infrastructure resemble serious manners which we believe ought to be addressed via multi-dimensional collaborations between the `Helium` vendors, hosts and the operational cyber security communities at large. In the sequel, we continue our security analysis via a developed Internet-scale, empirically-driven methodology to shed light on real `Helium` hotspots' exploitations and related vulnerabilities.

III. Empirical approach for inferring Helium exploitations

Figure 2 illustrates our proposed approach, which draws upon a publicly-available, Helium-centric database, along with more than 2TB of darknet (i.e., network telescope) traffic. The latter traffic resembles Internet-wide unsolicited traffic arriving at dark IP sensors; pure passive IP addresses which do not operate any legitimate services. Such one-way traffic arriving at the darknet is by default unsolicited as typically there is no reason to send legitimate traffic to IPs that operate no services. Darknet data has been frequently and repetitively used to shed light on Internet-scale exploitations [9], [10] but has never been employed before to pinpoint Helium-related hotspots' exploitations. We retrieve and leverage, in near real-time, darknet data from the Merit Orion network telescope, who operates around 0.5M dark IP addresses.

A. Helium blockchain database

We initially explore the global Helium hotspot distribution across different hotspot vendors. We infer hotspot devices on the Helium decentralized blockchain network by running SQL queries on the publicly available DeWi relational Helium blockchain database. We gather key information related to Internet-scale distributed Helium hotspot devices, such as owners' identifications, geographic locations, listening public IP addresses and ports, and vendors. It is important to note that in such empirical analysis, we focus on online hotspots operating on public IP addresses. Accordingly, we count the unique IP addresses resembling at least one hotspot within each network.

B. Data analysis from the network telescope

We scrutinize passive illicit traffic [11], namely scanning probes [12] arriving at the telescope (as an indicator of exploitation) and backscatter data (reply packets from victims of DDoS attacks) based on recent data from 2022 and 2023 to infer exploited (and attacked) Helium hotspots at scale. Similar to the work done by Durumeric et al. [13], we separate scanning traffic from backscatter by setting a threshold of 100 for the number of distinct darknet IP addresses that a source IP address contacts. Additionally, for scanning traffic, we specifically parse packets with TCP SYN, UDP or ICMP EchoRequest header fields. For DDoS backscatter, we separate events related to the same victims by utilizing a threshold of 627 seconds, similar to the technique employed by Moore et al. [14]. After processing the events from the darknet [15]–[17], we aggregate them by timestamps, IP addresses, scanner signatures, geolocation, and ports used correlated with the Helium blockchain database. This allows the identification of infected Helium hotspots and those which have fallen victims to DDoS attacks. For those hotspots which were found to be compromised and scanning the darknet IP space, we further deduced if they were Mirai-related (by searching for their known signature within their headers; namely, if the TCP sequence number is equal to the destination IP + 1).

C. Inferring Vulnerabilities in online Helium hotspots

Herein, we utilize active measurements by employing device search engines including Censys [18] and Zoomeye [19] to collect device artifacts such as banners/dashboards, open ports, services [20], vendors' names, firmware and geolocations to characterize hosts which are correlated with the IP addresses from the Helium blockchain database. We further rely on indicative services suggesting peer-to-peer, decentralized communications such as Point-to-Point Tunneling Protocol (PPTP), Erlang Port Mapper Daemon (EPMD), and LibP2P, which are directly relevant in the Helium context. Investigated ports of interest include 44158/TCP and 1680/UDP, which establish communication and Proof of Coverage (PoC) to infer the hotspots, respectively. We also perform static analysis on the obtained dashboards/web portals to search for embedded weaknesses, including weak/default credentials by scrutinizing the banners. We leverage this data to investigate the Common Vulnerabilities and Exposures (CVEs) and/or Common Weakness Enumerations (CWEs) pertaining to the pinpointed Helium hotspots by correlating the artifacts with public vulnerability databases such as NIST NVD. Indeed, given our understanding on how such Helium hotspots can be identified and remotely fingerprinted [21], we note that an attacker would be also capable of executing the same approach with malicious intents, pragmatically threatening the CIA of the hotspots and connected infrastructure.

IV. Empirical Results

A. Exploring Helium hotspots in the Wild

We disclose 987,290 active hotspots that are currently deployed globally. We analyze publicly-facing devices, which amount to 239,097. We find that 39.5% of all online hotspots belong to Bobcat, 19.9% to SenseCAP, 12.4% to Cal-Chip connected devices, and 8.6% owned by RAKWireless clients. By executing a statistical analysis on the associated ports, we find that 230,224 have port number 44158/TCP open, which is known to be employed by Helium hotspots to establish communications with other hotspots. We also discover that there are 6,811 instances with port number 44159, 1,390 with port 44160 and 672 with port 44161 opened. We deduced that Helium hotspots mostly operate on ports within a close range of 44158, which is associated with the "UNKNOWN" service and "multistream" from the banners' information. Such sample of data can be employed by malicious actors to remotely execute reconnaissance activities and possibly target/exploit Helium hotspots. Moreover, it is observed that most of the online hotspots of Bobcat vendors are located in London, UK, Cal-Chip are mostly deployed In Los Angeles, and SenseCAP hotspots are in Istanbul.

B. Internet-scale Infected Helium hotspots

Per the proposed approach of Figure 2, after inferring public IP addresses from the Helium blockchain relational database, we correlate the addresses with illicit network traffic (i.e., source IPs) targeting the Orion IP darknet address space. We find 869,822 events related to 6,036 unique hotspots; 5,984 of them are found to be compromised, emitting scanning

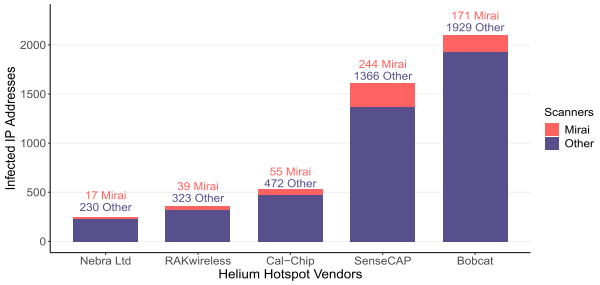

Figure 3. Number of `Mirai` and non-`Mirai` infected hotspots per vendor (Top 5)

activities, while the rest correspond to hotspots which have been targeted by DDoS. We note that 645 of the infections were attributed to `Mirai`, whereas the rest are originating from different, evolving variants. Figure 3 presents the number of `Mirai` (and non-`Mirai`) infections associated with the top 5 most infected `Helium` hotspot vendors. We perceive an evolving set of malware exposing the hotspots, which could resemble a neat idea for conducting further research work in this area. We further discover 51 TCP flooding DDoS targeting ports 80 and 443, and a number of attacks on port 5060 coupled with a few ICMP attacks targeting the hotspots. In order to vet our findings related to the inferred `Helium` infections, we correlated the output with the `greynoise` online service, which typically indexes Internet-wide scanning activities, including those of IoT botnets. We observe around 85% accuracy; note that `greynoise` does not have darknet visibility and is not `Helium`-specific. However, we believe this accuracy is representative of our approach's capability in disclosing "in-the-wild" infected `Helium` hotspots.

C. *Inferred `Helium` Vulnerabilities*

We aim herein to explore whether the deployed `Helium` hotspots contain any embedded vulnerabilities. To accomplish this, we first leverage Censys and Zoomeye, two search engines which index devices on the Internet. To attribute the hotspots to vulnerabilities, we search for empirical artifacts including dedicated ports, application-layer services and vendor terms (recall Section III-C) related to the publicly-available `Helium` hotspots. Table I summarizes our findings, detailing the exact uncovered vulnerability and the number of impacted hotspots. To the best of our knowledge, the inferences and insights herein are among the first to report on vulnerabilities, which specifically impact deployed `Helium` hotspots "in-the-wild".

Elaborately, we discover 644 instances of the software `AIOHTTP` having the terms "miner" and "helium" in the HTML tags belonging to their respective dashboards. These banners also include vendor terms `SyncroBi.t` and `FreedomFi` by observing data related to TCP ports 80 and 443. We correlate these instances with "CWE-601: URL Redirection to Untrusted Site", denoted in "CVE-2021-21330". Apart from this vulnerability, we find 4,563 instances of the software `PalletsProjects Werkzeug` tagged with the vendor `SenseCAP M1`. For certain versions of this software, we find a critical weakness, namely, "CWE-444: Inconsistent

Table I
UNCOVERED `HELIUM`-CENTRIC VULNERABILITIES

Severity	CVE/CWE	Description	# of Hotspots
Critical	CWE-264	Permissions, Privileges, and Access Controls	31,011
	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	2,601
	CWE-287	Improper Authentication	323
	CWE-787	Out-of-bound Write	298
High	CVE-2014-9222	Memory Corruption	21,866
	CVE-2011-3280	NAT Memory Leak	272
	CVE-2013-548	Device Reload on NATed Devices	116
	CVE-2009-3322	DoS (TCP Flood)	116
	CVE-2022-21972 116	Remote Code Execution	116
	CVE-2021-29379	Command Injection	62
	CVE-2022-23492	Resource Exhaustion	6
Medium	CVE-2007-1833	Loss of Voice Services	283
	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	134

Interpretation of HTTP Requests" which occurs in outdated versions of the HTTP protocol. Additionally, we find that port 44158 is associated with an "UNKNOWN" service and has the term `_x13/multistream/1.0.0` in their banners of all its instances. These artifacts are also shown to be embedded within those having *(i)* port 49152, which is found to be operating through the `libp2p-multistream` service and through *(ii)* port 2000, which is associated with the service `MIKROTIK_BW`. We also infer 4 instances of `Mikrotik` RouterOS with open port 44158, vulnerable to DoS attacks with reference to "CVE-2020-22844". Another interesting find concerns port 4369 with the `EPMD` service, for which we pinpoint 323 hotspots with banners including the phrase `_x00_x00_x11_x11name miner at port x`, where x resembles numerous ports. This service is associated with CWE-287. Derived from the web portals' static analysis, we infer 33 out of 828 dashboards related to `SyncroB.it`, containing very weak credentials with default passwords. 4 devices related to `Linxdot` are also exposed to weak/default credentials. Additionally, we note that `Panther` possess 375 default passwords, whereas we infer 87 `Pisces` with such credentials, enabling easy SSH brute-force. As depicted in Figure 4, we disclose that autonomous systems in Turkey and Germany hosts the largest number of vulnerable `Helium` hotspots.

V. RELATED WORK

Since the inception of the `Helium` decentralized wireless network in 2018 [2], there has been little or no research work elaborating the security and privacy posture of its software and coupled components. As previously noted throughout the paper, such critical components including `Helium` hotspots handle essential flow of information and operations, entailing prompt attention and thorough scrutiny. Jagtap et al. [22] conducted an empirical study to understand the usage, patterns,

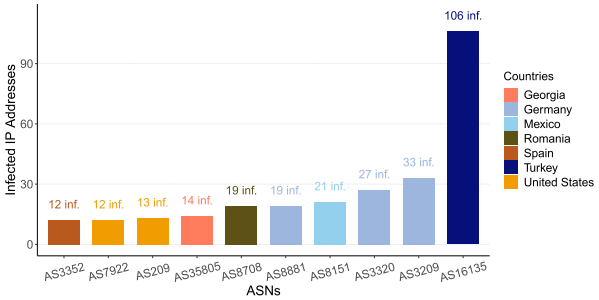

Figure 4. Vulnerable Autonomous Systems based on gathered insights.

and insights from what they called *"The People's Network"*, namely, the Helium network. The authors reported some relevant statistics such as the deployment of the hotspots, their ownerships, and the hotspot transfer transactions over time. Moreover, the authors accentuated on *(i)* the uncontrolled and unplanned deployment of Helium hotspots, *(ii)* the excessive dependence on residential ISPs, and *(iii)* the competition imposed by the Helium infrastructure on traditional communication markets (e.g., 5G networks). Additionally, Aras et al. [23] explored security vulnerabilities of LoRa, in which they discussed numerous vulnerabilities and attack vectors in that realm including jamming, replay, and wormhole attacks.

In this work, we take a first step towards characterizing and empirically evaluating the insecurity of Helium hotspots, which resemble key infrastructure components. We uniquely approach this by initially depicting a brief taxonomy of their plausible threat vectors, and by subsequently drawing-upon empirical network traffic, relevant databases, indexing services, and active/passive methodologies. Broadly speaking, the developed tools, methods and techniques present a transformative perspective to explore the security of such Helium hotspots, while the derived inferences and insights demonstrate the pragmatic issue of wide-scale spread of exploitations and embedded, yet to be patched vulnerabilities. While these outputs aim at alarming about the eminent threat, given this evolving new technology, the work also predominantly aims at laying down the foundation for future security and resiliency research work addressing the Helium infrastructure.

VI. Conclusion

The Helium network, powered by the blockchain, is a model to incentivize providers and consumers to offer low-power, low-bandwidth and short-range wireless communication services. The democratization of such service has indeed given rise to new emerging threats. In this paper, we shed light on the plausible attack vectors of Helium hotspots by characterizing and analyzing their security posture. We discover a significant number of infected hotspots, victims of DDoS attacks, and artifacts leaving the Helium hotspots at risk of being fingerprinted and targeted. We also uncovered embedded vulnerabilities, which not only could impact the security of the hotspots but also the coupled infrastructure. Mitigating such attacks necessitate proper hardening of Helium hotspots, which could possibly be achieved by using secure credentials, blackholing, vulnerability provisioning, among others. Further, we see a dire need for vendors, sector operators and consumers to work together for achieving the much-needed security objective, which will hopefully permit the wide-scale adoption of the Helium paradigm. As for future work, we are currently working on fortifying the malware-infection (and vulnerability) evidence as well as attempting to curate Helium-specific forensic artifacts using offensive methodologies.

References

[1] L. et al., "A review and state of art of internet of things (IoT)," *Archives of Computational Methods in Engineering*, pp. 1–19, 2021.

[2] Helium Team, "A whitepaper on helium," http://whitepaper.helium.com/, 2022.

[3] W. et al., "Development of iot-based hybrid helium drone for flight time enhancement," in *Proceedings of International Conference on Intelligent Manufacturing and Automation: ICIMA 2022*. Springer, 2023, pp. 329–339.

[4] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security vulnerabilities in lorawan," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2018, pp. 129–140.

[5] S. Torabi, E. Bou-Harb, C. Assi, E. B. Karbab, A. Boukhtouta, and M. Debbabi, "Inferring and investigating iot-generated scanning campaigns targeting a large network telescope," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 402–418, 2020.

[6] M. Dib, S. Torabi, E. Bou-Harb, and C. Assi, "A multi-dimensional deep learning framework for iot malware classification and family attribution," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1165–1177, 2021.

[7] B. Bowman, C. Laprade, Y. Ji, and H. H. Huang, "Detecting lateral movement in enterprise computer networks with unsupervised graph ai." in *RAID*, 2020, pp. 257–268.

[8] Y. et al., "Analysis of security in blockchain: Case study in 51%-attack detecting," in *2018 5th International conference on dependable systems and their applications (DSA)*. IEEE, 2018, pp. 15–24.

[9] M. S. Pour, J. Khoury, and E. Bou-Harb, "Honeycomb: A darknet-centric proactive deception technique for curating iot malware forensic artifacts," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2022, pp. 1–9.

[10] J. Khoury, M. Safaei Pour, and E. Bou-Harb, "A near real-time scheme for collecting and analyzing iot malware artifacts at scale," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–11.

[11] E. Bou-Harb, M. Debbabi, and C. Assi, "A systematic approach for detecting and clustering distributed cyber scanning," *Computer Networks*, vol. 57, no. 18, pp. 3826–3839, 2013.

[12] Bou-Harb, Elias and Debbabi, Mourad and Assi, Chadi, "Big data behavioral analytics meet graph theory: on effective botnet takedowns," *IEEE Network*, vol. 31, no. 1, pp. 18–26, 2016.

[13] Z. Durumeric, M. Bailey, and J. A. Halderman, "An Internet-Wide view of Internet-Wide scanning," in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 65–78.

[14] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, "Network telescopes: Technical report," 2004.

[15] E. Bou-Harb, N.-E. Lakhdari, H. Binsalleeh, and M. Debbabi, "Multidimensional investigation of source port 0 probing," *Digital Investigation*, vol. 11, pp. S114–S123, 2014.

[16] M. S. Pour, A. Mangino, K. Friday, M. Rathbun, E. Bou-Harb, F. Iqbal, S. Samtani, J. Crichigno, and N. Ghani, "On data-driven curation, learning, and analysis for inferring evolving internet-of-things (iot) botnets in the wild," *Computers & Security*, vol. 91, p. 101707, 2020.

[17] E. Bou-Harb, M. Debbabi, and C. Assi, "Behavioral analytics for inferring large-scale orchestrated probing events," in *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2014, pp. 506–511.

[18] Censys Team, "Censys: A search engine for internet-connected devices," https://censys.io/, 2022.

[19] Zoomeye Team, "Zoomeye: A search engine for internet-connected devices," https://www.zoomeye.org/, 2022.

[20] C. Wheelus, E. Bou-Harb, and X. Zhu, "Tackling class imbalance in cyber security datasets," in *2018 IEEE International Conference on Information Reuse and Integration (IRI)*. IEEE, 2018, pp. 229–232.

[21] E. Bou-Harb, M. Debbabi, and C. Assi, "A statistical approach for fingerprinting probing activities," in *2013 International Conference on Availability, Reliability and Security*. IEEE, 2013, pp. 21–30.

[22] Jagtap et al., "Federated infrastructure: usage, patterns, and insights from" the people's network"," in *Proceedings of the 21st ACM Internet Measurement Conference*, 2021, pp. 22–36.

[23] Aras et al., "Exploring the security vulnerabilities of lora," in *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*. IEEE, 2017, pp. 1–6.