

Your IP Camera Can Be Abused for Payments: A Study of IoT Exploitation for Financial Services Leveraging Shodan and Criminal Infrastructures

Yuba R. Siwakoti¹, Manish Bhurtel¹, Danda B. Rawat¹, *Senior Member, IEEE*, Adam Oest², and RC Johnson

Abstract—The Internet of Things (IoT) devices are being abused by exploiting their vulnerabilities. Despite the significant efforts to improve IoT security, IoT devices are still at higher risk of exploitation than computer systems. First, this paper identifies vulnerable IoT devices by applying a sampling strategy incorporating Common Vulnerabilities and Exposures (CVE) entries, Shodan’s exposure, and public research documents. Then, we investigated IoT abuses in financial crimes for 17 months (October 2021 to February 2023) by mapping IoT devices exposed by Shodan with proxies found in the darknet, underground forums, and Telegram channels. After investigation, we conclude with reasonable confidence that exposed IoT devices are taken over and abused as proxies in criminal activities such as credential stuffing attacks and financial crimes like illegal money transfers, cryptocurrency trading and stealing, and credit card fraud. Our study reveals that cameras (IP, network, security) are mostly abused IoT devices as proxies, followed by NAS storage.

Index Terms—IoT security, vulnerable IoT devices, IoT abuses, IoT proxies, malicious infrastructure, financial crimes.

I. INTRODUCTION

IoT SECURITY has been studied in the past focusing on different research topics such as vulnerability analysis [1], [2], threats and attacks [3], [4], [5], and criminal infrastructure [6], [7], [8]. Typical cyberattacks against IoT where IoT devices are used to spread malware or involved in botnets are well studied [9]. However, there is no sufficient study on the abuse of IoT devices in financial crimes.

Typical financial crimes are specific to stealing financial information, such as credit card numbers, bank account

login credentials, and private personal information, to commit fraud or identity theft, as well as manipulate financial transactions for illegal gain, attack vectors for committing financial crimes can be particularly inventive. In contrast, other forms of cybercrime could be motivated by espionage, political activities, or simply causing chaos. Several attack vectors, including phishing, social engineering, man-in-the-middle (MitM) attacks, ransomware, and malware attacks, are also employed in other forms of cybercrime. However, financial cybercriminals may also employ more specific attack vectors, including ATM skimming, point-of-sale (POS) attacks, or fraudulent money transfers using accounts that have been compromised.

Financial institutions (FIs) are one of the primary targets of attackers. A FI is not limited to a business entity but represents a trustful platform to many people and businesses. Cyberattacks on FI are more crucial than attacks on other businesses because such attacks involve monetary losses and pose greater risks to the overall security ecosystem, leading to societal imbalance. Attackers are constantly targeting FIs to impersonate accounts with high money value or accounts associated with rich people. Vulnerable IoT devices in financial services can provide the breeding ground for targeted impersonation attacks [7].

Lately, IoT-enabled and IoT-related security risks to FIs are rising as more and more smart devices are used for financial transactions, and most of those transactions are online [10]. Vulnerable IoT devices are easy targets for cyber attackers to enter the FIs’ network and potentially carry out large financial frauds. FIs may deploy insecure IoT devices in the same network with critical infrastructure, creating entry points for attackers and posing risks to the networked and critical financial systems.

Among these different security risks, this study consists of exploits where IoT devices participate in attacks posing growing threats to security, focusing on Financial Institutions (FIs). Collecting the evidence of exploits where IoT devices can be abused for financial crimes, such as transferring money illegally from an account, cryptocurrency stealing, and illegal trading, is an interesting research problem. Criminals can also exploit IoT devices to create fictitious accounts to carry out financial crimes. To address those issues, in this paper, we contribute to identifying major vulnerable IoT devices, associated exploits, and evidence of their abuses for financial crimes.

Received 17 November 2023; revised 21 May 2024; accepted 14 October 2024. Date of publication 17 October 2024; date of current version 31 December 2024. This work was supported in part by the MasterCard Research Impact Funds, PayPal Research Gift funds, the U.S. National Science Foundation under Grant CNS/SaTC 2039583, and in part by the DoD Center of Excellence in AI and Machine Learning (CoE-AIML) at Howard University with the U.S. Army Research Laboratory under Contract W911NF-20-2-0277. (Corresponding author: Danda B. Rawat.)

Yuba R. Siwakoti was with Howard University, Washington, DC 20059 USA. He is now with the Department of Computer Science, Central Washington University, Ellensburg, WA 98926 USA.

Manish Bhurtel and Danda B. Rawat are with the Department of Electrical and Computer Science, Howard University, Washington, DC 20059 USA (e-mail: db.rawat@ieee.org).

Adam Oest was with the Security Department, PayPal Inc., San Jose, CA 95131 USA. He is now with the Selling Partner Services, Amazon, Phoenix, AZ 85043 USA.

RC Johnson was with PayPal Inc., San Jose, CA 95131 USA. He is now with the Cybersecurity and Technology Controls Group, JPMorgan Chase, Phoenix, AZ 85018 USA.

Digital Object Identifier 10.1109/TCE.2024.3482708

Our Contributions:

- 1) *Identify major vulnerable Consumer IoT devices:* Selection of IoT devices is challenging in many IoT security research. If we choose popular device types, there is a probability that unpopular devices may be more vulnerable and contribute more security risks than popular ones. If we select the IoT device category randomly, again, there is a chance of missing insecure devices. Therefore, we apply a sampling strategy to select the potentially most vulnerable consumer IoT device categories. A similar strategy can be applied in other studies as per the requirement and relevance of the problem.
- 2) *Vulnerabilities enabled by IoT devices and status of IoT exploits:* We extract vulnerabilities enabled by selected IoT devices with reported CVE entries. We also rank IoT devices by exploits and their temporal statistics for all categories of IoT for the study period.
- 3) *Evidence of IoT abuses:* We investigate the evidence of IoT devices' abuse as proxies in criminal infrastructures. Attackers exploit those IoT proxies to hide their identities while executing financial crimes. We reveal that proxies are being exploited in criminal activities such as cracking accounts with credential stuffing, stealing/trading cryptocurrencies, illegal money transfer/trading in the darknet market, and credit card fraud.
- 4) *Security recommendations against IoT abuses:* We present security recommendations to consumers, policy-makers, industries, and FIs to act collaboratively against IoT-related financial crimes.

Paper Organization: The rest of the paper is organized as follows. Section II presents the background and related work followed by the threat model in Section III. The proposed methodology is discussed in Section IV. Section V presents the analysis of IoT exploitation followed by discussion and security recommendations in Section VI. Section VII points to the limitations of the paper and discusses possible future research problems. Finally, Section VIII concludes the paper.

II. BACKGROUND AND RELATED WORK

A. Background

In this section, we present a background of IoT architecture and layer-wise vulnerabilities and attacks, followed by a description of terms, concepts, and tools used in this paper in IoT security.

1) *IoT Architecture and Its Representative Layer-Wise Vulnerabilities:* A study of IoT architecture that delves into different aspects of IoT and its security challenges is conducted in a layered fashion. The security of IoT is contingent on its architectural elements, communication protocols, and applications. IoT encompasses diverse devices with varying capabilities, technologies, protocols, and security needs, resulting in vulnerabilities and threats at different levels of the IoT architecture. While there isn't a universally accepted IoT architecture, a widely recognized one involves a hierarchical arrangement of perception, network, and application

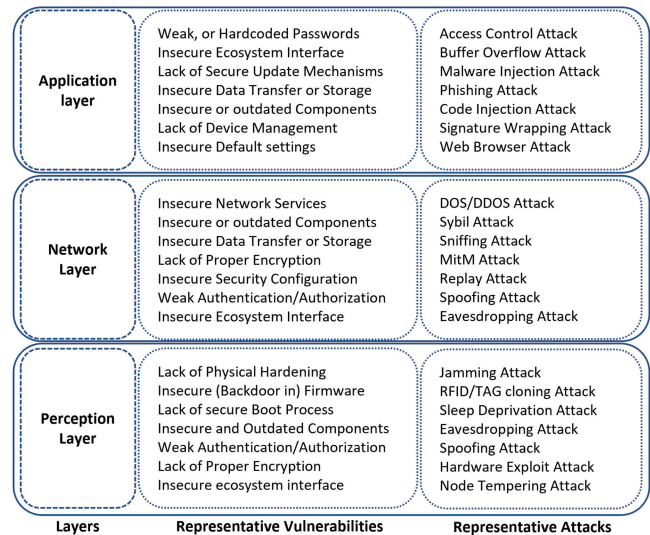


Fig. 1. IoT architecture and its layer-wise vulnerabilities.

layers [11], [12]. In this section, we introduce a three-layer IoT architecture and discuss communication protocols, potential vulnerabilities [13], and attacks [14] in each layer, as illustrated in Fig. 1. The associated vulnerabilities are broadly classified and ranked as per severity by Open Web Application Security Project (OWASP) [15] as the top ten IoT.

2) *A Description of Concepts, Terms, and Tools Used in This Paper:* Shodan¹ is an IoT search engine that has gained popularity recently for vulnerability assessment and security research. It explores exposed products and their services.

CVE (Common Vulnerability and Exposure) is a compilation of vulnerability databases that are maintained and made public by MITRE.² There is a synchronized version of this database that is maintained by NIST, which is referred to as NVD database [16].

Cyberattacks to FI consist of attacks causing business disruption, data breach, and financial fraud [17] while impacting the systems' availability, confidentiality, and integrity. Financial crimes include fictitious account creation, illegal transfers, stealing money and cryptocurrencies, and illegal trading.

Criminal infrastructure refers to a collection of software, devices, tools, and platforms cybercriminals use to carry out malicious activities. The toolkits that are frequently used in such criminal infrastructure include combos, bots, malware, configs, proxies, OpenBullet, Proxifier, FoxyProxy, ransomware, exploits, ProxyCap, Checker, and many more.

A *Proxy* can be a software or hardware component that functions as a mediator to conceal the true identities of the sender or receiver. HTTP, HTTPS, SOCKS4 (Socket Secure 4), and SOCKS5 are frequently employed proxies for anonymous Internet or network traffic.

Configs is an abbreviated version of configuration files containing crucial settings such as IP addresses, URLs, timer,

¹<https://www.shodan.io/>

²<https://cve.mitre.org/>

loader, encryption keys, and scripts required to carry out attacks [18].

Combos are stolen credentials consisting of user/password pairs that are formatted following the requirements of attack tools.

*OpenBullet*³ and *Checker* are attacking software that configures bots, combos, and proxies to automate large-scale attacks.

Proxyfier, *ProxyCap*, *FoxyProxy* are software to add proxies to tunnel traffic from the network/Internet anonymously. Proxyfier enables applications to communicate through HTTP and SOCKS proxies even though the applications don't support proxies directly: ProxyCap and Foxyproxy tunnel network connections and traffic with multiple proxy servers.

*TOR (The onion Router) Browser*⁴ is a browser mainly used to access the darknet onion channels that block trackers, defends against surveillance, resists fingerprinting, and provides multi-layer encryption.

*Nessus*⁵ is vulnerability scanning tool popular in security community.

Credential Stuffing is an attack where stolen usernames and passwords of one service are used to access other services.

Identity Theft is stealing someone's personal information such as credit card information, medical records, financial information, etc.

IoT abuses involve exploiting flaws or security vulnerabilities to compromise or infect IoT devices, which are then misused along with other attack software or toolkits to benefit the attackers.

A *bot* is a software application designed to automate tasks or replicate human actions to make processes more efficient. Malicious bots, utilized by cybercriminals, are responsible for illicitly acquiring content, spreading spam, or carrying out attacks. A *botnet*, on the other hand, refers to a collection of infected machines, each known as a "bot," which is remotely controlled by an attacker to execute large-scale attacks.

Cyber Threat Intelligence (CTI) sources are various channels from which information and data related to cyber threats can be collected. Some of the CTI sources used in this paper are darknet, underground forums, Telegram channels, etc. These sources provide insights into potential security risks and vulnerabilities.

Darknet is an obscure section of the Internet that remains unlisted by conventional search engines, which offers privacy and a shield of anonymity to its users and is frequently utilized for illicit purposes.

Underground Forums are online communities where people engage in discussions and exchange information related to unlawful or unauthorized actions, frequently operating on the open, publicly accessible Internet.

2FA and MFA Bypassing involves finding ways to circumvent the extra layer of security layers deployed to authenticate users. Malicious Users often use phishing and

social engineering to exploit existing vulnerabilities and gain unauthorized access.

B. Related Work

IoT devices are one of the major targets of attackers as those devices are widespread and easier to compromise due to their vulnerable security position [1], [3]. Weak programming practices and the utilization of outdated components [19], weak security interfaces, lack of security updates, inadequate privacy protection, and insecure data transfer and storage [15] are among the other significant vulnerabilities. Reference [20] reviewed the mechanism of cybercrime facilitated by insecure IoT devices and discussed that the vulnerability of such IoT devices is expected to offer a broader range of possibilities for wrongdoers to engage in criminal activities and furnish them with more valuable data to leverage.

Webcams, printers, and smart TVs were found vulnerable in a study [2] using Shodan and Nessus. However, the study was conducted on a limited scale, with only a few types of IoT devices out of the thousands available. Similarly, [21] analyzed consumer IoT devices like IP cameras, DVRs, routers, printers, and home media servers. As per the authors, their selection is influenced by past exploitation, wide deployment, and adoption without further explanation.

In underground communities for cyberspace, attackers discuss attack tools, device exploits, and hacking innovations [6], [7], [22]. Active underground communities are looking for ways to improve their attack & monetization capabilities in different languages. Among them, the Russian underground is at the top in attack sophistication & monetization capabilities, followed by Portuguese, English, Arabic, and Spanish communities [6].

Billions of misconfigured programable IoT devices are found online, and among them, more than ten thousand are exploited by adversaries and attacked honeypots set with 200,000 attack instances [23]. Attackers use proxies to make live requests to legitimate websites, circumventing multi-factor authentication while intercepting data submitted by victims, posing serious challenges to financial organizations [24]. Security vulnerability related to exposures and SSL/TLS deployment status has been studied in [25] where the majority of studied IoT devices have either no SSL/TLS deployed or insecure and outdated versions have deployed, which poses higher risks on IoT and overall Internet security.

Some criminal services already exist while others are evolving and emerging with systematic hacking innovations [22]. One of the evolving organized criminal services was discussed in impersonation-as-a-service (IMPaaS) [7], which sells user profiles consisting of credentials, cookies, fingerprints of users & devices. Such leaked users' profiles and other meta-data enable attackers to circumvent risk-based authentication systems. In addition to IMPaaS, other criminal services are evolving and may pose significant threats to IoT security. These services include PPaaS (Personal Profile as a Service), VDaaS (Vulnerability Discovery as a Service), TSaaS (Target Selection as a Service), and HRaaS (Hacker Recruiting as a Service) [22].

³<https://openbullet.github.io/>

⁴<https://www.torproject.org/>

⁵<https://www.tenable.com/products/nessus>

TABLE I
COMPARING OUR PAPER WITH RELATED LITERATURE

Speciality/Feature Covered	[1]	[2]	[3]	[6]	[7]	[8]	[20]	[21]	[23]	[26]	[27]	[29]	Our Paper
Vulnerabilities Associated with Exposure	●	●	◐	○	○	○	◐	◐	●	○	○	●	●
Vulnerabilities/Attacks Enabled by IoT Devices	●	●	◐	○	○	○	●	●	●	●	●	◐	●
Vulnerabilities Scanning Performed	●	●	○	○	○	○	○	●	●	○	●	◐	◐
Exploits in the Wild	○	○	◐	◐	◐	◐	○	●	◐	◐	●	●	●
Temporal Analysis of Exploits	○	○	○	◐	○	○	○	○	○	◐	●	○	●
Insights from Cyber Threat Intelligence Sources	○	○	●	●	●	●	○	●	○	●	◐	◐	●
Sampling Strategy to Identify Vulnerable Devices	◐	◐	○	○	○	○	○	◐	◐	○	○	○	●
Study Collaborated with Industry's Intelligence	●	○	○	○	◐	○	○	○	○	○	○	○	●
Mechanisms of Exploitation	○	◐	●	●	●	●	●	○	●	●	●	●	●
Evidence of Exploitation	○	○	●	●	●	◐	○	○	●	◐	●	○	●

Legend: ● Yes ○ No ◐ Partially/Indirectly

Hack-for-hire services have been available in the Underground, where attackers gain control of victim accounts by continuously enhancing their hacking capability [8]. In those criminal services, attackers use sophisticated phishing techniques to circumvent multi-factor authentication.

IoT malware threats, including their evolution, attack vectors, target architecture, target device, delivery methods, exploitation techniques, and detection methods, are discussed in [26] leveraging two investigation frameworks Cyber Kill Chain and Mitre ATT&CK for ICS. They presented common threat patterns of malware families in different phases, starting from network scanning, initial access of IoT devices, malware delivery, exploitation, and evasion from security measures. Similarly, the evolution of the Mirai botnet and how Mirai variants exploit IoT devices for various cyberattacks are discussed in [27]. The IoT malware analysis and detection technique proposed in IoT malware detection architecture (iMDA) using channel-boosted and squeezed CNN [28] that effectively discriminates malware from benign instances by analyzing textural, contrast, and pattern variations.

The aforementioned literature did not sufficiently discuss how IoT devices are abused and how identified malicious activities are connected to financial crimes. Additionally, those studies lacked validation of criminal services and exploitation with FI's security intelligence. However, we collected evidence of IoT abuses and validated those exploitations with feedback from reputed FI's security intelligence, which discussed how IoT devices are abused in financial crimes. Such validation increases the trust and reliability of the study and helps assess the real impacts of the attack landscape. Furthermore, past studies lacked a proper selection method to choose major vulnerable devices under study, so we applied a sampling strategy in our research.

We presented a comparison of our study with related literature in Table I, which shows the novelty of our paper and how this paper advances our understanding of IoT vulnerabilities and their exploitation.

III. THREAT MODEL

Attackers are looking for exposed IoT devices, usually by tools like Shodan, and are aiming to compromise them by leveraging attacking software like OpenBullet, configuring with bots and combos. Once compromised, IoT devices are

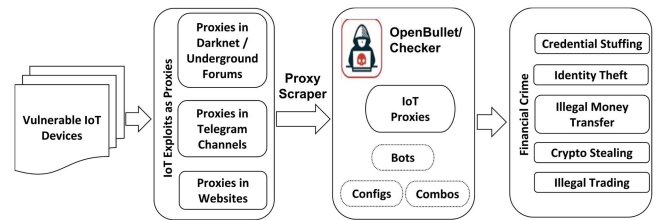


Fig. 2. Threat model depicting how vulnerable IoT devices are abused as proxies to carry out financial crimes.

abused as part of botnets or proxies to launch other attacks related to financial institutions. Sometimes, compromised IoT devices can be used as an entry point to the targeted financial service to execute financial crimes. There are many possible threat scenarios where IoT devices can be compromised and abused as a part of the criminal infrastructure.

This paper discusses a threat scenario in which attackers can abuse vulnerable IoT devices to perform different attacks. Plenty of users set the same password in different accounts, including IoT devices, and that can be compromised easily by brute force and credential stuffing. Compromised IoT devices have been used as bots and malware carriers to launch attacks. Furthermore, IoT devices are abused as proxies for financial crime, as depicted in Fig. 2.

Initially, attackers look for exposed IoT devices and their vulnerabilities. Once device vulnerabilities are discovered, they look for ways to compromise and exploit those vulnerable IoT devices. Compromised IoT devices are abused as proxies to hide criminals' identities, including IP addresses and locations, so the attackers' IP addresses won't get banned from security solutions, and they can carry out attacks without being caught by authorities. The Mirai-based bot "OMG" can convert IoT devices into proxies [30].

Compromised IoT proxies are being listed for sale on the Cyber Threat Intelligence (CTI) sources [31] such as darknet markets, underground forums, Telegram channels, discords, and proxy provider websites. Experienced attackers leverage proxy scrapers and crawlers to collect IoT proxies from CTI sources and other proxy provider websites. IoT proxies are on sale, usually in virtual currencies or shared as data leaks in the CTI sources. Once attackers acquire those proxies, they abuse proxies along with cybercrime toolkits like bots, configs, and combos to carry out attacks.

Attackers usually deploy attacking software like OpenBullet, which is an easy-to-configure attack toolkit. OpenBullet, equipped with configs, can execute automated attacks by loading proxies, bots, and combos in this software, enabling even less technical attackers for successful cybercrime. Notable threats that impact financial institutions are credential stuffing, identity theft, illegal money transfers, stealing money/cryptocurrencies, and illegal trading.

Threat model can be mathematically represented as below: Let:

- S represent the set of IoT devices, where S_j denotes a specific IoT device in S .
- T be the set of threats, including tools like Shodan and OpenBullet, etc.
- A represents the set of possible attacks.
- Cr encompasses criminal activities such as identity theft, credential stuffing, and illegal money transfers.
- M denote mitigation strategies.

Define:

$$V(S_j, T) = \begin{cases} 1 & \text{if device } S_j \text{ is vulnerable to threat } T \\ 0 & \text{otherwise} \end{cases}$$

$$C(S_j) = \begin{cases} 1 & \text{if device } S_j \text{ is compromised} \\ 0 & \text{otherwise} \end{cases}$$

$$P(S_j) = \begin{cases} 1 & \text{if device } S_j \text{ is used as a proxy} \\ 0 & \text{otherwise} \end{cases}$$

$$X(S_j, A) = \begin{cases} 1 & \text{if attack } A \text{ is carried out using device } S_j \\ 0 & \text{otherwise} \end{cases}$$

Mitigation strategies M aims to reduce the risk and decision rules $R: S \times T \rightarrow M$ determines which mitigation strategies are applied based on detected vulnerabilities or threats.

IV. THE PROPOSED METHOD

In this paper, our study involves exploratory analysis of data collected from sources like CVE entries, Shodan exposure, documented research, and CTI sources, including underground forums, darknet, and Telegram channels. This data collection methodology combines a sampling strategy and a data collection framework. We deploy the same sampling strategy [32] to select major vulnerable IoT devices under study among thousands of IoT devices and vendors. The data collection framework consists of Shodan queries to collect exposed IoT devices under the categories identified by the sampling strategy, followed by the deployment of crawlers to collect evidence of IoT exploitation from the CTI sources. We deployed the data collection framework for 17 months (October 2021 to February 2023) to collect exposed IoT devices and evidence of their abuses. Additionally, we use the VARIOt dataset [33] to present the temporal status of infected IoT devices.

A. Identify Major Vulnerable Consumer IoT Devices

We have applied the sampling strategy [32], which is the intersection of three approaches (CVE, Shodan exposure, documented research) to select major vulnerable IoT devices. We have given a vulnerability base score for IoT devices if found in any approach, i.e., if a device is found in all three

approaches, it gets three times the base scores. Additionally, the quantitative value of an IoT device in each approach gets an additional score. For instance, the higher the count of CVE entries in the device category, the more additional scores are assigned. Finally, we identify major vulnerable categories of IoT devices by the higher commutative vulnerability scores they receive.

Let D be a set of all IoT device categories. Let V_{bc}, V_{bs} , and V_{br} be the vulnerability base score and V_c, V_s , and V_r represent the additional vulnerability score based on the quantitative value of IoT device categories collected from the CVE list, Shodan exposure, and documented research, respectively.

The cumulative vulnerability score, V_d for an IoT device category $d \in D$ can be calculated as:

$$V_d = (V_{bc} + V_c) \cdot I_c + (V_{bs} + V_s) \cdot I_s + (V_{br} + V_r) \cdot I_r \quad (1)$$

where I_c, I_s , and I_r are indicator functions for CVE, Shodan exposure, and documented research, respectively, such that:

$$I_c, I_s, I_r = \begin{cases} 1, & \text{if device category found in the approach} \\ 0, & \text{otherwise} \end{cases}$$

The sampling strategy combines set theory, indicator functions, and weighted scoring to identify and rank vulnerable IoT devices. The set of vulnerable IoT device categories identified (D_{select}) applying sampling strategy with regards to the broader IoT ecosystem can be expressed as:

$$D_{select} = \{x \mid x \in D \text{ and } |D_{select}| < |D|\} \quad (2)$$

The top ten vulnerable consumer IoT device categories identified by applying the sampling strategy as mentioned above are camera, router, printer, NAS storage, DVR, modem, smart TV, VOIP phone, NVR, and toaster.

The sampling approach we applied is more rational and has more representative coverage than previous approaches [2], [21], [34], [35] for the reason that we selected vulnerable IoT device types using credible sources like CVE entries, exposure from Shodan, documented research as depicted in Table II. Other literature has selected IoT devices under study either by popularity, randomly, home IoT, or industrial IoT, so they may miss more vulnerable devices while studying less vulnerable ones without considering credible sources or ignoring many potentially vulnerable exposed devices without the required selection strategy.

Since there are millions of IoT devices with thousands of categories, it becomes complex and time-consuming if we consider all IoT device categories in our study. There, we need a rational approach that can represent real-world scenarios and considers the majority of vulnerable and exposed devices susceptible to exploitation. Our sampling strategy can fulfill this purpose and be leveraged in similar studies. This sampling strategy has some limitations we also discussed in Section VII.

B. Collection of Exposed IoT Devices Using Shodan

After identifying major vulnerable IoT device categories in Section IV, we used Shodan again to collect a list of exposed IoT devices and their metadata, including IP addresses in identified categories. We use Shodan academic API and Shodan CLI to collect the dataset exposed by it for selected IoT device

TABLE II
COMPARISON OF APPROACHES TO SELECT IoT DEVICES UNDER STUDY

Reference Paper	IoT Devices categories selected for vulnerability/exploitation study	Selection Based On						Number of IoT Devices Studied
		NVD Entries	Shodan exposure	Exploitation history	Documented Research	Popularity	Random	
[2]	Webcam, Smart TV, Printer	No	Yes	No	No	Yes	No	156 K
[21]	IP Camera, DVR, Router, Printer, Home Media Server	No	No	Yes	No	Yes	No	862 K
[34]	IP Camera, NVR, IP Phone, TV Set-top Box, Kettle, Smart Lamp, Refrigerator, AC Control System	No	No	No	No	No	Yes	530 K
[35]	Webcam, Socket, Speaker, Streamer, Light Bulb, Doorbell	Yes	No	Yes	No	No	No	Not Clear
Our Paper	Camera (IP, Security, Network), Router, NAS Storage, Printer, DVR, NVR, VOIP Phone, Toaster, Smart TV, Modem	Yes	Yes	Yes	Yes	Yes	No	934 K ^a

^a Sample taken from more than 8 million IoT devices exposed by Shodan.

categories. We use Shodan queries specific to selected IoT devices. For example, to obtain a list of D-Link IP cameras that are exposed and their screenshot are available, we use the Shodan query “D-Link IP Camera has_screenshot:true”.

First, we downloaded the exposed IoT devices’ row data into JSON files for 17 months, which were later converted to CSV files. Then, those CSV files are preprocessed to remove unnecessary metadata and select only relevant features. Initially, we obtained 24 features in the dataset downloaded from Shodan. These features are data, hostnames, IP, IP_str, ipv6, org, isp, location(country_code, city, country_name, latitude, longitude), os, asn, port, tags, timestamp, transport, product, version, vulns, SSL, HTML, and title. Among these 24 features, we select only six highly relevant features primarily based on their relevance to this research and quantitatively given by correlation values. After feature extraction, the features we selected for this research are IP, product, location, timestamp, port, and vulns. Then after, we merge all CSV files while removing honeypots and duplicate data in some cases. Finally, we obtained nearly a million exposed IoT devices dataset including IP addresses for selected ten categories of IoT devices obtained from the sampling strategy discussed in Section IV.

Note that a particular IP address may be assigned to different IoT devices at different times. To verify that the exposed IP address belongs to the selected category of IoT devices, we cross-checked Shodan’s historical data. We tabulated the product and timestamp for each IoT device collected. Then, we verified all IoT IP addresses collected from Shodan with IP addresses collected from CTI sources in the same-day window.

C. Collection of Proxies From Cyber Threat Intelligence Sources

Once selected IoT devices have been collected in Section IV-B, we analyze criminal infrastructure to see whether those IoT devices have been discussed, targeted, or abused in underground communities. We deployed three crawlers on the CTI source to collect evidence of IoT abuses in financial crimes.

The IoT abuse scenario has been discussed in the threat model shown in Fig. 2 where IoT devices are abused in financial crimes by being exploited as proxies. Attackers hide behind the proxy to execute their malicious activities so security solutions and authorities can’t trace their original IP addresses and locations. Users of the Tor (The Onion Router) browser and onion channels also use proxies and VPNs to work anonymously. We collect proxies being discussed, listed as exploits, and used for financial crimes from CTI sources. We map them with IoT devices collected in Section IV-B so that IoT exploitation as proxies can be traced.

Furthermore, we started crawling through a CTI source named deepdarkCTI [31], an open-source intelligence (OSINT). It contains forums related to cyber criminal activities and data leaks, darknet markets, exploit databases, Telegram channels about data leaks and exploits, etc. DeepdarkCTI source is a reliable directory with 3.9K GitHub stars, and the directory list is updated frequently so that new onion links are added while expired onion sites are removed. Apart from deepdarkCTI, we crawled proxy provider Web links such as premsocks.com, truesocks.net, vn5socks.net, shopssocks5.com, hidemyna.me, proxynova.com, etc.

Initially, we developed two crawlers, one to list onion channels and another to crawl content within the channels leveraging the VPN, TOR browser, Python, Selenium, Firefox binary, and Pandas. For telegram channels’ scraping, we developed another crawler leveraging Telegram API and the Python library Telethon. The benefit of a crawler with Telegram API is we don’t get blocked while scraping Telegram channels. We customized our crawlers depending on the structure of the darknet, underground forums, and Telegram Channels. We encountered different anti-crawling measures like captcha, account verification, restriction of bot behavior, multi-factor authentication, crawling speed/limit, cookie expiration time, account blocking, IP address banning, etc. Accordingly, we utilized anti-crawling measures like captcha solver, manual entry when required, multiple creations of fake accounts and changing if blocked, and change of IP with TOR, VPN, and proxies, storing and reusing of session cookies as discussed in [36].

We used Python script leveraging Selenium and saved it in the Pandas DataFrame to extract the contents and proxies from clear Web proxy providers. Meanwhile, for the deep Web, we made frequent manual entries for login and verification of accounts, followed by content extraction. For the darknet, we extracted onion sites from different CTI sources, including underground forums, using simple regex and followed the crawling process to extract the desired content. Our initial CTI source, deepdarkCTI [31], has a lot of onion links, but many such onion links were not active during crawl time.

We crawled for 17 months (October 2021 to February 2023), collecting about 1.2 million proxies specifically discussed, targeted, abused, and leaked for financial crimes. We acknowledge that it was impossible to gather all proxies for free as many of them in criminal networks cannot be accessed without payment.

D. Ethical Considerations

Since this research involved cybersecurity and financial crimes, we obtained IRB approval and ensured compliance with pertinent data protection laws and obligations. To maintain ethical integrity, we collected only essential data, anonymized personal identifiers, and used secure, encrypted storage methods with restricted access. Additionally, to protect the privacy and security of the FI that we collaborated with, we concealed its identity. We presented only the data and insights FI allowed us to disclose. Furthermore, we didn't disclose personally identifiable instances from CTI sources such as IP addresses of the proxies collected, snapshots of exploits and chats related to financial crimes, seller identities, victims' details, and vendors of IoT products exploited without their approval.

V. ANALYSIS OF VULNERABILITIES AND IOT EXPLOITATION

Leveraging data collected in the previous section, we analyze IoT exploitation on a broader scale, covering different aspects such as vulnerabilities enabled by selected IoT device categories, identified IoT exploits available in the wild, and evidence of IoT exploitation we mapped with dataset crawled from the darknet and underground forums. Then, we discuss evidence of financial crimes and validate IoT exploitation with feedback from reputed FI security intelligence.

A. Vulnerabilities Reported for IoT Devices

We compile vulnerabilities enabled by selected categories of IoT devices based on the CVE entries [16], [37] as depicted in Table III. This table shows that cameras and routers are reported to have more vulnerabilities than smart TVs and printers. This indicates that cameras and routers are potentially more vulnerable, and corresponding vendors and users need additional caution to avoid their exploitation.

For example, in the NVD database, CVE-2019-11890 disclosed an issue with Sony Bravia Smart TV devices, where attackers could remotely trigger a denial of service through a SYN flood attack over LAN, whether wired or Wi-Fi. This vulnerability led to device unresponsiveness or rebooting.

TABLE III
VULNERABILITIES ENABLED BY IOT DEVICE CATEGORY [16], [37]

Device Category	Reported Vulnerabilities in CVE Entries
Router	Overflow, Execute Code, Cross-site Request Forgery (CSRF), Obtain Information, Cross-site Scripting, Denial of Service, Bypass a Restriction, Gain Privilege, Directory Traversal
Camera	Overflow, Execute Code, Obtain Information, CSRF, Denial of Service, Cross Site Scripting, Bypass a Restriction
VOIP	Execute Code, Directory Traversal, Denial of Service, CSRF, Cross Site Scripting, Bypass a Restriction
DVR	Obtain Information, Execute Code, Denial of Service, Bypass a Restriction
NAS Storage	Obtain Information, Gain Privilege, Execute Code, Bypass a Restriction
Modem	Overflow, Gain Privilege, Denial of Service, CSRF
Printer	Denial of Service, CSRF, Bypass a Restriction
TV	Denial of Service

TABLE IV
NUMBER OF IOT EXPLOITS BY DEVICE CATEGORY WITH REPORTED CVE (SOURCE: SHODAN)

Device Category	Number of IoT Exploits
Camera	98373
NAS	829
Router	539
Toaster	284
NVR	212
Printer	166
Modem	39
VOIP Phone	14
Smart TV	3
DVR	2

Likewise, CVE-2021-3616 affected Lenovo Smart Cameras X3, X5, and C2E, enabling unauthorized access to device details, modification of firmware, and device setup. This vulnerability corresponds to CNVD-2020-68651.

One of the causes of attackers targeting IoT devices is exposure to the devices. Digging a bit deeper, we explored about 5.5 million (IP, Network, and security) cameras, and 1.5 million routers were exposed by Shodan in March 2023. Another reason why IoT devices are prime targets of attackers is SSL/TLS deployment status. In March 2023, only about 22% of the selected IoT devices supported encrypted communications; about half were outdated and insecure SSL/TLS versions. We presented details of this analysis in [25].

B. IoT Exploits in the Wild

We have collected IoT exploits by two means. *First*, we leveraged the Shodan to explore specific groups of IoT devices that have already been identified as vulnerable due to associated CVEs. However, these devices are still accessible to unauthorized individuals, either because the original users are unaware of the security issues or compromised or not being monitored/updated with the latest security patches. We found over 100 K such IoT exploits, as shown in Table IV, posing threats to the IoT ecosystem and the Internet. Among those IoT exploits, about 98% are cameras, i.e., webcams, security cameras, IP cameras, and Network Cameras. *Second*, we leveraged the VARIOt dataset [33] to see the temporal

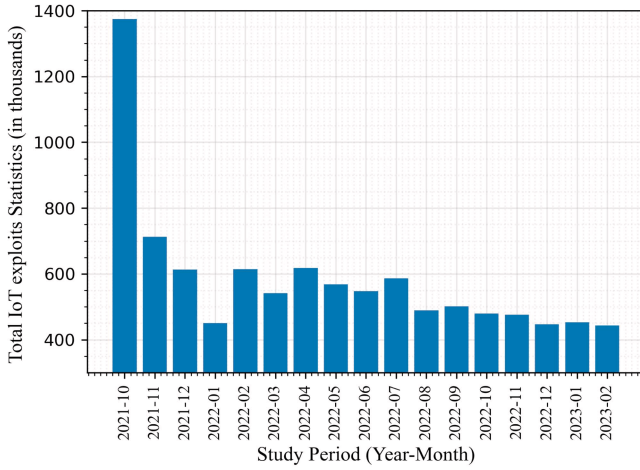


Fig. 3. Temporal status of infected IoT devices.

status of all categories of infected IoT devices during our study period. As shown in Fig. 3, the total number of infected IoT devices was about 1400K in October 2021, drastically reducing to 700K at the end of November 2021. The most possible reason for this reduction is the security updates to mass IoT devices. Then, the status of infected IoT devices is less variable and decreasing trends for the rest of the study period as depicted in Fig. 3.

C. Evidence of IoT Exploitation

Using data collected in Section IV, we explore evidence of IoT exploitation by mapping 1.2 million proxies collected in Section IV-C with nearly a million exposed IoT devices sampled in Section IV-B.

Let E be a set of exposed IoT devices extracted from Shodan queries under identified vulnerable categories by sampling strategy. It can be represented as a set of IP addresses: $E = \{\mathcal{I}_{E_1}, \mathcal{I}_{E_2}, \dots, \mathcal{I}_{E_n}\}$. Let P as a set of proxy IPs collected from cyber threat intelligence sources: $P = \{\mathcal{I}_{P_1}, \mathcal{I}_{P_2}, \dots, \mathcal{I}_{P_m}\}$. The mapping function M can be represented as a function $M: E \rightarrow P$, where $M(\mathcal{I}_{E_i}) = \mathcal{I}_{P_j}$ signifies that IoT device \mathcal{I}_{E_i} maps to proxy \mathcal{I}_{P_j} .

We obtained 1922 unique IoT proxies⁶ using the above-mentioned mapping function in selected IoT device categories. After mapping IoT proxies in the sampled dataset, we estimate IoT proxies in the total IoT population.

As per the report “State of IoT – Spring 2023” by IoT Analytics [38], there are approximately 16.5 billion connected IoT devices (14.3 billion in 2022 with an estimated growth rate of 16%). Similarly, as per the report from RiskRecon and cybersecurity research firm Cyentia Institute, the base rate for IoT devices’ exposure is 0.5% [39]. Here, the probability of IoT exposure $P(\mathcal{T}_{\mathcal{E}}) = 0.005$ and the probability of IoT not exposed is $P(\mathcal{T}_{\mathcal{N}\mathcal{E}}) = 1 - 0.005 = 0.995$.

⁶Ethical concern: We can’t reveal IoT proxy IP address and other details that violate the privacy of the users/organization. Additionally, we can’t disclose vendors or manufacturers of IoT products related to exploits found in CTI sources. We are in the process of getting approval from vendors before revealing their names.

Total IoT proxies ($\mathcal{T}_{\mathcal{P}}$) is the sum of IoT proxies in exposed IoT devices ($\mathcal{T}_{\mathcal{P}_{\mathcal{E}}}$) and IoT proxies in devices that are not exposed ($\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}}$), given by equation (3).

$$\mathcal{T}_{\mathcal{P}} = \mathcal{T}_{\mathcal{P}_{\mathcal{E}}} + \mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}} \quad (3)$$

Since we mapped about 2000 IoT proxies out of approximately 1 million exposed IoT devices, the probability of IoT proxies for exposed IoT devices is given by

$$P(\mathcal{T}_{\mathcal{P}_{\mathcal{E}}}|\mathcal{T}_{\mathcal{E}}) = \frac{\text{Sample IoT proxies}}{\text{Sample exposed IoT devices}} \approx \frac{2000}{1\text{million}} = 0.002.$$

Moreover, we found a linear relation between the number of IoT devices collected and the number of IoT proxies mapped, we can reasonably assume that the probability of IoT proxies for exposed IoT devices $P(\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}}|\mathcal{T}_{\mathcal{N}\mathcal{E}}) \approx P(\mathcal{T}_{\mathcal{P}_{\mathcal{E}}}|\mathcal{T}_{\mathcal{E}}) \approx 0.002$.

Now, we estimate the total number of IoT proxies from exposed devices ($\mathcal{T}_{\mathcal{P}_{\mathcal{E}}}$) and the total number of IoT proxies from not exposed devices ($\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}}$) using conditional probability based on Bayes theorem [40] as given by equations (4) and (5).

$$P(\mathcal{T}_{\mathcal{P}_{\mathcal{E}}}|\mathcal{T}_{\mathcal{E}}) = \frac{P(\mathcal{T}_{\mathcal{P}_{\mathcal{E}}} \cap \mathcal{T}_{\mathcal{E}})}{P(\mathcal{T}_{\mathcal{E}})} \quad (4)$$

$$P(\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}}|\mathcal{T}_{\mathcal{N}\mathcal{E}}) = \frac{P(\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}} \cap \mathcal{T}_{\mathcal{N}\mathcal{E}})}{P(\mathcal{T}_{\mathcal{N}\mathcal{E}})} \quad (5)$$

Using Eq. (5), $P(\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}} \cap \mathcal{T}_{\mathcal{N}\mathcal{E}}) = P(\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}}|\mathcal{T}_{\mathcal{N}\mathcal{E}}) \times P(\mathcal{T}_{\mathcal{N}\mathcal{E}})$, since $\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}} \subset \mathcal{T}_{\mathcal{N}\mathcal{E}}$ and $P(\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}}) = \frac{\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}}}{\mathcal{T}_{\mathcal{N}\mathcal{E}}}$, we can get

$$\mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}} = 0.002 \times 0.995 \times 16.5 \text{ Billion} = 32.835 \text{ Million.}$$

Similarly, using Eq. (4), we can get

$$\mathcal{T}_{\mathcal{P}_{\mathcal{E}}} = 0.002 \times 0.005 \times 16.5 \text{ Billion} = 165 \text{ Thousands.}$$

Thus, the total number of IoT proxies as per Eq. (3) are

$$\mathcal{T}_{\mathcal{P}} = \mathcal{T}_{\mathcal{P}_{\mathcal{E}}} + \mathcal{T}_{\mathcal{P}_{\mathcal{N}\mathcal{E}}} \approx 33 \text{ Million.}$$

Furthermore, we observe that among the IoT device categories, a higher number of cameras (including IP cameras, security cameras, network cameras, and webcams) are exposed in Shodan as well as exploited as proxies which are also supported by previous research [1], [2] and public documents [41], [42]. NAS storage is the second device exploited as proxies, followed by the router, modem, and printer.

Table V depicts the number of exposed IoT devices we collected under selected categories mapped with crawled proxies. The number of IoT proxies mapped linearly correlated with the number of IoT devices exposed by Shodan.

We further analyze IoT proxies with finer granularity by location. We found IoT proxies located in 98 countries. Among them, the top 10 countries contribute more than 50% of IoT proxies, as depicted in Fig. 4. The top ten countries with IoT proxies in descending order are Russia, Ukraine, Cambodia, Indonesia, Thailand, the United States, China, Brazil, the Czech Republic, and India.

The collected IoT proxies from CTI sources were advertised or listed on sale to abuse them as tools for different cybercrimes. Among those abuses where IoT proxies are advertised are:

TABLE V
NUMBER OF EXPOSED IoT DEVICES COLLECTED VS IoT PROXIES FOUND

Product Category	Exposed IPs Count	IoT Proxy Count
IP/Net/Security Camera	650275	1310
NAS Storage	187213	377
Router	51919	165
Modem	25243	32
Smart TV	9994	4
Printer	7472	25
Toaster	2251	5
NVR	255	1
VOIP Phone	144	3
DVR	90	0
Total	934856	1922

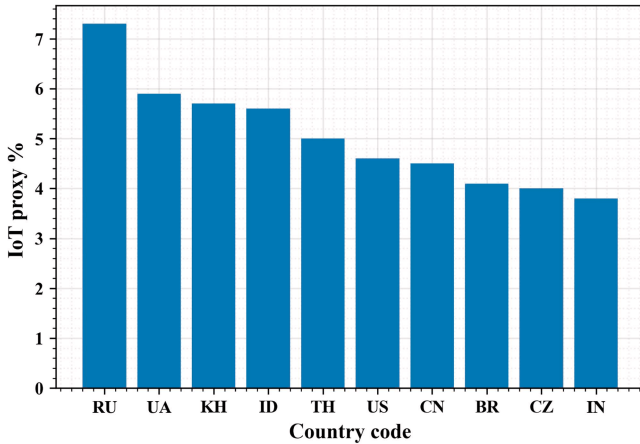


Fig. 4. IoT proxy by country.

- Avoid blocking and hiding behind IoT proxies
- Account creating and cracking
- Identity theft
- Money transferring and stealing
- Cryptocurrency mining, trading, and stealing
- Card theft and stealing
- 2FA and MFA bypassing
- Porn/adult streaming
- Credential stuffing

D. Evidence of Financial Crime

While crawling into the darknet, underground digital forums, Telegram channels, etc., we find that attackers are looking for fresh proxies since popular proxies, VPNs, and Tors can be blocked. In contrast, fresh proxies are less likely to be blocked and more cost-effective than VPNs and Tor. Due to the abundance of IoT devices with weak security postures, IoT devices are likely the main sources to provide fresh proxies.

We observed myriad instances of such IoT proxies advertised as exploits for different cyberattacks, including financial crimes such as illegal money transfer, cryptocurrency stealing, identity theft, illegal trading, and credential stuffing.⁷ Exploiting IoT proxies, attackers can log in and money transfer anonymously in financial services like banks, Venmo,

⁷Ethical concern: We are unable to disclose snapshots/chats of exploits used/listed for financial crime, sellers' identities, and victims' details due to privacy and security concern.

TABLE VI
IoT PROXIES CLASSIFIED BY THE FI'S SECURITY INTELLIGENCE

Classification	Rounded Percentage
Proxy/VNC	45
Spam	9
Malicious	1
Infrastructure	4
VOIP	1
Mail	3
SSH	1
Not Classified	36

PayPal, Western Union, and Cash App. The darknet vendors offered/advertised proxies within 50 to 80 miles of credit card owners' locations for effective credit card fraud.

Attackers also shared exploitation tutorials and financial crime success stories in underground forums, motivating others to buy exploits. In forums, attackers discuss the software designed to tunnel the Internet traffic, such as Proxifier, ProxyCap, FoxyProxy, etc., where attackers can add purchased IoT proxies, set rules to tunnel applications, and execute targeted attacks on FIs. As per the darknet advisors, attackers should not repeat Email, card number, IP address, or user agent for successful financial crime. They suggest creating a Stripe account and leveraging cex.io to transfer money from victims' credit cards to the attacker's account. To validate the evidence of IoT exploitation and financial crime discussions in CTI sources, we asked for feedback from a large financial institution, which is discussed in the following subsection.

1) *Feedback Provided by FI on the Collected Data:* In the previous section, we observed that attackers abuse IoT devices as proxies to send malicious traffic. Cameras (IP cameras, security cameras, network cameras) and NAS units are the most common IoT devices exploited as proxies, as shown in Tables IV and V.

Given these observations, two natural questions to explore are (i) What type of abuse is enabled by such proxies, and (ii) can this abuse lead to real-world harm? To dive deeper, we collaborated with a large financial institution (FI) to analyze large-scale real-world attack traffic.

In mid-2022, the FI⁸ analyzed platform traffic linked to the IP addresses we associated with the aforementioned IoT proxies. Thirty percent of the IP addresses attempted to log in to the FI's platform at least once. Of these login attempts, 64% had an IP address previously classified as risky by the FI, as detailed in Table VI. Moreover, the FI found that 32% of the IP addresses had an anomalous (high) login failure rate trying to reuse hacked passwords associated with one victim's account to another, indicating credential stuffing abuse. The distribution of the types of IoT devices that attempted logins to the FI is depicted in Fig. 5.

To augment the IP-based analysis, we also generated JA3 TLS fingerprints [43] of IP cameras and other IoT devices and shared those with the FI. Because TLS fingerprints can more uniquely identify specific devices or software libraries, they

⁸We can't disclose the name of the financial company to maintain FI's privacy and security as well as anonymity in the paper reviewing process. The FI is a U.S.-based digital financial service provider with millions of users worldwide.

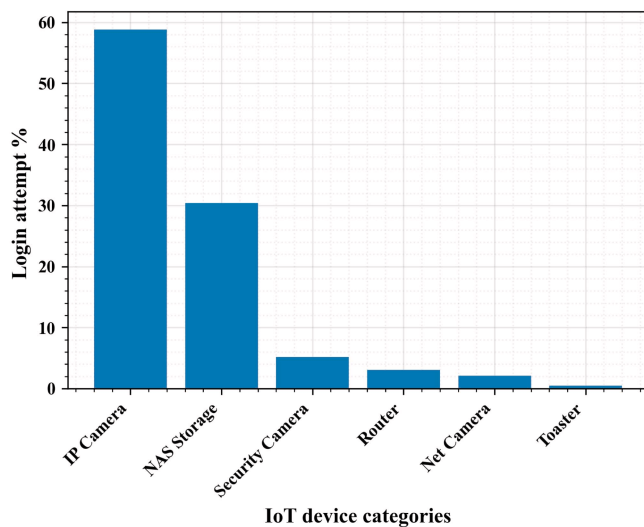


Fig. 5. IoT proxy by device category attempted to login to FI.

can serve as a more precise indicator of the corresponding abuse. The FI performed a similar analysis of its platform traffic and found that the traffic associated with several fingerprints showed anomalous access patterns compared to legitimate traffic. This resulted in high request failure rates due to action by the FI's security and risk solutions. These findings allow us to conclude with reasonably high confidence that attackers exploit IoT infrastructure by using it as proxies for credential-stuffing attacks.

Although the FI did not share any financial or account-based metrics related to its analysis due to security and privacy concerns, a credential stuffing attack aims for a criminal to validate stolen account credentials. Subsequently, using other techniques, the criminal may attempt to gain access to a victim's account fraudulently.

Proxies enable attackers to send a large volume of traffic evenly distributed across multiple IP addresses, thus reducing the likelihood that IP-based velocity checks alone would suffice for a firewall to block the attack traffic. Leveraging (proactively obtained) IP intelligence derived using techniques discussed in this paper (such as IPs associated with known vulnerable devices) and appropriately actioning traffic based on indicators such as TLS fingerprints can help better protect systems against such attacks.

VI. DISCUSSION AND SECURITY RECOMMENDATIONS

As discussed in the threat model, the initial step of IoT abuse starts with device compromise by exploiting vulnerabilities. If we minimize device compromise in the first step, we can certainly minimize cyberattacks and associated financial crime. Both FIs and consumers must remain vigilant for attack vectors related to IoT devices. Attack vectors related to most IoT devices are default passwords, firmware vulnerabilities, brute-force attacks, man-in-the-middle (MitM) attacks, phishing attacks, malware attacks, denial of services, and ransomware attacks.

All organizations, including financial institutions, should monitor their network regularly to detect vulnerabilities before exploiting them. They can also leverage tools like Shodan to

check if their IoT devices are exposed. Some indicators that IoT devices could be compromised are - performance degradation, a spike of activities, restart/shutdown unnecessarily, the battery draining faster than expected, and applications/services exposed. IoT device owners should reboot IoT devices frequently, as rebooting can help to remove malware residing in memory. Firewall rules also need to be checked regularly for the integrity of security policies. For instance, if IoT devices are exploited as proxies, firewall rules may be modified to accept proxy services like HTTP and SOCKS. Exploited/compromised nodes should be immediately isolated from the network and take required security actions.

Financial services and users are more targeted by attackers after the widespread implementation of digital/online transactions. For FI, we recommend robust RBA (Risk Based Authentication) incorporating five security layers (username, password, national ID, multi-factor authentication (MFA), and token device) coping with the country's regulations. Additionally, financial institutions should incorporate FBI recommendations of digital defense for the Internet of Things [44]. They should separate IoT networks from critical infrastructure with separate router or virtual LAN (VLAN) implementations so that attacks on weak IoT devices may not compromise the primary FI system.

The widespread distribution of IoT nodes can be utilized to fight against criminal ecosystems with integrated efforts from financial service providers and customers. FIs can harness data-driven analytic and machine learning (ML) approaches for the detection/prevention of financial crimes by collecting data from distributed IoT nodes. Furthermore, it will be result-oriented if we can combat cyber crimes while combining technologies like IoT, AI, Blockchain, and Cloud computing. Additionally, anti-financial crime tools can help reduce financial crimes.

Furthermore, suppose IoT devices and associated operating systems are found vulnerable and reported publicly in the CVE database or other vulnerable and exploited databases. In that case, FIs should immediately flag those IoT devices and restrict communication until security issues are resolved. If FI or customers find such devices within their networks, they should remove them from the network, update their firmware/security configurations, and connect only if they are secure. FIs can also deploy crawlers in criminal infrastructure to monitor the IoT devices communicated to their system. They should take necessary security action with immediate isolation if they are found. Indeed, FIs can deploy automated device identification scripts or tools to identify and block vulnerable and exploited IoT devices on the fly so that other devices in the network can communicate safely.

In addition to the security recommendations mentioned above, we present security suggestions tailored to IoT-related vulnerability and exploitation as below:

- 1) *Credential stuffing* can be prevented with a unique password and multifactor authentication (MFA) by requiring users to authenticate using multiple methods, like passwords and biometrics. This multi-layered approach makes it tough for attackers to gain unauthorized access, even with the right password.

- 2) *Identity theft* can be reduced by using a strong password for each account combined with MFA and regularly monitoring financial accounts and credit reports.
- 3) *Illegal money transfers* can be minimized by ensuring strict adherence to regulatory compliance standards for IoT device usage and by implementing robust transaction monitoring systems that analyze patterns and anomalies in financial data.
- 4) *Cryptocurrency stealing* can be reduced by storing digital assets in secure, offline hardware wallets and by practicing strict cybersecurity measures such as using unique, complex passwords and enabling multi-factor authentication on all accounts.
- 5) *Illegal trading* can be minimized by implementing encryption protocols and access controls to secure trading platforms and data transmissions.

The research findings highlight important implications for policymakers, businesses, and cybersecurity experts. First, policymakers should focus on creating rules that enforce strong security standards for IoT devices. This means ensuring companies update their devices and share information about security issues. It's also important for policymakers to invest in research to better understand and address new threats. Businesses, especially those making IoT devices, must prioritize security at every stage of a product's life. They can also collaborate through industry groups to share knowledge and best practices. Cybersecurity experts must keep a close watch on threats and use strong security measures to protect against vulnerabilities in IoT devices. Lastly, consumers must know the risks and make smart choices when buying and using IoT devices. Working together can make IoT devices safer and better protect against cyberattacks and financial crimes.

VII. LIMITATIONS AND FUTURE PROSPECTS

The limitations associated with our study are:

Sampling strategy: Our sampling approach is not exhaustive since we use only three selection criteria (Shodan exposure, CVE entries, and documented articles) as described in [32] to identify vulnerable IoT devices. We can improve the sampling strategy by adding more selection criteria such as vulnerable components and software like System-on-chip (SOC), Wi-Fi modules, OSs and their versions, firmware, TCP/IP stacks, etc.

Scales of study: We studied ten major vulnerable IoT device categories selected by sampling strategy. We can increase the scale of the study by increasing the categories of IoT devices.

Analysis of criminal infrastructure: Coping with research ethics and Institutional Review Board (IRB) approval guidance, we have not made any direct connections/communications to cyber criminals. So, there might be some missing in the analysis of criminal infrastructure.

Our study also lacks first-hand vulnerability assessment of IoT devices in the physical environment using vulnerability assessment tools like Nessus. Additionally, we didn't assess the vulnerability of IoT infrastructures based on packet manipulation.

Open future research problems in IoT security are:

- Empirical study of IoT devices in the lab to assess the vulnerability types and generate a unique IoT dataset that

can be utilized later to model and evaluate the current IoT threat landscape.

- Mass scanning of vulnerable IoT infrastructure over the Internet with pre-approval from regulatory authorities, vendors, and device owners. Moreover, this approach needs high processing capacity, storage size, and time.
- Vulnerability analysis with packet manipulation based on packet manipulation at layer two and layer 3.
- *AI/ML for predictive analysis of IoT infrastructure:* We can leverage ML to conduct predictive analysis on historical data related to IoT vulnerable infrastructure, something similar to [45] in large scale. Moreover, studies to improve the defense system focusing on financial crimes can be carried out similar to the impactful study on multi-layer IoT-DDoS [46].

VIII. CONCLUSION

In this paper, we identified the major vulnerable IoT device categories, investigated the vulnerabilities enabled by those selected categories, and collected evidence of abuses of those devices by attackers. We mapped the IoT device categories exposed by Shodan with proxies crawled from the darknet, underground forums, and Telegram channels for 17 months (October 2021 to February 2023). We estimated that about 33 million IoT devices are exploited as proxies based on IoT proxy mapped from sample IoT devices exposed by Shodan. We found that cameras and NAS storage are the most abused IoT devices among the identified IoT device categories. Additionally, we found that only ten countries host most of the identified IoT proxies.

We validated the activities of discovered IoT proxies with feedback from a reputed financial institution. FI found that most of those proxies were already flagged as bad based on their interactions with financial systems. However, they were not aware of their device types. In addition, based on the insights provided by FI regarding multiple failed login attempts from IoT proxies, we can confidently conclude that attackers are exploiting these devices for credential-stuffing attacks. Ultimately, we present security recommendations to financial institutions and consumers to reduce IoT-related financial crimes.

ACKNOWLEDGMENT

However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies.

REFERENCES

- [1] D. Kumar et al., "All things considered: An analysis of IoT devices on home networks," in *Proc. 28th USENIX Secur. Symp. (USENIX Secur.)*, 2019, pp. 1169–1185.
- [2] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach," in *Proc. IEEE Int. Conf. Intell. Security Inform. (ISI)*, 2017, pp. 179–181.

- [3] M. Bada and I. Pete, "An exploration of the Cybercrime ecosystem around Shodan," in *Proc. 7th Int. Conf. Internet Things Syst., Manag. Security*, 2020, pp. 1–8.
- [4] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020.
- [5] S. Devarakonda, M. N. Halgamuge, and A. Mohammad, "Critical issues in the invasion of the Internet of Things (IoT): Security, privacy, and other vulnerabilities," in *Research Anthology on Privatizing and Securing Data*. Hershey, PA, USA: IGI Glob., 2021, pp. 1672–1694.
- [6] S. Hilt et al., *The Internet of Things in the Cybercrime Underground*. Trend Micro Res., Tokyo, Japan, 2019.
- [7] M. Campobasso and L. Allodi, "Impersonation-as-a-service: Characterizing the emerging criminal infrastructure for user impersonation at scale," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2020, pp. 1665–1680.
- [8] A. Mirian, J. DeBlasio, S. Savage, G. M. Voelker, and K. Thomas, "Hack for hire: Exploring the emerging market for account hijacking," in *Proc. World Wide Web Conf.*, 2019, pp. 1279–1289.
- [9] M. Wazzan, D. Algazzawi, O. Bamasqa, A. Albeshri, and L. Cheng, "Internet of Things botnet detection approaches: Analysis and recommendations for future research," *Appl. Sci.*, vol. 11, no. 12, p. 5713, 2021.
- [10] "Focus: Banks and cyber security." Accessed: Jan. 18, 2024. [Online]. Available: <https://cba.ca/banks-and-cyber-security>
- [11] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, protocols, and applications," *J. Elect. Comput. Eng.*, vol. 2017, no. 1, 2017, Art. no. 9324035.
- [12] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, 2010, pp. 484–487.
- [13] K. Chen et al., "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," *J. Hardw. Syst. Secur.*, vol. 2, no. 2, pp. 97–110, 2018.
- [14] M. B. M. Noor, and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.
- [15] "OWASP Internet of Things project." 2018. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10
- [16] (Nat. Inst. Stand. Technol. Gov. Agency, Gaithersburg, MD, USA). *National Vulnerability Database*. (2020). [Online]. Available: <https://nvd.nist.gov/vuln/search>
- [17] "Operational risk management in financial services | ORX." Accessed: Mar. 15, 2024. [Online]. Available: <https://managingriskstogether.orx.org/>
- [18] A. Alazab, J. Abawajy, M. Hobbs, R. Layton, and A. Khraisat, "Crime toolkits: The productisation of cybercrime," in *Proc. 12th IEEE Int. Conf. Trust, Security Privacy Comput. Commun.*, 2013, pp. 1626–1632.
- [19] Forescout Technol. Softw. Co., San Jose, CA, USA). *AMNESIA:33 Identify and Mitigate the Risk From Vulnerabilities Lurking in Millions of IoT, OT and IT Device*. (2020). [Online]. Available: <https://www.forescout.com/research-labs/amnesia33/>
- [20] J. M. Blythe and S. D. Johnson, "A systematic review of crime facilitated by the consumer Internet of Things," *Secur. J.*, vol. 34, pp. 97–125, Mar. 2021.
- [21] M. Galluscio et al., "A first empirical look on Internet-scale exploitations of IoT devices," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, 2017, pp. 1–7.
- [22] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, 2018.
- [23] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, "Open for hire: Attack trends and misconfiguration pitfalls of IoT devices," in *Proc. 21st ACM Internet Meas. Conf.*, 2021, pp. 195–215.
- [24] E. Ulqinaku, D. Lain, and S. Capkun, "2FA-PP: 2nd factor phishing prevention," in *Proc. 12th Conf. Security Privacy Wireless Mobile Netw.*, 2019, pp. 60–70.
- [25] Y. R. Siwakoti and D. B. Rawat, "Investigating security vulnerability related to exposure and TLS ecosystem in IoT devices," in *Proc. IEEE 24th Int. Conf. Inf. Reuse Integr. Data Sci. (IRI)*, 2023, pp. 7–12.
- [26] I. Gulatas, H. H. Kilinc, A. H. Zaim, and M. A. Aydin, "Malware threat on edge/fog computing environments from Internet of Things devices perspective," *IEEE Access*, vol. 11, pp. 33584–33606, 2023.
- [27] A. Affinito, S. Zinno, G. Stanco, A. Botta, and G. Ventre, "The evolution of Mirai botnet scans over a six-year period," *J. Inf. Secur. Appl.*, vol. 79, Dec. 2023, Art. no. 103629.
- [28] M. Asam et al., "IoT malware detection architecture using a novel channel boosted and squeezed CNN," *Sci. Rep.*, vol. 12, no. 1, 2022, Art. no. 15498.
- [29] J. Choi, A. Anwar, H. Alasmary, J. Spaulding, D. Nyang, and A. Mohaisen, "IoT malware ecosystem in the wild: A glimpse into analysis and exposures," in *Proc. 4th ACM/IEEE Symp. Edge Comput.*, 2019, pp. 413–418.
- [30] (Fortinet Cybersec. Co., Sunnyvale, CA, USA). *OMG: Mirai-Based Bot Turns IoT Devices Into Proxy Servers*. (2018). [Online]. Available: <https://www.fortinet.com/blog/threat-research/omg-mirai-based-bot-turns-iot-devices-into-proxy-servers>
- [31] "GitHub—Fastfire/deepdarkCTI: Collection of cyber threat intelligence sources from the deep and dark Web." Accessed: May 19, 2024. [Online]. Available: <https://github.com/fastfire/deepdarkCTI>
- [32] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. C. Johnson, "Advances in IoT security: Vulnerabilities, enabled criminal services, attacks, and countermeasures," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11224–11239, Jul. 2023.
- [33] "Infected and exposed IoT device statistics—Data Europa EU," Dataset. Accessed: May 20, 2024. [Online]. Available: <https://data.europa.eu/data/datasets/infected-and-exposed-iot-device-statistics?locale=en>
- [34] A. Iskhakova, R. Meshcheryakov, A. Iskhakov, and S. Timchenko, "Analysis of the vulnerabilities of the embedded information systems of IoT-devices through the honeypot network implementation," in *Proc. 4th Int. Res. Conf. Inf. Technol. Sci., Manag., Soc. Sphere Med. (ITSMSM)*, 2017, pp. 363–367.
- [35] Y. Meidan, V. Sachidananda, H. Peng, R. Sagron, Y. Elovici, and A. Shabtai, "A novel approach for detecting vulnerable IoT devices connected behind a home NAT," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101968.
- [36] K. Turck, S. Pastrana, and B. Collier, "A tight scrape: Methodological approaches to cybercrime research data collection in adversarial environments," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS & PW)*, 2020, pp. 428–437.
- [37] "Vulnerability distribution of CVE security vulnerabilities by types." Accessed: May 19, 2024. [Online]. Available: <https://www.cvedetails.com/vulnerabilities-by-types.php>
- [38] "Number of connected IoT devices growing 13% to 18.8 billion globally." Accessed: May 19, 2024. [Online]. Available: <https://iot-analytics.com/number-connected-iot-devices/>
- [39] "Study of IoT devices | RiskRecon." Accessed: Jan. 15, 2024. [Online]. Available: <https://www.riskrecon.com/iot-device-study>
- [40] J. Joyce. "Bayes' theorem." 2003. [Online]. Available: <https://seop.illc.uva.nl/entries/bayes-theorem/>
- [41] "The biggest Internet of Things, smart home hacks of 2019 | ZDNet." 2019. [Online]. Available: <https://www.zdnet.com/pictures/the-biggest-internet-of-things-smart-home-hacks-over-2019/>
- [42] "Millions of connected cameras open to eavesdropping | Threatpost." Accessed: May 20, 2024. [Online]. Available: <https://threatpost.com/millions-connected-cameras-eavesdropping/166950/>
- [43] "GitHub—Salesforce/JA3: JA3 is a standard for creating SSL client fingerprints in an easy to produce and shareable way." Accessed: May 20, 2024. [Online]. Available: <https://github.com/salesforce/ja3>
- [44] (FBI, Washington, DC, USA). *Tech Tuesday: Internet of Things (IoT)*. Accessed: May 18, 2024. [Online]. Available: <https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot>
- [45] Y. R. Siwakoti and D. B. Rawat, "Detect-IoT: A comparative analysis of machine learning algorithms for detecting compromised IoT devices," in *Proc. 24th Int. Symp. Theory, Algorithmic Found., Protocol Design Mobile Netw. Mobile Comput.*, 2023, pp. 370–375.
- [46] Y. Liu, K.-F. Tsang, C. K. Wu, Y. Wei, H. Wang, and H. Zhu, "IEEE P2668-compliant multi-layer IoT-DDoS defense system using deep reinforcement learning," *IEEE Trans. Consum. Electron.*, vol. 69, no. 1, pp. 49–64, Feb. 2023.