Data-driven Curation, Learning and Analysis for Inferring Evolving IoT Botnets in the Wild

Morteza Safaei Pour  
Antonio Mangino  
Cyber Threat Intelligence Laboratory  
Florida Atlantic University

Kurt Friday  
Matthias Rathbun  
Elias Bou-Harb  
Cyber Threat Intelligence Laboratory  
Florida Atlantic University

Farkhund Iqbal  
College of Technological Innovation  
Zayed University

Khaled Shaban  
Abdelkarim Erradi  
Department of Computer Science and Engineering  
Qatar University

ABSTRACT
The insecurity of the Internet-of-Things (IoT) paradigm continues to wreak havoc in consumer and critical infrastructure realms. Several challenges impede addressing IoT security at large, including, the lack of IoT-centric data that can be collected, analyzed and correlated, due to the highly heterogeneous nature of such devices and their widespread deployments in Internet-wide environments. To this end, this paper explores macroscopic, passive empirical data to shed light on this evolving threat phenomena. This not only aims at classifying and inferring Internet-scale compromised IoT devices by solely observing such one-way network traffic, but also endeavors to uncover, track and report on orchestrated “in the wild” IoT botnets. Initially, to prepare the effective utilization of such data, a novel probabilistic model is designed and developed to cleanse such traffic from noise samples (i.e., misconfiguration traffic). Subsequently, several shallow and deep learning models are evaluated to ultimately design and develop a multi-window convolution neural network trained on active and passive measurements to accurately identify compromised IoT devices. Consequently, to infer orchestrated and unsolicited activities that have been generated by well-coordinated IoT botnets, hierarchical agglomerative clustering is deployed by scrutinizing a set of innovative and efficient network feature sets. By analyzing 3.6 TB of recent darknet traffic, the proposed approach uncovers a momentous 440,000 compromised IoT devices and generates evidence-based artifacts related to 350 IoT botnets. While some of these detected botnets refer to previously documented campaigns such as the Hide and Seek, Hajime and Fbot, other events illustrate evolving threats such as those with cryptojacking capabilities and those that are targeting industrial control system communication and control services.

KEYWORDS
Internet-of-Things, IoT botnets, network security, network telescopes, Internet measurements, deep learning

ACM Reference Format:

1 INTRODUCTION
With the escalating adoption of the Internet-of-Things (IoT) paradigm in numerous realms such as critical infrastructure, home networks [2], transportation [11], and various others [8], an increasing number of devices are becoming directly Internet-facing. Although IoT devices can be deployed behind NAT gateways, a plethora of such devices are indeed directly connected to the Internet and/or employ port-forwarding for proper and simplified provisioning and management [16]. Such devices, unfortunately, continue to lack basic security protocols and measures, rendering them easy targets for exploitations and hence recruitment within coordinated IoT botnets [7]. Furthermore, there exists several IoT inherent factors such as their heterogeneous nature and limited processing resources, which further complicate addressing their security requirements. Additionally, despite much attention to IoT in the security community [25, 36, 41], subpar attention is being paid to IoT security aspects by their manufacturers and users, on top of an overwhelming lack of maturity of IoT-specific update procedures for patch management.

In this context, the broad topic of IoT security has been a particular area of focus in the security community after it was revealed that Mirai [5], via infecting more than 200,000 devices, was behind the debilitating Distributed Denial of Service (DDoS) attacks of late 2016 - a direct result of such deficiencies. Indeed, this event demonstrated the sheer capabilities for maliciousness by way of instrumenting exploitable IoT devices. Moreover, the IoT botnet environment has been evolving and expanding to include several more players who ultimately compete for control of IoT devices by means of newly-disclosed vulnerabilities. In order to supersede the opposition, the removal of any existing malware on the given device is now amongst the attackers’ objectives. Additionally, such IoT-centric malware will additionally kill running services [5, 29] and...
can perform checks to evade honeypots [35, 54]. Further exacerbating the situation, an unfortunate by-product of this competition is the promotion of even more sophisticated methods of exploitation—versus that of the first generation of Mirai. These novel adversarial approaches frequently result in the exposure of ports and services other than that of Telnet [32], the most common attack vector associated within IoT. All-in-all, this race between adversaries ultimately leads to an extremely dynamic behavior which makes the tasks of inferring and attributing compromised IoT devices and their coordinated illicit activities incredibly daunting.

Moreover, acquiring IoT-centric empirical data to be curated and analyzed for maliciousness is problematic, given the large-scale deployments of such devices in Internet-wide realms. Broadly, a major challenge related to the inference of IoT botnets through the analysis of network traffic is the lack of sound data-driven artifacts to assert that the perceived activities are actually originating from IoT devices and not typical machines. One solution would be to correlate such inferred probing IP addresses with databases gathered by services such as Shodan [48] and/or Censys [49], which collect and index information pertaining to IoT devices via IP crawlers, active scanning based on open ports and available services, and banner grabbing. At the same time, while doing so provides large-scale and valuable information regarding Internet-facing IoT devices, the set of those identified is indeed incomplete. This issue is in large part due to the scope of said services being limited to only the devices that are reachable by their scanners; a vast number of the targeted services and ports end up filtered out by firewalls. Moreover, upon infection, IoT malware typically blocks ports and disables common outward facing services (i.e., Telnet, CWMP, ADB, etc.) [5, 29] or modify the banners, which further impedes the indexing of all the inferred IoT devices. To this end, it becomes highly desirable to employ learning techniques for predicting (i.e., fingerprinting) the device types of previously unknown IoT sources.

In light of the aforementioned information, in this work, we explore passive measurements rendered by analyzing darknet data (i.e., Internet-scale traffic targeting routable yet unused IP address) to shed light on the insecurity of the IoT paradigm at large. Additionally, to motivate empirical (and operational) IoT cyber security initiatives as well as aid in reproducibility of the obtained results, we employ learning techniques for predicting (i.e., fingerprinting) the infection, IoT malware typically blocks ports and disables common services and ports end up filtered out by firewalls. Moreover, upon infection, IoT malware typically blocks ports and disables common outward facing services (i.e., Telnet, CWMP, ADB, etc.) [5, 29] or modify the banners, which further impedes the indexing of all the inferred IoT devices. To this end, it becomes highly desirable to employ learning techniques for predicting (i.e., fingerprinting) the device types of previously unknown IoT sources.

In this section, we elaborate on three topics central to the contemporary IoT security landscape. The first point of emphasis focuses on network telescopes as powerful mechanisms to capture IoT-specific, illicit network traffic. The second of which encompasses efforts pertaining to IoT device fingerprinting and the detection of compromised IoT devices. Finally, we enumerate the literature related to IoT-specific botnet analysis.

**Network telescopes.** A network telescope, or a darknet, is a set of deployed, routable, allocated, yet unused IP addresses to passively observe incoming Internet-scale traffic [23]. Given that these IP addresses are not associated with any services, traffic targeting them is thereby deemed as unsolicited [10]; originating from infected devices, victims of denial of service attacks, or misconfiguration. Network telescopes have been recurrently proven to be credible sources for the investigation of large-scale, Internet-wide activities such as that of probing [9, 17] and DDoS attacks [22, 34].

In a recent study [40], the authors revealed more than 120,000 Internet-scale exploited IoT devices, by correlating darknet traffic and Shodan databases to investigate IoT probing campaigns. Further, Torabi et al. [53] conducted large-scale correlations between passive measurements and IoT-relevant information to investigate and disclose malicious activities associated with more than 26,000 IoT devices. Moreover, by means of applying filters to network telescope data in order to discern Mirai-relevant traffic, Antonakakis et al. [5] were able to gather IoT-related information pertaining to roughly 1.2 million Mirai-infected IP addresses during 7 months, in addition to examining their associated detection-avoidance techniques. Cetin et al. [12] conducted empirical studies on IoT malware cleanup efforts and remediation rates in a medium-sized Internet Service Provider (ISP) leveraging darknet and honeypot sources.

The remainder of this paper is organized as follows. In the next section, we review the literature to demonstrate the state-of-the-art contributions of this work. In Section 3, we detail the darknet pre-processing model, the studied machine/deep learning models for fingerprinting compromised IoT devices, in addition to elaborating on the IoT-centric botnet inference methodology. Further, in Section 4, we execute and evaluate the proposed approach to report on its results and discuss the obtained findings. Finally, Section 5 summarizes the contributions of this paper, discusses a few limitations and pinpoints several topics which pave the way for future work.
While such contributions are noteworthy, several shortcomings can be noted. First, such works rely on a specific IoT malware signature (i.e., tcpSeq == dstIP) which indeed can not provide a comprehensive identification of all IoT bots since many do not follow this signature; our measurements have revealed that less than 25% of all the inferred IoT bots match this specific signature. Second, the majority of these and related works solely depend on databases gathered by Internet scanning services, which miss a large portion of the actual IoT bot population. In contrast, we propose herein an approach consisting of active and passive measurements, coupled with machine/deep learning techniques, which leads to a more comprehensive view of the IoT bots’ populations.

**IoT device fingerprinting.** The vast majority of IoT inference methods utilized in previous works rely on text information in gathered banners and leverage regular expressions to find specific patterns, or using text summarization methods [47] as input to classifiers [2]. In turn, several research efforts have alternatively elected to attempt IoT device fingerprinting by observing network traffic. For instance, Meidan et al. [31] manually labeled network traffic generated by IoT devices and employed a supervised learning algorithm to classify IoT devices for a given organization’s network. Moreover, Miettinen et al. [33] leveraged network traffic generated by IoT devices during their setup process for capturing device-specific traits, and subsequently mapped these signatures to the device type by way of random forest classification. Thangavelu et al. [51] also leveraged machine learning in order to classify types of IoT devices, but managed to also do so with that not presented in the training set. With that being said, one shortcoming of the aforementioned procedures is that their scope is limited to local IoT networks and thus do not present an Internet-wide perspective. Further, their proposed techniques are not applicable on one-way scan flows arriving at network telescopes. Additionally, in contrast, we present a deep learning approach to distinguish compromised IoT devices from infected multi-purpose systems using features in sequences of TCP SYN packets.

**IoT botnet analysis.** Within the context of botnet analysis through tailored honeypots, Pa et al. [37] were able to infer several malware families by constructing a honeypot for the purpose of analyzing attacks against Telnet services. Furthermore, Guarnizo et al. [28] designed the IoT-centric Scalable high-Interaction Honeypot (SIPHON) which showed an ability to attract a tremendous amount of malicious IoT botnet-generated traffic through a combination of worldwide wormholes and a small number of IoT devices. Moreover, Metongnon and Sadre [32] have recently reported on a large portion of the actual IoT bot population. In contrast, we propose herein an approach consisting of active and passive measurements, coupled with machine/deep learning techniques, which leads to a more comprehensive view of the IoT bots’ populations.

3 PROPOSED METHODOLOGY

This section details the proposed approach as depicted in Figure 1. Its core components include (i) data collection and dataset preparation, which entails preprocessing, introduces the darknet sanitization probabilistic model to filter out misconfiguration traffic along with the inference of Internet-scale probing activities and labeling their sources; (ii) the utilization of a deep learning binary classifier for fingerprinting compromised IoT devices; and (iii) the feature engineering process coupled with executing hierarchical agglomerative clustering to infer and report on IoT botnets. These steps are subsequently detailed.

3.1 Network telescope sanitization model

Although network telescope (darknet) data predominantly consists of malicious packets originating from probes, backscattered packets from victims of distributed denial of service attacks, and malware propagation attempts, it might also contain what is dubbed as misconfiguration traffic. The latter non-malicious packets frequently result from network/routing or hardware/software faults that were erroneously directed towards a darknet. Another prospect is it being an artifact of improper configuration during darknet deployment. Indeed, misconfiguration traffic impedes the proper functioning of cyber threat intelligence algorithms operating on darknet data, which often yields numerous undesirable false positives and false negatives. Additionally, its excessive existence is a sheer waste of valuable storage resources. As a result, given the lack of formalism in addressing this problem, the objective herein is to elaborate on a probabilistic model that is specifically tailored towards the preprocessing of darknet data by way of fingerprinting, and in turn, filtering out embedded misconfiguration traffic.

In a nutshell, the model formulates and computes two metrics, with dependencies associated with typical network flows, the model initially estimates the rareness of access of the destination. Secondly, to ensure the inclusion of the unique characteristics of the given flow as well, the scope of access is considered, which accounts for the number of distinct darknet IP addresses that a specific remote source has accessed. Subsequently, the joint probability is formulated, computed, and compared. If the probability of the source generating a
misconfiguration flow is higher than that of the source being malicious (or unsolicited), then that particular source is deemed to be generating misconfiguration traffic, flagged, and the corresponding flows are filtered out. In the following, we detail the notions of both rarity and scope of access.

Let \( D = \{d_1, d_2, d_3, \cdots \} \) represent the set of darknet IP addresses, with \( D_i \) being a subset of those accessed by source \( s_i \). First, the model captures how unusual these accessed destinations are. The underlying idea in doing so stems from the fact that misconfigured sources target destinations seldom called upon by others [26]. Thus, the model estimates the distribution of a darknet IP \( d_i \) as being accessed by such a source as

\[
P_{\text{misc}}(d_i) = \frac{n_s(d_i)}{\sum_{d_j \in D} n_s(d_j)},
\]

where \( n_s(d_i) \) is the number of sources that have accessed \( d_i \); in contrast, a malicious darknet source will target a given destination at random. Typically, defining a suitable probability distribution to exemplify the randomness of a malicious source taking aim at a specific darknet destination is quite tedious; therefore, a simplistic assumption is often applied to resolve this potential headache. In this context, Durumeric et al. [19] demonstrated that sources probe their darknet targets following a Gaussian distribution. By adopting that assumption, one can model the probability of a darknet destination being accessed by a malicious source as

\[
P_{\text{mal}}(d_i) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x_{d_i} - \mu)^2}{2\sigma^2}}
\]

where \( \sigma \) is the standard deviation, \( \mu \) is the mean, \( \sigma^2 \) is the variance, and \( x \) is the location of the darknet destination following the aforementioned distribution. Recall that not only does the model capture how unusual the accessed destinations are, but it also considers the number of darknet destinations accessed by a particular source, which we subsequently describe. Given a set of \( D_i \) darknet destinations accessed by a specific source \( s_i \), the model ultimately measures two probability distributions, namely, \( P_{\text{misc}}(D_i) \) and \( P_{\text{mal}}(D_i) \), the former being the probability that \( D_i \) has been generated by a misconfigured source and the latter originating from that with a malicious intent towards darknet \( D_i \). For example, if the darknet addresses accessed by \( s_i \) are \( D_i = \{d_{i1}, d_{i2}, d_{i3} \} \), \( P(D_i) \) equates to the probability of \( s_i \) accessing the specific combination of addresses \( \{d_{i1}, d_{i2}, d_{i3} \} \) given three targeted destinations, multiplied by the probability of \( s_i \) accessing any three destinations. In turn, we can generalize \( P(D_i) \) as

\[
P(D_i) = P(D_i = \{d_{i1}, d_{i2}, \cdots, d_{in} \} | |D_i| = n) \times P(|D_i| = n).
\]

For both a misconfigured and malicious source, the first term of equation (2) can be modeled as

\[
P(D_i) = \frac{1}{K} \prod_{d_j \in D_i} P(d_j)
\]

where \( K \), acting as a normalization constant and solely being used as a means of summing the probabilities to 1, could be defined as \( K = \frac{|D_i|!}{\prod_{d_j \in D_i} |d_j|!} \). Please note that \( K \) is a standard normalization constant that is often employed in Bayesian probability [27].

Moreover, \( n \) encompasses all sources in the data set, whereas \( |D_i| \), as previously mentioned, represents the darknet IP space. Consequently, the likelihood that a source will target a certain number of darknet destinations (i.e., the second term of equation (2)) depends upon whether it is malicious or misconfigured. Characteristically, misconfigured sources access one or few destinations while those with malicious intent target a larger pool. In accordance, we have modeled such distributions as

\[
P_{\text{misc}}(|D_i|) = \frac{1}{(e - 1)|D_i|!}
\]

\[
P_{\text{mal}}(|D_i|) = \frac{1}{|D_i|!}
\]

where the term \((e - 1)\) in equation (4) ensures the distribution’s summing equates to 1. It should also be noted that equation (4) guarantees a significant decrease in the probability as the number of targeted destinations increases. In contrast, equation (5) captures that of a random number of darknet addresses being accessed by a malicious source. Thereby, via plugging in of equations (4) and (5) into (3), respectively, we can represent the probability of a source being either misconfigured or malicious, given a set of darknet destination addresses, as

\[
P_{\text{misc}}(D_i) = \frac{1}{K(e - 1)|D_i|!} \prod_{d_j \in D_i} P_{\text{misc}}(d_j)
\]

\[
P_{\text{mal}}(D_i) = \frac{1}{K|D_i|!} \prod_{d_j \in D_i} P_{\text{mal}}(d_j).
\]

It is imperative to observe that equations (6) and (7) provide two distinct likelihood models to distinguish between misconfiguration and malicious, darknet-bound traffic, which enables their simplified and systematic post-processing. As the proposed model generalizes and formalizes the concepts of misconfiguration and malicious darknet traffic, it does not make any assumptions regarding the nature of the sources from which the given types of traffic are originating. Thus, the method deems a source and its corresponding flows as misconfiguration traffic if \( \ln P_{\text{misc}}(D_i) - \ln P_{\text{mal}}(D_i) > 0 \).

Indeed, given that the field of Internet measurements for cyber security heavily relies on processing network telescope data, we make the code available in the mentioned repository to the research and operations communities at large.

### 3.2 Data collection and dataset preparation

#### 3.2.1 Inferring probing activities

After the sanitization of the misconfiguration traffic by leveraging the aforementioned pre-processing model, the objective herein is to dissect the malicious traffic to extract probing flows as indicators of exploitation. This is achieved through a Threshold Random Walk (TRW)-based probing detection algorithm [39]. Essentially, the algorithm looks for subsequent packets from the same source IP address for a duration of 300 seconds; if a threshold is reached prior to the packet’s arrival, the given counter is reset. If, on the other hand, the threshold has held and the duration has not expired, the counter will be incremented. If the counter reaches a threshold of 64 [46], the flow would be deemed as a probing event.

#### 3.2.2 Features’ extraction for IoT classification

Following the amalgamation of packets into flows, the first \( t \) consecutive packets are extracted from each. Given that the majority of the observed scanning traffic are TCP SYN scans, the applicable features would reside in the TCP and IP header fields (i.e., ToS, Total Length, Identification, TTL, Dst IP Address, srcPort, dstPort, TCP SEQ, TCP ACK SEQ, TCP offset, TCP DATA Length, TCP Reserve, TCP Flags, TCP
Win, TCP UDP, TCP option, Packet Inter-arrival Time). Overall, along with the inter-arrival time of the consecutive packets within a flow, \(d = 17\) features are gathered for each packet. In turn, the data samples for each scanner IP address would consist of a \(t \times d\) matrix. To elaborate on the model’s training procedure, we subsequently detail the labeling process.

3.2.3 Port scanning and banner grabbing. In order to annotate decidedly accurate labels for the training dataset, it was imperative to immediately perform the procedure herein upon detection of a scan activity to circumvent any potential complications due to the dynamic reallocation of the associated device’s IP address (i.e., DHCP). To accomplish this, we utilized the gigabit open-source Internet scanning tool ZMap [20] as well as the high-speed application scanner ZGrab [18], in tandem, to provide comprehensive results necessary for guaranteeing the versatility of the classification task. Specifically, ZMap was used to probe the 45 most frequent ports \(^1\) of the IP addresses (that were previously inferred as probing sources) that were still found to be active. These ports are selected to cover most of the default ports of various devices (based on reports by ZoomEye [57]) in order to maximize the number of captured banners. Furthermore, via ZGrab, we were able to obtain banner fields and application handshakes from various protocols such as HTTP(s), CWMP, TELNET, SMTP(s), IMAP(s), POP3(s), SSH, FTP, SMB, DNP3, MODBUS, BACNET, FOX, Siemens S7 and SSL certificates. Additionally, we designed and developed two custom scanning modules to extract RTSP and SIP banners.

3.2.4 Tagging/Labeling. We amalgamated a comprehensive list of keywords related to major Internet-facing IoT devices and vendors. As previously noted, these are typically the devices that are most targeted by IoT botnets. This list consists of devices provided by Nmap along with results from ZoomEye Internet Scanner and ZTag, Censys’s tagging module. Although it is unrealistic to claim that we cover all IoT products from all vendors, we indeed employed information from various sources and focused on widely deployed Internet devices. In addition, we implemented a parsing algorithm which extracts useful keywords from banners and SSL certificates such as the combination of letters, digits, “-” and “_” signs, which typically represent device models [24] to enrich our list of devices. We further considered devices running multi-purpose OSs as non-IoT, which were identified using keywords such as “Win64”, “Ubuntu”, “Microsoft IIS” and “CentOS”, etc. while we deemed other specialized devices as IoT where their OS types were indicated as being “embedded”, “RouterOS”, “FritzOS” etc. \(^\dagger\) We also filter out benign scanners that have targeted the network telescope based on an obtained list \(^\dagger\) from Greynoise.io and returned information in banners.

3.3 Model training for fingerprinting compromised IoT devices

We propose herein a learning approach for the extraction of embedded features within unsolicited scan flows for the training of a binary classifier which distinguishes between traffic originating from both malicious IoT and non-IoT devices. The underlying methodology is based upon determining similarities in network traffic that are exclusively associated with IoT devices and their corresponding IoT malware in order to fingerprint flows originating from them. Additionally, it is known that IoT products manufactured by the same vendor possess a uniform, low-level architecture such as sharing a similar network card, operating system, etc., and happen to share the same TCP/IP stack information, including but not limited to TTL value and initial TCP window size, thus permitting the fingerprinting of IP addresses that Internet scanning services (i.e., Shodan) may have overlooked or could not identify.

To select a suitable and a sound learning technique, we compare and contrast the performance of 5 models to permit the classification of compromised IoT devices in order to distinguish them from compromised, multi-purpose hosts. The first three are based on Convolutional Neural Networks (CNN), which are a category of deep learning models that use dynamic kernels to automatically extract features. To this end, we assess a two-dimensional CNN (2D-CNN), a one-dimensional CNN (1D-CNN) [15] and a multi-window one-dimensional CNN (MW-1D-CNN) [13] along with two “shallow” learning methods rooted in Random Forest (RF) models.

In this context, an input sample consists of a matrix representation \(X\) of a flow with \(t\) packets and the number of extracted features \(d\) from a packet is considered, yielding \(X \in \mathbb{R}^{t \times d}\). Namely, the \(i^{th}\) packet in a given flow is \(x_i \in \mathbb{R}^d\). Convolution operations are also defined by applying local kernels \(w \in \mathbb{R}^{h \times w}\) on the input to extract spatially local correlations in the data. In terms of the 2D-CNN model, it contains \(L\) number of consecutive two dimensional convolutional layers (with \(k\) kernels of size \(w \times w\)) and max pooling, followed by two dense hidden layers of sizes 64 and 32, respectively, and a Softmax classifier at the end (Figure 2a). The 1D-CNN model has a similar architecture to the 2D-CNN, but instead, the convolution kernels have a fixed kernel width equal to the input sample width (i.e., \(h \times d\)) (Figure 2b). Further, the MW-1D-CNN model mixes the outputs of various kernel heights \(h\) to capture the features. In turn, the output of the first layer of the proposed model is given by \(c_i = f(w \cdot x_{i_1 \ldots i_{h-1}} + b)\), where \(x_{i_1 \ldots i_{h-1}}\) defines the notation for a sequence of packs \(x_1, x_2, \ldots, x_{h-1}\) \(b\) representing the bias, and \(f\) denoting the non-linear activation function. The filter is applied to each 2D sample instance to produce a feature map \(c = [c_1, c_2, \ldots, c_{t\times h}]\). Subsequently, max pooling is applied over the feature map \(c\), taking the value max \(c\). We used kernels \(w\) of different window heights \(h\) \((h = [2, 4, 6, \ldots, h_{max}]\)) to enable the capture

---

\(^1\)We make this list publicly available in the mentioned repository.

---

Figure 2: CNN models for IoT/non-IoT binary classification
of varying dynamics specific to darknet packet flows (Figure 2c). We also devise two RF models, one that has been constructed using raw packet features while the other operates on feature statistics. We define feature statistics as the 5-tuple \{min, 1-quantile, median, 3-quantile, max\} of each field in flows of packets, which overall produces 85 features. These statistics can be considered as an estimation of the probability distribution function related to each field of the packet sequence in each flow.

3.4 IoT botnets: features’ extraction and campaign inference

Following filtering out non-IoT sources by employing the developed classifier, we conduct a thorough investigation of the individual scan flows FlowIP, each comprising of at least 500 (t ≥ 500) sequential packets originating from a particular unsolicited IoT device, and extract the corresponding feature set FIP = <PortsIP, πIP, FlagIP, ARRIP>. PortsIP is the grouping of the targeted transport protocols paired with their associated ports in ascending order (e.g. PortsIP = [TCP:23, TCP:80, TCP:8080]). In turn, πIP is the corresponding discrete probability distribution function which represents the frequency of appearance of each of these ports within the given flow of packets (e.g. πIP = [0.15, 0.70, 0.15]). This is relevant due to the fact that IoT devices typically possess a limited supply of resources and as a result, in the midst of conducting illicit scanning activities, are often allocated to different ports and weighted based on the expected return. On the other hand, FlagIP is a boolean variable, holding a value 1 if the IoT device conducting the scanning has the signature tcpSeq = distIP and 0 otherwise. This inference would provide some insights about a Mirai-like behavior, possibly indicating a variant or a code-reuse practice. Lastly, the Address Repetition Ratio, or ARRIP, is the ratio of the total number of packets sent by a specific source IP address over the number of unique destination IP addresses, and is defined as ARRIP = \frac{\text{FlowIP}}{\text{distIP} \times \text{FlowIP}}. Such scenarios as an ARRIP greater than one are a consequence of the sending of multiple packets to a particular destination in order to compensate for packet loss and/or the probing of multiple ports at each destination. Note that, each instance of the same probing campaign will exhibit an equivalent ARRIP due to the underlying IoT orchestrated probing machinery. Consequently, we hierarchically divide the IP addresses of the IoT scanners into separate groups GI based on the given PortsIP, FlagIP and ARRIP of their feature set FIP. Upon completion, we cluster members of each group GI to identify those scanning for the same set of ports but with a different probability distribution function π. This enables us to leverage hierarchical agglomerative clustering [56], which determines the proximity matrix by calculating the distance between every pair of probability distribution functions \{πIP | IP ∈ GI\} based upon the Jensen-Shannon Divergence (JSD) distance metric. JSD, defined in (8), is typically utilized to estimate the distance between two discrete distribution functions, and is the symmetrized version of the well-known Kullback-Leibler Divergence (KLD).

\[
\text{JSD}(\pi_i | \pi_j) = \frac{1}{2} KLD(\pi_i | M) + \frac{1}{2} KLD(\pi_j | M),
\]

(8)

where \(M = \frac{1}{2}(\pi_i + \pi_j)\), and \(KLD(\mathbf{P}|\mathbf{Q}) = -\sum_i P(i) \log \left( \frac{Q(i)}{P(i)} \right)\) for discrete PDFs \(P\) and \(Q\).

We select hierarchical agglomerative clustering due to the fact that other clustering methods (such as K-means) are based on the assumption of equal cluster sizes which is not correct in this case while density-based techniques are computationally intensive with the increase in input data samples. Thereupon and proceeding in a bottom-up fashion, each observation forms its own cluster and begins moving up the distance-based hierarchy, subsequently merging with the clusters positioned along the way. To designate appropriate consolidation, we use a distance threshold (of 0.05) in which merging only occurs if the distance between the two given cluster centers falls beneath.

4 EMPIRICAL EVALUATION

The evaluation was executed using 3.6 TB of darknet traffic that was collected for a 24-hour period on Dec. 13th, 2018. This data was provided by the Center for Applied Internet Data Analysis (CAIDA) /8 network telescope. While the dataset per se is subject to MOUs and thus cannot be shared as is, interested readers can request access to CAIDA’s real-time darknet data through DHS IMPACT [38]. Additionally, a 24-hour sample is available in the mentioned repository.

4.1 Results of the darknet sanitization model

By executing the proposed model of Section 3.1, the distribution of malicious and misconfiguration traffic with respect to the number of packets were found to be 88.21% and 11.21%, while in the matter of source IP addresses were 26.17% and 73.83%, respectively. Validation of such outcome revealed that close to 90% of the misconfiguration traffic defines packets that hit the /8 network telescope only once, while the remaining appeared to be malformed packets. Further, it can be observed that even though the misconfiguration traffic is relatively low (11.79%), it is responsible for a large proportion of the source IP addresses (73.83%). These findings not only shed more light on the problematic nature of misconfiguration traffic with regards to Internet measurements via network telescopes, but consequentially emphasize the effectiveness of the proposed pre-processing model.

For the runtime specifics of the implementation which heavily relied on the Linux-derived libpcap C++ library, running on an Ubuntu 18.04 system with a quad core Intel Core i7-8550 at 1.80GHz processor, and 16GB of RAM, the developed approach was able to process close to 10 GB of darknet data in around 8 minutes. We believe this could be vastly improved by switching to SSD storage (since most of the delay was I/O related) and by adopting multithreading.

4.2 Results of datasets preparation

Regarding the data collection and dataset preparation steps of Section 3.2, and by immediately scanning back about 1.7M Internet scanners inferred through the network telescope, about 25.84% of them were found to have at least one open port. Further, amongst total 543,392 gathered banners, most of them were HTTP (54.11%), FTP (11.10%), SSL Certificate (10.50%), TELNET (10.19%), RTSP (7.00%), and CWMP (2.60%). Having completed this task, we were able to distinguish between 45,184 IoT and7,763 non-IoT devices to design the training data set. At this juncture, the label and corresponding metadata were incorporated into \(t \times d\) training and
test data matrices of IoT and non-IoT devices. We shuffled them and then performed normalization by way of the MinMax method, after which we computed and removed the mean from the data. Consequently, to evaluate the proposed model, we trained it using a prepared dataset captured in Nov. 2018 and then tested it using our dataset from Dec. 2018. The one month gap between the training and test datasets ensured that there exists no correlation between them for sound evaluation. The test dataset consisted of 34,974 IoT and 7,193 non-IoT sources.

4.3 Evaluating the IoT classification models

The proposed CNN models were implemented in Keras [14] over Tensorflow. To address the problem of class imbalance within the training dataset, cost-sensitive learning was applied [50]. The number of epochs was found to be 30 to avoid over-fitting. Further, we performed a random search on subspaces of hyper-parameters as presented in Table 1, leveraging Hyperas [42], and selected the best model (out of 100 trials) with regards to the loss. Accordingly, the RF models were implemented and trained using the scikit-learn package and the best model was retrieved based upon random search (using the RandomizedSearchCV method) in the search space as summarized in Table 2. In Tables 1 and 2, parameter ranges are reported with begin:step:end format. For evaluating the CNN models, we leverage an NVIDIA GeForce RTX 2070 GPU with 8GB of memory, 2304 CUDA cores and 288 Tensor cores to accommodate for parallelization.

To compare the performance of the different models, we rely on typical metrics such as precision, recall and F-measure for the IoT class. We report the results in Figures 3 and 4. We can note that the AUC-ROC score for the RF model trained on quantiles is slightly higher than that of the other models. Further, both of the figures reveal that the CNN-based models result in higher recall and lower precision scores in contrast to the RF models. The outcome also reveals that the CNN-based models result in higher recall and lower precision scores in contrast to the RF models. The outcome also shows that the multi-window 1D-CNN (MW-1D-CNN) outperforms the 1D-CNN and the 2D-CNN; this is quite expected, since packet fields (unlike image pixels) lack temporal or spatial relationships with one another, and thus moving the kernels over the horizontal dimension would not lead to better learning. Furthermore, the multi-window 1D-CNN can capture varying dynamics being that only a portion of packets hit the /8 darknet.

Features’ importance. Although CNN models extract complex features, they are typically not interpretable. Nevertheless, to shed light on which features were most decisive in the learning process, and given that the RF models performed closely to the CNN models, we illustrate the features’ scores (derived from the RF model on quantiles) in Figure 5. Expectedly, the distribution of destination ports which typically reveals the scans’ intentions is indeed playing the most noteworthy role for fingerprinting IoT devices. This is closely followed by other fields such as total packet length and total header length, in addition to TCP/IP stack and OS-related fields such as TCP window size, option fields and TTL.

4.4 Inferring and characterizing compromised IoT devices and campaigns

Given the aforementioned classification results, we selected the MW-1D-CNN model since it provided the highest true positive rate while strictly limiting the false positive rate to around 0.08 (Figure 4). We further re-trained the model on recent data from Dec. 2018 to accompany for any evolving dynamics. By applying the binary classifier on 24 hours of darknet data of Dec. 13th, it was capable of fingerprinting 441,766 out of the 1,787,718 unique scanners to be originating from compromised IoT devices. Although previous works solely considered those with a Mirai signature as IoT-related [5], we inferred that in fact, they make up less than 25% of the IoT scanner population that the proposed model was able to uncover, leaving a whopping 75% to go about their malicious activities without any semblance of an adequate attribution. Regarding the location of these exploited devices, Brazil (41.93%) was found to be hosting a significant portion, followed by Iran (10.17%), China (5.14%), Russia (3.59%), Egypt (3.36%), India (2.47%) and Turkey (2.32%). Furthermore, the top three Internet Service Providers (ISP) housing the largest number of compromised IoT devices were Vivo (134,021), TE Data (11,804) and Iran Telecom Co. (9,912). While the extensive presence of IoT scanners in and of itself gives pause for concern, a relatively significant proportion residing within the telecommunication and ISP sectors is rather expected; conversely, their existence within sectors including but not limited to critical infrastructures (87), government entities (86), manufacturing (99), and commercial businesses (38).

Along those lines, the lengthy list of 50 identified vendors reveals a broad range of manufactures and device types that IoT botnets demonstrate preference for exploitation. Amongst them, MikroTik (14,090), Aposonic (2,222), Huawei (732), Foscam (594) and Hikvision (417) are the topmost five targeted by the tagged

---

Table 1: Tuned hyperparameters of the selected CNN models

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Space</th>
<th>1D-CNN</th>
<th>2D-CNN</th>
<th>MW-1D-CNN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimizer</td>
<td>Sgd</td>
<td>RMSProp</td>
<td>RMSProp</td>
<td>RMSProp</td>
</tr>
<tr>
<td>Num. kernels (k)</td>
<td>32,64,128</td>
<td>32</td>
<td>128</td>
<td>64</td>
</tr>
<tr>
<td>Kernel size (w x w)</td>
<td>2,2/3,1,3</td>
<td>2,2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Kernel height (h)</td>
<td>2,4,8,16,32,64</td>
<td>-</td>
<td>64</td>
<td>-</td>
</tr>
<tr>
<td>Max kernel height (hmax)</td>
<td>40:10:80</td>
<td>-</td>
<td>-</td>
<td>80</td>
</tr>
<tr>
<td>Pool size (p)</td>
<td>2,3</td>
<td>2</td>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td>Batch size</td>
<td>128,256</td>
<td>128</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>Activations</td>
<td>Relu, Sigmoid, Tanh</td>
<td>Sigmoid</td>
<td>Tanh</td>
<td>Sigmoid</td>
</tr>
<tr>
<td>Dropout</td>
<td>0.0,0.1,0.3</td>
<td>0.195</td>
<td>0.296</td>
<td>0.298</td>
</tr>
<tr>
<td>learning rate</td>
<td>0.001</td>
<td>0.001</td>
<td>0.001</td>
<td>0.001</td>
</tr>
<tr>
<td>Num. CNN layers (L)</td>
<td>1:1:4</td>
<td>4</td>
<td>3</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 2: Tuned hyperparameters of the RF models

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Space</th>
<th>RF on raw fields</th>
<th>RF on Quantiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num. estimators</td>
<td>20-20-100</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Max depth</td>
<td>4-20</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Min samples leaf</td>
<td>2-10-102</td>
<td>52</td>
<td>52</td>
</tr>
<tr>
<td>Min samples split</td>
<td>U(2, 10)</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Bootstrap</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>Criticism</td>
<td>Gini, Entropy</td>
<td>Gini, Entropy</td>
<td>Gini</td>
</tr>
</tbody>
</table>

Figure 3: Performance metrics of the devised models
Coinhive for injecting JavaScript crypto-currency miners into the HTTP requests’ responses to the IoT scanners, tagging those that contain the xmrMiner or Coinhive JavaScript modules, and exporting their corresponding keys. By doing so, we were able to discover 1,134 xmrMiner and 923 Coinhive instances with 23 and 30 distinct keys, respectively. The campaigns designated as containing members with cryptojacking capabilities are pinpointed in Table 3. In addition, we uncovered large campaigns maintaining crypto miner instances with and without the presence of Mirai-like signatures. Moreover, 943 out of 1,134 devices, belonging to a total of 18 campaigns (#1, #2, #4, #5, #7, #8, #11, #13, #15, #16, #19, #20, #21, #24, #32, #33, #35 and #36), share the same xmrMiner-related key “4983e34ef01b4b579725b3a228e59f79”. In other words, large portions of immense IoT campaigns could be reported to be attributed to the same “player”. On top of that, upon exploring the key in Censys, 54,743 Mikrotiks were shown to possess it. In total, these campaigns equate to approximately 250,000 compromised IoT devices—more than 54% of all the identified compromised devices.

A closer look at other campaigns of interest. Campaign #3 with 36,464 bots was inferred to be targeting ports 23 and 2323 with a proportion of 9:1, which is the same as instructed within the Mirai released code. Another interesting observation is related to botnet #26 (of Table 3) where packets to random TCP and UDP ports were sent in addition to targeting the defined set of ports of [23, 2480, 5555, 5984, 80, 8080]. Additionally, this campaign targeted port 2480 (OrientDB) and 5984 (CouchDB), as well as other common IoT-related ports including 23, 5555 (ADB) and 8080. Upon further analysis, this behavior could be indeed attributed to the infamous Hide and Seek botnet [45].

In the context of port 32764 which is related to a backdoor vulnerability [52], the proposed IoT botnet clustering approach revealed a campaign of substantial size (#19 in Table 3), consisting of 2,140 active IoT scanners with the following signature <[23, 32764, 80, 8000, 8080, 8081, 8089, 8090, 81, 8181, 8443, 8888, 9000]>, Flag=1, ARR=1>. We did not come across any previously reported botnet families that scan such ports. As a result, we postulated that this campaign is either new or specific ports have recently been added to the target list of a previously known IoT botnet. Another aspect is that this is the only large campaign that exploited a relatively significant number of NPPD products, which is a common indicator of the Reaper IoT botnet. The JexX botnet [21], which scans ports 37215 and 52869, was also disclosed. Moreover, a botnet with <[2004, 80, 8080, 81]>, Flag=0, ARR=2> was also discovered and consisted of 35 coordinated IoT scanners, all of which compromised QNAP NAS. This campaign strongly resembles that of the Muhstik botnet [44], with the exception of the substitution of port 7001 with 81 in the target port set.

With the prevalence of IoT botnets, port 5555 (Android debug bridge) has become a popular target port. We found 23 IoT botnets that port 5555 is among their target port set. Based on the reports on ADB miner [3] and the similarity of its scanning module to Mirai, we can attribute the inferred large IoT botnet (#5 in Table 3) to Mirai or its variant Fbot [4]. Additionally, we found xmrMiner instances with the same previously noted key in the latter campaign and in campaign #16. Based off the set of target ports pertaining to campaign #25 (port 23, 5358), it seems to be highly likely attributed to that of the Hajime [29, 43] IoT botnet. In total, this campaign...
possessed 1,059 active IoT scanners (made up of IP cameras/DVRs). Furthermore, amidst the inferred campaigns exists those whose geo-distributions do not comply with that of the global distribution of infections. For instance, with respect to campaigns #13, #22 and #27, more than 98% of their infected IoT devices are located in Iran. In another instances, campaign #30 has upwards of 50% and 10% of compromised IoT devices located in USA and the UK, respectively, and the majority of the members of campaign #28 are located in North America (40%) and Europe (21%).

Table 3: Orchestrated IoT botnets in the wild

<table>
<thead>
<tr>
<th>Id</th>
<th>Ports</th>
<th>Flag</th>
<th>ARR</th>
<th>#Bots</th>
<th># Miners</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>23, 80, 8080</td>
<td>1</td>
<td>139,858</td>
<td>0.33, 0.33, 0.34</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>23, 80, 8080</td>
<td>1</td>
<td>155,139</td>
<td>0.294, 0.295, 0.411</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>23, 2323</td>
<td>✓</td>
<td>36,464</td>
<td>0.9, 0.1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>80</td>
<td>✓</td>
<td>12,895</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>3335</td>
<td>✓</td>
<td>11,950</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>23, 81</td>
<td>1</td>
<td>9,805</td>
<td>0.495, 0.505</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>23, 80, 8080</td>
<td>2</td>
<td>7,610</td>
<td>0.171, 0.650, 0.179</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>23</td>
<td>✓</td>
<td>7,200</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>23, 80, 8080</td>
<td>1</td>
<td>5,971</td>
<td>0.242, 0.244, 0.514</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>23</td>
<td>3</td>
<td>5,491</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>80, 8080</td>
<td>1</td>
<td>5,162</td>
<td>0.492, 0.508</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>23</td>
<td>1</td>
<td>4,689</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>23, 80, 8080</td>
<td>1</td>
<td>4,468</td>
<td>0.442, 0.032, 0.526</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>23</td>
<td>4</td>
<td>3,911</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>22, 2222</td>
<td>✓</td>
<td>3,783</td>
<td>0.897, 1.03</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>23, 2323, 3555</td>
<td>✓</td>
<td>3,545</td>
<td>0.249, 0.32, 0.719</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>23, 2323</td>
<td>✓</td>
<td>2,727</td>
<td>0.967, 0.033</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>23</td>
<td>2</td>
<td>2,146</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>23, 32764, 80, 8000, 8080, 8080, 8089, 8090, 81, 8181, 8443, 8888, 9000</td>
<td>✓</td>
<td>2,140</td>
<td>0.034, 0.122, 0.153</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>23, 8080</td>
<td>1</td>
<td>1,591</td>
<td>0.48, 0.52</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>23, 80, 8080</td>
<td>1</td>
<td>1,286</td>
<td>0.384, 0.319, 0.298</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>80, 8080+ rnd</td>
<td>1</td>
<td>1,247</td>
<td>0.45, 0.45</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>23, 81</td>
<td>1</td>
<td>1,191</td>
<td>0.095, 0.905</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>23, 80, 8080</td>
<td>1</td>
<td>1,083</td>
<td>0.226, 0.3, 0.274</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>23, 3555</td>
<td>1</td>
<td>1,059</td>
<td>0.5, 0.5</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>23, 2480, 3555, 5984, 80, 8080+ rnd</td>
<td>✓</td>
<td>783</td>
<td>0.126, 0.120, 0.134</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>80, 8080</td>
<td>3</td>
<td>756</td>
<td>0.814, 0.186</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>443, 80, 8000, 8081, 8080, 8081, 8088, 81, 82, 83, 84, 85, 88, 8888</td>
<td>✓</td>
<td>723</td>
<td>0.071, 0.071, 0.071</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>23, 2323</td>
<td>✓</td>
<td>691</td>
<td>0.794, 0.206</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>23, 9000</td>
<td>1</td>
<td>677</td>
<td>0.49, 0.51</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>23</td>
<td>5</td>
<td>642</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>80</td>
<td>1</td>
<td>616</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>23, 80, 8080</td>
<td>1</td>
<td>544</td>
<td>0.15, 0.3, 0.53</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>23, 81</td>
<td>1</td>
<td>541</td>
<td>0.291, 0.709</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>23, 445, 80, 8080</td>
<td>1</td>
<td>376</td>
<td>0.314, 0.3, 0.315</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>23, 7547, 80, 8080, 8291</td>
<td>1</td>
<td>340</td>
<td>0.334, 0.002, 0.33, 0.331, 0.002</td>
<td></td>
</tr>
</tbody>
</table>


