The Persistent Threat of DGA-Domains Used by Botnets

Arthur Drichel
RWTH Aachen University
drichel@itsec.rwth-aachen.de

Ulrike Meyer
RWTH Aachen University
meyer@itsec.rwth-aachen.de

***Abstract*—Botnets often employ Domain Generation Algorithms (DGAs) to evade detection and maintain communication with their Command and Control (C2) servers. Despite extensive efforts to contain individual botnets and take down their C2 infrastructure, a significant knowledge gap remains regarding the extent to which their associated DGA-generated domains continue to be registered by malicious actors, posing a latent threat. In this paper, we close this gap through a comprehensive measurement study in which we quantify the threats posed by botnets, including both active botnets and those that have been subject to previous takedown operations, by analyzing the daily registered domain names included in 1165 DNS zone files, covering 80.62% of all 1445 currently valid Top-Level Domains (TLDs), over a period of 13 months. During our study, we observe a decade-old botnet being reactivated by new actors, allowing them to receive incoming connections from previous dormant infections and take over a number of machines. In total, we uncover malicious activities associated with 7058 domains generated by 58 different known DGAs, at least 17 of which are used by botnets that have been the target of previous takedown operations. To improve the status quo, we discuss approaches that could have prevented the malicious acts and highlight the potential of recently proposed Machine Learning (ML) techniques to uncover yet unknown DGAs, enabling a more proactive approach to threat detection.**

***Index Terms*—Network security, DNS security, Domain Generation Algorithm (DGA), botnet, intrusion detection, Machine Learning (ML)**

I. Introduction

Botnets are networks of multiple malware-infected hosts (bots) that are remotely controlled by a botnet master via a Command and Control (C2) server and used for malicious activities such as Distributed Denial-of-Service (DDoS) attacks, stealing personal data, or sending spam. Bots often use Domain Generation Algorithms (DGAs) to establish a connection with the botnet master's C2 server to receive updates and instructions. DGAs are pseudorandom algorithms that, based on a seed shared between the malware and the botnet master, produce a large number of Algorithmically-Generated Domains (AGDs) that are queried by the bots one by one until they finally obtain the currently valid IP address of the C2 server. The botnet master knows the generation scheme and can therefore register an AGD before the AGD's validity period (i.e., before the bots query the AGD) to enable future botnet communication. For the botnet master, the advantage of DGAs over using fixed IP addresses or fixed domain names is that DGAs create an asymmetric situation in which defenders have to block all possible AGDs, while it is sufficient for the botnet master if a single domain successfully resolves.

In the past years the DGAs for many known malware samples have been time-consumingly reverse engineered and collected, e.g., in Open Source Intelligence (OSINT) feeds such as DGArchive [1]. Based on these efforts, lists of AGDs can be pre-generated before they are used by a botnet. Such lists can effectively be used to block DNS queries of infected devices and thus prevent them from obtaining the current IP address of their C2 servers. However, this approach only disrupts the communication of infected devices for which the DNS traffic is checked against the list of AGDs. Other infected devices will still be able to resolve AGDs.

In parallel, several large-scale takedown operations have been carried out in collaborations of various parties, in which millions of domains were seized across national borders to disrupt the C2 communication of botnets on a more global basis. Containing a botnet is, however, a Sisyphean task due to the underlying asymmetry, where a single domain registered by a malicious actor that is not blocked is enough to nullify all defense efforts as long as devices are infected. What additionally complicates botnet takedown operations is that the duration for which containment measures must be maintained is uncertain, and even legal or regulatory orders often omit to specify the period for which domain seizure or hold actions should be enforced [2]. Seemingly effective takedown operations are therefore often only of temporary nature [3]–[5]. A recent example is the attempted takedown of the *Qakbot* botnet, which was the target of a multinational operation led by the FBI in August 2023 [6]. The *Qakbot* botnet is one of the largest and longest-running botnets as of this date, which has infected more than 700 000 computers worldwide and has generated ransom payments of at least €54 million since 2007 [7]. Just three months after the takedown, the revival of the botnet was noticed through new phishing campaigns [8]. This situation is further deteriorated by the slow cleanup rates of infected devices. Asghari et al. [3] showed that even six years after the demise of the *Conficker* botnet, nearly one million machines were still infected. This creates a particularly dangerous situation because, although their C2 infrastructure was taken down in the past, the bots continue to query AGDs and wait for the attackers to find a way to reconnect to them. Moreover, the bots left behind after the takedown of their C2 infrastructure also attract other attackers, since these machines often remain vulnerable and can therefore be compromised again. In this context, Asghari et al. [3] found an unusually high number of machines infected with *Conficker* that were also infected with the *Gameover* malware. Additionally, the authors found that even large-scale national cleanup initiatives for *Conficker*-infected machines had no observable impact on the growth, peak height, or decay of the botnet. Orthogonal to this, Alowaisheq et al. [9] uncovered flaws in the life cycle of takedown operations, where outdated DNS records allow attackers to regain control over sinkholed domains. Overall, the long-term success of botnet takedowns is therefore questionable.

Given the potential for latent threats and the continued growth of botnets that have been the target of takedowns in the past, a comprehensive analysis is essential to quantify the threat landscape and mitigate the risks posed by botnets. Thus, in our work, we determine the prevalence of AGDs of *known* DGAs across various zones and assess their association with previously disrupted botnets. Moreover, we investigate whether these AGDs continue to facilitate current malicious activities despite prior takedown efforts.

To gain a more holistic understanding of the AGD landscape, identifying *unknown* DGAs through DNS zone file examination is crucial. While prior research has demonstrated that Machine Learning (ML) classifiers, trained on known benign and malicious domains, can detect AGDs generated by both known [10]–[13] and unknown [10], [11], [14] DGAs in DNS traffic, the feasibility of using ML classifiers to detect new DGAs in zone files remains unexplored. Analyzing zone files has two advantages over monitoring DNS traffic: it may reveal unknown DGAs before an infection, and it can be performed independently of access to DNS traffic.

In this work, we conduct a comprehensive measurement study on the current landscape of registered AGDs, closing the gaps outlined above. To this end, we analyze registered domain names included in 1165 DNS zone files, covering 80.62% of all 1445 valid Top-Level Domains (TLDs) [15], over a period of 13 months. In total, the observed TLDs account for approximately 240 million domain names, which corresponds to 66.24% of all 362.3 million domains registered at the end of the third quarter of 2024 [16]. We analyze the distribution of registered AGDs, identify active DGA-related malicious campaigns, and quantify the number of registered AGDs across the analyzed TLDs. We identify botnets with seemingly defunct C2 infrastructure that are still exploited for malicious purposes, indicating that past takedowns were only temporarily effective. In total, we uncover malicious activities associated with 7058 domains generated by 58 different known DGAs, at least 17 of which are used by botnets that have been the target of previous takedown operations. In addition, our study provides insights into the extent to which registrars could prevent malicious domain registrations if they refused to register AGDs contained in pre-generated blocklists.

Furthermore, we analyze recent advances in ML for the use case of DGA detection and investigate to what extent they can be used to detect newly registered malicious domains, focusing on AGDs generated by yet unknown DGAs. We compare an ML-based detection approach for detecting AGDs of yet unknown DGAs among the newly registered domains in zone files against the blocklists of two major DNS service providers (Cloudflare [17] and Quad9 [18]) that have integrated both commercial and publicly available threat intelligence feeds. In particular, we show that the "*window of opportunity*", namely the time required to include malicious AGDs into blocklists and during which botnet communication cannot yet be prevented, present in blocklist-based approaches, can be reduced by an ML-based approach. Thus, we quantify the time benefit of using recent ML-based techniques to detect unknown AGDs in zone files before they are added to blocklists.

In summary, our main contributions are:

1) We conduct a comprehensive measurement study on the current landscape of registered AGDs. Thereby, we are the first to systematically quantify the latent threat posed by DGA-based botnets, yielding unprecedented insights into the scope and scale of this threat.
2) We show that even botnets that have been the target of takedown operations in the past, resulting in a seemingly defunct C2 infrastructure, are still actively exploited for malicious purposes. To this end, we use a novel methodology that provides a strict lower bound on the number of AGDs generated by known DGAs that were recently used for malicious acts. Our findings highlight the inadequacy of current containment measures and underscore the need for enhanced countermeasures to effectively combat botnets.
3) We leverage recent advances in ML-based AGD detection to shed light on the threat posed by unknown botnets. Specifically, we analyze to what extent ML-based techniques can be used to detect AGDs generated by yet unknown DGAs among newly registered domains. We empirically demonstrate the benefits of such an approach and compare its effectiveness to that of public blocklists and commercial threat intelligence feeds.
4) We critically analyze the available measures to contain botnets and provide pointers for defusing the current situation, which would have prevented the malicious activities uncovered in our study.

II. Background & Related Work

First, we summarize research on DGA blocklisting efforts, analyze state-of-the-art approaches to DGA detection, and provide an overview of various studies on registered domains.

A. DGA Blocklisting Ecosystem

In the context of DGA detection, Kührer et al. [19] showed that in 2014 most blocklists operated by antivirus vendors did not sufficiently cover DGA domains to protect their users effectively. Xu et al. [20] pointed out that unlike other blocklists (e.g., for spam or phishing), AGDs can be generated in advance to enable predictive blocking once a DGA has been reverse engineered. Plohmann et al. [1] evaluated the effectiveness of predictive blocking based on reverse engineering the DGAs of 43 malware families. The authors generated approximately 18 million AGDs using these DGAs and analyzed their registration status based on historical WHOIS data. They concluded that predictive blocking is extremely effective with almost no false positives. In addition, Plohmann et al. introduced the web service DGArchive [1] offering reverse domain lookups and forward generation of DGA blocklists. At the time of writing DGArchive consists of approximately 199 million unique AGDs generated by 115 reverse engineered DGAs, making it the OSINT feed containing the most DGAs.

Note that of the 18 million pre-calculated AGDs analyzed by Plohmann et al. [1], only 115 079 (0.62%) were actually registered. In contrast, in our work, we take the opposite approach by directly observing all registered domains in 1165 DNS zone files over a 13-month period to map the landscape of registered DGA domains. We use DGArchive as the basis for ground truth, which allows us to detect all registered AGDs contained in this OSINT feed. However, the analysis of all registered domains in our study also allows us to identify still unknown AGDs. Thus, with our work we significantly extend the study by Plohmann et al. [1] and provide a holistic view on the threats posed by DGA-based botnets. In addition, we quantify the level of adoption of predictive blocking and propose an approach that significantly improves botnet containment.

We base our analysis of registered domains generated by known DGAs on DGArchive, as DGArchive is the most complete blocklist for DGAs at the time of writing. The use of more general blocklists that do not specifically specialize in DGAs, such as Google Safe Browsing [21], Spamhaus [22], SURBL [23], or URLhaus [24], is of little help when it comes to portraying the prevalence of AGDs, as these blocklists usually only contain AGDs that have been identified in being associated with a malicious action. However, such blocklists are still useful when it comes to identifying malicious domains. Therefore, in our work, we make use of two major DNS service providers that block malicious domains based on a combination of several commercial and publicly available blocklists and compare their effectiveness with the most complete blocklist for DGAs (DGArchive).

B. DGA Detection Algorithms

Unlike blocklisting, DGA detection algorithms have been shown to generalize well and can even detect AGDs generated by known DGAs that are using unknown seeds or even by yet unknown DGAs [10], [11], [14].

In general, approaches to DGA detection can be divided into two groups: context-less (e.g., [10]–[13], [25]–[27]) and context-aware (e.g., [28]–[35]) approaches. Context-less approaches use only the information that can be extracted from the domain name being classified for decision-making, and do not consider any additional information. Context-aware approaches, on the other hand, leverage additional contextual information such as statistical data from the monitored network in an attempt to further improve detection performance. Previous studies (e.g., [10]–[13]) have shown that context-less approaches achieve state-of-the-art detection performance, while requiring fewer resources and being less intrusive than context-aware approaches.

Within the group of context-less approaches, several studies (e.g., [10], [12], [36]–[38]) have shown that Deep Learning (DL) based classifiers (e.g., [10], [12], [13]) consistently outperform feature-based approaches (e.g., [11], [31], [39]).

Recently, Drichel and Meyer [25] analyzed the explainability of context-less DL classifiers for DGA detection and uncovered several biases inherent in state-of-the-art approaches, including a large bias related to the TLDs used in domain names. For instance, an attacker can simply replace the TLD of a malicious AGD (which would otherwise be detected with high confidence) to bypass detection by a biased classifier. As we analyze a large variety of TLDs, we use their proposed bias-reduced classifier in our ML-based classification study to detect AGDs generated by unknown DGAs.

Note, DL classifiers are known to be vulnerable to adversarial attacks in which semantic gaps in the training data create blind spots that make the classifiers susceptible to small input perturbations that lead to misclassifications. Adversarial training can be used to mitigate this issue [40]. The robustness of the classifier against adversarial attacks is outside the scope of our study, as several works have addressed this issue in the context of DGA detection (e.g., [10], [36], [38], [41]–[53]).

None of the previous work analyzed registered AGDs in DNS zone files. Most proposed classification approaches (e.g., [10], [11], [30], [35], [39], [54], [55]) focus on the classification of non-resolving DNS traffic (NX-traffic) to detect hosts infected with DGA-based malware within networks. In contrast, by analyzing DNS zone files, we can classify domains across network boundaries that would allow C2 communication once registered, rather than classifying requests by already infected machines that do not resolve.

To the best of our knowledge, we are the first to systematically analyze DNS zone files to conduct a large-scale study of registered DGA domains. The work by Antonakakis et al. [29] is most closely related to analyzing zone files. The authors proposed a detection system called Kopis which monitors DNS traffic at upper levels of the DNS hierarchy to detect malware domains by analyzing global DNS query resolution patterns. Antonakakis et al.'s approach, however, incurs a 14-day detection delay, making it unsuitable for identifying short-lived AGDs that become inactive before being reported. In addition, Kopis relies on extensive tracking of DNS traffic and is therefore not suitable for analyzing a large number of different TLDs. For these reasons, and due to the fact that the reported FPR of Kopis is higher compared to context-less state-of-the-art approaches (e.g. [10]–[12]), we focus our work on context-less classification. This allows us to analyze all domains added daily in 1165 zone files and detect malicious AGDs as soon as they are registered.

C. Studies on Registered Domains

Multiple studies dealt with the identification and analysis of sinkholed and parked domains (e.g. [56]–[62]).

In our work, we aim to quantify the threat posed by DGA-based botnets and provide an overview of AGDs that have recently been used for malicious acts. Therefore, we are only implicitly interested in classifying AGDs according to whether they are sinkholed or parked. Nevertheless, as a secondary contribution, we use proposed classification approaches to provide an overview of all registered AGDs in Appendix A.

Of greater relevance to our work is the study by Alowaisheq et al. [9], in which the authors analyzed the domain takedown procedure and uncovered several flaws in the live cycle of takedown operations that allow attackers to regain control over sinkholed domains. Within their study, they identified seized domains for "some supported TLDs" using historical WHOIS information and passive DNS data, and also tried to provide an overview over DGA domains. To identify DGA domains within the group of seized domains, the authors used a classification approach [63] based on the bigram frequency of domain names which was not the state of the art at the time of the study. While the authors acknowledge the high False-Negative Rate (FNR) of 8%, they ignore the FPR, which according to the tool developer can be as high as 8% [63]. Due to the data and classification approach used and the focus on historically seized domains, the authors only provide an incomplete view on DGA domains.

Other studies that have dealt specifically with botnets are the studies by Asghari et al. [3] and Nadji et al. [4], [5]. Asghari et al. [3] analyzed sinkhole logs to quantify the cleanup rates for *Conficker*-infected machines and concluded that the cleanup rates for this particular botnet are rather slow, so that even six years after the botnet was taken down, one million machines were still infected and thus potentially vulnerable. Nadji et al. [4], [5] analyzed the malicious domain coverage of five historical botnet takedowns. The authors relied heavily on passive DNS data to retrospectively detect missed malicious domains in botnet takedowns, and showed that multiple takedown operations had no real long-term impact.

Our work fundamentally differs from previous studies on botnets in several ways:

First, previous studies on botnets [1], [3]–[5], [9] all rely heavily on historical data, such as sinkhole server logs, historical WHOIS information, or passive DNS data. Thereby, these studies provide only limited insight, while our focus on DNS zone files provides a holistic view of the current landscape of registered DGA domains.

Second, whereas previous work focuses on analyzing malicious domains generated by known DGAs, our study utilizes recent ML advancements to also reveal AGDs generated by unknown DGAs, providing a more comprehensive view of the current threats posed by botnets.

Third, prior studies are limited to a retrospective analysis of malicious domains after they have already been used for malicious purposes. In contrast, we focus on analyzing DNS zone files, which enables the evaluation of domains as soon as they are registered and before potential harm.

All in all, we significantly extend the previous work by conducting a comprehensive measurement study on the current landscape of registered DGA domains, quantifying the threat posed by botnets, critically analyzing the available measures to contain botnets, and proposing mitigation strategies.

III. Evaluation Setup

After reviewing related work and identifying shortcomings, we establish our evaluation setup to extend previous work and address gaps. To this end, we define our data and methodology used as well as discuss our ethical considerations.

A. Data

We collect publicly available country code TLD zone files as well as generic TLD zone files via the Centralized Zone Data Service (CZDS) [64] operated by the Internet Corporation for Assigned Names and Numbers (ICANN) for TLDs that have actively granted us access for our research. Additionally, we use DGArchive as a source of ground truth for AGDs generated by known DGAs.

1) Zone Data: ICANN introduced CZDS to facilitate access to the zone files of generic TLDs. In total, we collect 1165 zone files daily, 1152 via CZDS and 13 via publicly available sources during the 13-month period between 2022-06-01 and 2023-07-01.

The publicly available TLDs include: *.ee* [65]; *.fr*, *.pm*, *.re*, *.tf*, *.wf*, *.yt* [66]; *.nu*, *.se* [67]; *.ru*, *.su*, *.xn–p1ai* (.рф) [68]; *.sk* [69]. For the TLDs *.fr*, *.pm*, *.re*, *.tf*, *.wf*, and *.yt*, we only collect the daily registered domains since AFNIC [66] provides only those on a daily basis.

Through ICANN's CZDS, we requested access to 1171 zone files in total. 1152 registry operators accepted our request, eight rejected it, and eleven requests remain unanswered after more than 14 months. After we applied for access, we waited 20 days to give the registry operators time to process our application. The majority acted in a timely manner such that we decided to start our evaluation on the 2022-06-01. However, for 39 of the 1152 TLDs, the decision to accept our application was made after the evaluation period had begun. The longest time it took to accept our request was 370 days. For 88 of the 1152 TLDs, registry operators did not renew the download permission in time, so for these zone files, the observation period ends before the end of the evaluation period on 2023-07-01. For another 16 TLDs, the observation period also ends prematurely because the TLDs were set inactive during our study.

In summary, we collect a total of 1165 DNS zone files, covering 80.62% of all 1445 valid TLDs [15] including the large generic TLDs such as *.com*, *.net*, and *.org*, over a 13-month period. Note that the domain distribution over the TLDs is highly imbalanced, e.g., the domains in the *.com* zone file account for approximately 167 million samples (46.21% of all registered domains). In total, the observed TLDs account for approximately 240 million domain names, which corresponds to 66.24% of all 362.3 million domains registered at the end of the third quarter of 2024 [16].

2) DGArchive: We use the OSINT feed of DGArchive [1] as a source of ground truth for our evaluation. To this end, we received a full dump of DGArchive including AGDs and their validity periods up to 2022-12-31. We expand the full dump with all domains included in the daily blocklists of all following days until 2023-08-01. In total, we collect approximately 199 million AGDs generated by 115 DGAs.

B. Methodology

We divide our study into two parts: (1) a comprehensive measurement study to map the current landscape of *known* registered DGA domains, and (2) an ML-based classification study to detect clusters of potential *unknown* DGAs.

1) Newly Registered DGA Domains Study: In this study, we map the current landscape of newly registered DGA domains and provide an overview of the distribution of AGDs among the various TLDs and DGAs. To this end, we track all AGDs that are registered or removed from zone files daily over the course of 13 months between 2022-06-01 and 2023-07-01. We begin our analysis by identifying the intersection of the observed zone files and the TLDs used by the DGAs. The 115 DGAs included in DGArchive use a total of 628 effective Top-Level Domains (eTLDs), of which 213 are regular TLDs (e.g., *.com*) and 41 are domain names of dynamic DNS services. The rest consists of different public suffixes such as *.co.uk*, under which Internet users can directly register domain names. Four of the TLDs used (*.bazar*, *.load*, *.bit*, and *.onion*) are invalid in the sense that they do not resolve in the most widely used DNS root administered by ICANN, but are application-specific or are contained in alternative DNS roots. In total, the intersection of the 209 valid TLDs used by the DGAs and the 1165 monitored zone files is 64 TLDs. This allows us to track AGDs for 106 out of the 115 DGAs included in DGArchive, as these DGAs use at least one TLD we observe. For 57 DGAs we monitor all TLDs they use. For 63 of the 64 relevant TLDs used by the DGAs and monitored by us, we were able to download the zone files daily throughout the entire evaluation period. Only for the *.top* TLD the download permission extension was not granted in time and therefore our daily data for this TLD ends on 2022-08-17.

We divide this study into an analysis of *time-dependent* and an analysis of *time-independent* DGAs. Time-dependent DGAs incorporate a time source in calculating AGDs and have a validity period during which infected hosts will query the generated domains. We use DGArchive data available up to 2023-08-01 to filter the zone data and to identify all newly registered DGA domains within the evaluation period. We intentionally included an additional month of DGArchive data to get a more accurate picture of the registered DGA domains, as domains of time-dependent DGAs must be registered before their validity period ends to ensure they can be resolved once bots query the domains. In addition, we analyze how far in advance the AGDs are registered to gain insights into the extent to which predictive blocking could be used to prevent malicious registrations for known time-dependent DGAs. In contrast, time-independent DGAs do not use a time source for the calculation of AGDs and therefore their AGDs could directly serve as potential C2 domains upon registration.

For both time-dependent and time-independent DGAs, we examine how many of the AGDs generated per DGA are actually registered to estimate how many requests from infected hosts result in non-existent (NX) domain responses. Thereby, we are also able to analyze whether the approach of classifying NX-traffic is suitable for detecting DGAs.

Finally, we determine a lower bound on the number of AGDs that are used for malicious purposes during the monitoring period, which we refer to as "*verified malicious*".

Determining Malicious Activity: We use a novel methodology that utilizes multiple data points provided by VirusTotal [70] for verification. We classify a domain as malicious only if it has been reported to communicated malicious executables, that were identified as malicious by at least ten security vendors, during the monitoring period. Thereby, we deliberately avoid relying solely on domain reports that indicate how many security vendors have classified a domain as malicious, as their classification process is opaque. Our goal here is to determine if a domain was not only flagged as malicious, e.g., through the use of a blocklist, or labeled as malicious by a DGA classifier, but was indeed observed to be used in the context of distributing executables that were marked as malicious by at least ten vendors. For instance, a domain might be registered by a security researcher or sinkhole operator and still be labeled as malicious, even if it was not used for malicious purposes. To further minimize incorrectly labeled domains, i.e., domains labeled as malicious without being used for malicious purposes, we consider multiple factors:

First, we verify that the domain creation date, reported by VirusTotal, coincides with our observed zone entry date.

Second, we filter domains based on additional timestamps contained in historical WHOIS, passive DNS data, and historical domain popularity rankings, excluding any domains with timestamps that predate our observed zone entry date. This ensures that a domain was not previously used for malicious purposes and then re-registered, e.g., by a benign party.

Third, for time-dependent AGDs, we focus on domains that were *registered in time* (i.e., before the end of their validity periods) and that *became active* (i.e., they were not deregistered before the start of the validity period or potentially re-registered by a benign party).

By incorporating these additional data points, we aim to ensure that our classification of malicious AGDs is robust and accurate. However, we acknowledge that our approach may still not capture all malicious activities, such as C2 domains used to exfiltrate sensitive data or issue bot instructions. With the available data and due to the large scale of our study, it is currently not possible to identify all botnet domains associated with malicious activity. Nonetheless, this methodology allows us to derive a strict lower bound on botnet domains that have recently been used for malicious acts, which is unprecedented in related work and allows us to be the first to estimate the latent threat posed by botnets. Thereby, our approach is effective in highlighting the ongoing need for improved measures to combat the persistent challenge of botnet containment. We present the results of this study in Section IV-A.

As a secondary contribution, we additionally classify all registered AGDs of a single day according to whether they are sinkholed, parked, or blocked in Appendix A.

2) ML-based Classification Study: In our second study, we focus on portraying the threats posed by yet *unknown* DGA-based botnets and analyze to what extent recent advances in ML can be used to detect AGDs among newly registered domains. To this end, we make use of a DL classifier that has been shown to also support the detection of AGDs generated by *unknown DGAs* and *unknown seeds* [10], [14] to assess all domains added daily in all observed zone files. Moreover, we use unsupervised ML to cluster the domains classified as malicious and identify groups of AGDs that are spread across multiple TLDs and are generated by unknown DGAs.

Classifier: We base our classification approach on the context-less ResNet-based binary classifier [10] that operates exclusively on the domain name to be classified to separate benign from malicious domains. Currently this classifier achieves the highest TPR at the lowest FPR [10]. We follow the recommendations by Drichel and Meyer [25] to reduce the biases inherent in state-of-the-art classifiers. We thus train our classifier solely on effective Second-Level Domains (e2LDs), i.e., we ignore domain names of dynamic DNS services[1], public suffixes, TLDs, and any lower-level domains. Thereby, for malicious domains, we focus only on the part of a domain that is generated by a DGA and must be registered by a botnet master, and ignore any information that can be freely chosen. This is particularly important for the TLD as we analyze a variety of different zone files, and it was demonstrated that the detection by a bias-affected classifier can be bypassed by simply switching the TLD [25].

To train the ML classifier, we obtain samples labeled as malicious from the OSINT feed of DGArchive [1]. In contrast to previous work, we cannot use benign labeled training data extracted from real-world networks due to our classification setting in which we classify newly registered domains. One way to obtain benign training samples is to generate them artificially based on public top sites rankings such as Tranco [71]. The problem with artificial data, however, is that it may not accurately reflect the true distribution, leading to bias and misleading results. Due to the lack of ground truth, we cannot extract benign training samples directly from the zone files, as they also contain malicious domains. While filtering against all samples of DGArchive would remove most AGDs of known DGAs, AGDs of unknown DGAs would remain.

In our work, we therefore use a simple heuristic to determine benign domains. An initial analysis of registered AGDs revealed that they generally do not contain any mail exchange (`MX`) records together with `TLSA` records [72]. Thus, we assume that domains which contain `MX` records alongside with `TLSA` records are, on average, significantly more likely to be used for benign purposes than for malicious purposes, since going through the trouble of setting up a `TLSA` record is another hurdle that an attacker must overcome. In our study, we found evidence that this statement is currently true, but this may change in the future, and therefore new strategies need to be developed to train unbiased classifiers for classifying DNS zone files. From the OpenINTEL project [73], which performs active DNS measurements, we obtain domain names that have `MX` records with the constraint that all `MX` records have a corresponding `TLSA` record. In total, we obtain approximately 1.5 million unique e2LDs under 620 different TLDs as measured on 2022-06-01. Although these domains do not necessarily represent the true distribution of newly registered benign domains, we still think that they are better suited for classifier training in our setting than artificially generated training data. We opt for this heuristic because there is simply no ground truth data available. Note that as early as 2008 [74], `MX` entries were suggested to be potentially beneficial for botnet detection, yet this opportunity has remained largely unexploited. In Section IV-B, we analyze the usefulness of this approach and show that this heuristic is currently sufficient for our purpose of identifying training domains that are not AGDs. While this could change in the future if attackers intentionally set up these entries for AGDs as well, the sheer amount of benign domains would still significantly outweigh the registered AGDs, resulting in only minor contamination of the training data. Note that solely the e2LD and no other information is still used for classifier training and inference.

To train the classifier, we create a balanced dataset consisting of all unique benign labeled e2LDs and malicious labeled e2LDs from DGArchive that were in the OSINT feed until 2022-06-01. We stratify all malicious samples across all DGAs known up to that point in time. Thereby, in total, the training dataset contains approximately three million samples, with malicious samples generated by 105 different DGAs. By using training data available up to 2022-06-01 with malicious samples generated only by DGAs known up to that date, we can guarantee that our evaluations, which include classification of domains registered after 2022-06-01, are free of temporal experimental bias [75].

Methodology: We use the trained classifier to evaluate all daily added domains in all observed zone files for the last month of our evaluation period, i.e., between 2023-06-01 and 2023-07-01. Then, for all domains classified as malicious, we query the address (`A`) records via the various DNS service providers on a daily basis as long as the domains remain in the zone files. This way, we can compare the effectiveness of the classifier not only with the blocklists created by DGArchive, but also with the blocking performed by Cloudflare and Quad9. Additionally, we also measure the reduction in the "window of opportunity" that results from the classifier, i.e., the reduction in time required to include malicious AGDs to the reactive blocklists of security vendors, during which botnet communication is not prevented. During this study, we set

[1] Some DGAs use dynamic DNS services, causing the algorithmically generated part to appear at the third level. However, the domain names of dynamic DNS services should not be marked as malicious by our classifier.

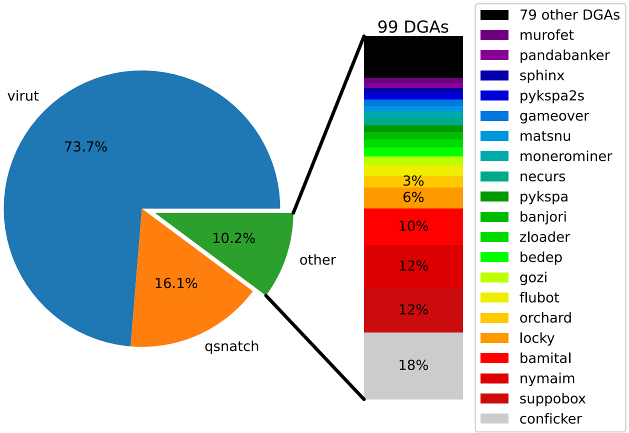

Fig. 1: Distribution of AGDs along different DGAs.

the decision threshold to 0.9 to limit subsequent queries to domains for which the classifier is very confident.

Then, all domains marked by the classifier and finally blocked by the DNS service providers are clustered to find groups of similar domains that most likely belong to the same DGA. Here we use a semi-automatic approach for clustering both TLD-specific domains and all domains together using domain name features that were proposed in [11], [39] as a basis. The features can generally be divided into linguistic, structural, and statistical features, and include features based on length, character distribution, or entropy. We additionally extend the feature set to include the number of English words contained in a domain name to facilitate the clustering of wordlist-based DGAs. In addition, we manually review the found clusters and merge them if necessary. We also examine the proportion of domains that were classified as malicious by the classifier but not blocked by the DNS service providers, from the perspective of whether they can be classified into similar clusters as the blocked samples. We present the results of this study in Section IV-B.

C. Ethical Considerations

We base our research on well-established guidelines [76] and community best practices [77]. As part of our study, we only collect publicly available data and zone files obtained through ICANN's CZDS for TLDs that have actively granted us access for our research. Thereby, our data does not contain any human-derived data and therefore does not contain any Personally Identifiable Information (PII) or quasi-identifiers. To reduce the impact of our measurements, we follow widely accepted Internet measurement guidelines [78]. At all stages of our evaluation, we keep the burden on third parties as low as possible. First, we download all zone files on a daily basis. In deciding to download the data at one-day intervals, we aimed to find an optimal trade-off between obtaining fine-grained data that would allow us to perform our research and avoiding a heavy burden on the data providers. Second, in our ML-based classification study, we set the decision threshold to 0.9 to limit subsequent querying to domains for which the classifier is very confident. This significantly reduces the volume of generated traffic. We always limit the polling rate such that it is completed before the next evaluation epoch in order to spread the traffic over time. Thereby, we avoid traffic peaks at third parties and rate limiting. In addition, we set a pointer (PTR) record for our querying machine, enabling reverse DNS lookups to identify us to third parties and to signal the benign nature of our measurements. During our study, we did not receive any requests with the intent to opt-out of our measurements.

TABLE I: Distribution of DGAs and AGDs across TLDs.

	with *Virut* & *Qsnatch*		**w/o *Virut* & *Qsnatch***	
TLD	**#DGAs**	**#AGDs**	**#DGAs**	**#AGDs**
com	69	506667	67	26363
net	47	17137	46	10762
info	37	26632	36	11990
org	36	12555	35	9884
biz	28	5365	27	1200
ru	24	5149	23	2393
xyz	11	22859	10	651
su	8	1370	7	66
pro	6	1666	5	750
top	5	6659	4	92
other	17	(34 TLDs) 31414	16	(27 TLDs) 773

IV. Evaluation Results

In this section, we present the results of the evaluations outlined in Section III-B1 and Section III-B2.

A. Newly Registered DGA Domains Study

During the 13-month monitoring period, we observe 637 473 unique AGDs spread across 44 TLDs and generated by 101 DGAs entering and exiting the zone files. Conversely, only for 5 out of 106 DGAs we detect no AGD registrations.

In Fig. 1, we visualize the distribution of AGDs along the DGAs. The distribution is strongly imbalanced, with *Virut* and *Qsnatch* generating 89.8% of all AGDs. The other 99 DGAs account only for 10.2% of all AGDs, 79 of which generate less than 1.18% of all AGDs.

In Table I, we display the distribution of DGAs and AGDs across the different TLDs. On the left side of the table we show the results including *Virut* and *Qsnatch*, while on the right side we exclude the two DGAs. Again, the distribution of DGAs and number of samples is very imbalanced, and it can be seen that DGAs favor the large generic TLDs (*.com*, *.net*, *.info*, *.org*), but there are also tendencies towards other generic TLDs such as *.biz*, *.xyz* and *.pro*. In total, there are eleven country code TLDs among the 64 TLDs used by the observed DGAs and monitored by us. Only the two country code TLDs *.ru* and *.su* are used more frequently.

For further analysis, we separate the 101 DGAs into 64 time-dependent and 37 time-independent DGAs.

1) Time-dependent DGAs: In Table II, we show the statistics over all 64 time-dependent DGAs. In total, we observed 633 040 time-dependent AGD registrations over the 13-month monitoring period. 134 194 (21.2%) of the AGDs were registered in time according to their expected DGA schedule (i.e., before their validity period ends and the bots stop querying them). 76 751 (57.2%) of which became active, i.e, they were not deregistered before the start of the validity period or re-registered, e.g., by a benign party. For 5806 (7.6%) of them, we were able to verify that they performed malicious actions as described in Section III-B1.

The 5806 verified malicious samples are generated by 28 different DGAs. We argue that this number is alarmingly high because the registrations as well as the execution of malicious actions could have been prevented by predictive blocking. Moreover, an Internet search of publicly available takedown notices and reports revealed that at least 11 of the 28 DGAs, which are highlighted in bold in the table, have been the target of previous takedown operations, showing that the respective takedown attempts were only of a temporary nature. This does not necessarily mean that the original botnet is still active in its entirety, but it is an indicator that partitions of the botnet may be active or that new botnets may have emerged that reuse a particular DGA. Note that it is possible that an even larger number of botnets have been the target of previous takedown attempts. However, as malware is often known by several names and does not have a unique designation, it is difficult to determine the exact number.

For *Suppobox*, we were able to classify 3864 AGDs as verified malicious, which is particularly high compared to the other DGAs. *Suppobox* is a wordlist-based DGA that concatenates two English words from one of three different wordlists and a total of 1144 words, and appends either the *.ru* or *.net* TLD. The latest wordlist has been known at least since 2015-12-17 [79], and we have confirmed that all detected verified malicious samples consist of the concatenation of exactly two words from the publicly available lists.

For three DGAs (*Ccleaner*, *Darkwatchman*, and *Goznym*) there are no timely registrations at all. We assume that the 87 observed registrations coincidentally match domains generated by these three DGAs, as they generate very short AGDs.

Regarding the percentage of AGDs that are registered and become active afterwards, it is noticeable that for five DGAs (*Blackhole*, *Corebot*, *Cryptolocker*, *Ranbyus*, and *Sutra*) the percentage is zero. One possible reason for this could be that benign parties actively seize and deregister these domains as part of takedown operations. In the case of the two DGAs *Blackhole* and *Sutra*, this is particularly striking, since all the registered domains were registered in time, but none of them ever became active.

Note, in our work, we focus on AGDs that were registered in time to concentrate on AGDs that are most likely to be used for malicious purposes, thereby significantly reducing the number of AGDs to be observed, which aligns with quota limitations for verifying malicious domains. However, it is worth noting that the 498 846 (78.8%) registered AGDs that were not registered in a timely manner could also be used for malicious purposes. In [10], the authors found AGDs queried in large corporate networks outside of their actual validity periods, which they hypothesize could be an intentional attempt to evade simple blocklisting, warranting further investigation to determine the extent of this phenomenon.

TABLE II: Statistics on all 64 time-dependent DGAs.

	total	**reg. in**	**became**	**ver.**	**total**	**reg.-gen.**	**rv-delta[7]**			
DGA	**reg.[1]**	**time[2]**	**active[3]**	**mal.[4]**	**gen.[5]**	**ratio[6]**	**min**	**med**	**avg**	**max**
alien	34	34	73.53%	0	38	89.47%	1	11	23	62
ares	23	14	100.00%	0	1600	0.88%	1	6	7	15
bamital	6528	90	65.56%	0	20540	0.44%	0	24	25	53
bedep	1574	595	100.00%	1	10186	5.84%	0	7	7	7
bigviktor	19	9	100.00%	0	11752	0.08%	1	6	7	15
blackhole	37	37	0.00%	0	730	5.07%	-	-	-	-
ccleaner	3	0	0.00%	0	13	0.00%	-	-	-	-
chaes	13	11	100.00%	0	741	1.48%	4	5	5	5
chinad	504	436	92.89%	0	339323	0.13%	0	0	4	53
conficker	11899	1962	84.81%	3	160437	1.22%	0	1	18	372
corebot	1	1	0.00%	0	18300	0.01%	-	-	-	-
cryptolocker	300	119	0.00%	0	338515	0.04%	-	-	-	-
darkwatchman	81	0	0.00%	0	197500	0.00%	-	-	-	-
diamondfox	5	5	20.00%	0	269	1.86%	0	0	0	0
flubot	1848	916	99.67%	116	539409	0.17%	0	24	26	88
gameover	1127	888	93.02%	4	4345000	0.02%	0	0	4	53
gameover_p2p	259	142	96.48%	109	65000	0.22%	0	6	7	58
gozi	1607	1082	73.66%	11	18146	5.96%	0	5	19	307
goznym	3	0	0.00%	0	0	-	-	-	-	-
infy	56	47	68.09%	0	10260	0.46%	4	20	25	54
kingminer	124	102	68.63%	0	920	11.09%	0	23	24	58
locky	3758	3300	65.24%	40	188017	1.76%	0	24	26	53
m0yvtdd	27	18	61.11%	0	48500	0.04%	5	31	91	235
madmax	14	13	69.23%	0	104	12.50%	6	29	30	59
matsnu	1131	136	81.62%	0	10199	1.33%	14	173	173	332
mirai	7	7	42.86%	0	280	2.50%	26	26	26	26
modpack	73	73	94.52%	1	103	70.87%	1	8	16	353
monerominer	1145	621	99.68%	6	985530	0.06%	0	0	1	3
murofet	837	712	65.17%	0	2986200	0.02%	0	24	25	53
murofetweekly	39	16	68.75%	0	65000	0.02%	5	28	30	58
mydoom	162	162	78.40%	40	1314	12.33%	0	2	12	29
necurs	1184	604	84.44%	4	364459	0.17%	0	49	68	196
nymaim	7697	2813	96.80%	127	84189	3.34%	0	2	41	368
nymaim2	132	32	62.50%	1	8399	0.38%	0	8	16	48
oderoor	51	31	83.87%	8	4948	0.63%	0	14	39	208
orchard	2092	1855	81.40%	77	28440	6.52%	0	24	26	68
orchardgenesis	3	1	100.00%	0	2604	0.04%	0	0	0	0
padcrypt	299	267	65.54%	1	44018	0.61%	0	24	25	53
pandabanker	924	502	84.66%	0	8904	5.64%	0	32	33	68
pitou	240	60	90.00%	0	15156	0.40%	0	0	6	53
proslikefan	297	96	63.54%	0	31600	0.30%	0	25	30	291
pushdo	114	95	98.95%	0	25218	0.38%	10	21	23	84
pykspa	1246	172	76.74%	96	4000	4.30%	0	17	37	303
pykspa2	298	241	91.29%	214	2175	11.08%	0	1	5	53
qadars	186	150	68.00%	8	114400	0.13%	0	22	25	57
qakbot	232	110	89.09%	6	780000	0.01%	0	2	11	62
qsnatch	102800	43438	51.98%	97	112247	38.70%	0	52	80	390
ranbyus	152	9	0.00%	0	117240	0.01%	-	-	-	-
sharkbot	421	412	88.35%	11	3235	12.74%	0	8	21	72
sisron	13	11	72.73%	6	1616	0.68%	2	20	25	55
sphinx	1012	756	83.60%	2	50123	1.51%	0	0	14	67
suppobox	7958	7904	88.75%	3864	138504	5.71%	0	2	19	351
sutra	48	48	0.00%	0	1095	4.38%	-	-	-	-
szribi	46	40	52.50%	0	1940	2.06%	1	25	26	54
tempedrevetdd	541	288	86.81%	46	395	72.91%	0	2	8	53
tinynuke	302	270	65.56%	0	50560	0.53%	0	24	25	53
tofsee	19	3	100.00%	0	580	0.52%	1	1	2	2
torpig	126	66	69.70%	0	5064	1.30%	1	15	21	80
ud2	6	6	83.33%	0	140	4.29%	1	2	16	51
vidro	53	27	62.96%	0	11400	0.24%	0	14	26	208
virut	469751	61294	48.63%	905	3902464	1.57%	0	113	131	394
wd	98	89	65.17%	0	23384	0.38%	0	24	26	53
xshellghost	5	5	80.00%	0	13	38.46%	8	37	42	83
zloader	1456	951	50.16%	2	96644	0.98%	0	2	16	285
64 DGAs	633040	134194	76751	5806	16399080	0.82%				

[1] Total amount of observed AGD registrations.
[2] AGDs that are registered before their validity period ends (registered in time).
[3] AGDs registered in time and not de-/re-registered before the start of their validity period.
[4] AGDs verified as having perpetrated malicious actions as described in Section III-B1.
[5] Total amount of AGDs generated by a DGA during the study period.
[6] Ratio of AGDs registered in time and AGDs generated during the study period.
[7] Days between registration time and start of validity period of AGDs that become active.

In total, over the 13-month period the observed DGAs generated 16 399 080 AGDs across the 44 TLDs. In the seventh column of Table II, we display the ratio of the domains that were registered in time and the total generated samples per DGA. We refer to this ratio as the *reg.-gen.* ratio. This ratio is generally small, indicating that most queries from an infected host result in NX-domain responses.

What remains noticeable are the large reg.-gen. ratios for *Alien*, *Modpack*, and *Tempedrevetdd*. For *Alien* the reg.-gen. ratio is as high as 89.47%. We assume that the reason for this is that the malware which incorporates the *Alien* DGA started to use its DGA during our evaluation period on 2022-12-15 [80]. Since we have not classified any AGDs as verified malicious for this DGA, it is conceivable that a benign party registered the domains in order to prevent harm.

For *Modpack*, we also observe a large reg.-gen. ratio of 70.87%. However, in this case, we observed one verified malicious sample. *Modpack* is also known as *Andromeda*, *Gamarue*, and *Wauchos* [81] and was a common commodity malware that was widespread in 2010 [82]. During our observation period, malicious actors re-registered at least three expired *Modpack* C2 domains, allowing them to receive incoming connections from previous dormant infections and to take over a number of machines [82]–[85]. This again shows the temporary nature of botnet takedowns and the latent danger posed by the supposedly defunct C2 infrastructure.

Tempedrevetdd is the last DGA that shows a strikingly large reg.-gen. ratio of 72.91%. Here, we are able to classify 46 AGDs as verified malicious which corresponds to 18.4% of all *Tempedrevetdd* AGDs that became active. We argue that this is a strong indicator that the botnet is still actively used to spread malware. For other DGAs, such as *Qsnatch*, similar statements can be made, but the reg.-gen. ratios are smaller.

To analyze how far DGA domains would have to be pre-generated to prevent malicious domain registrations we measure the time in days between the registration of a domain and the start of its validity period for all AGDs that become active. We refer to this time difference as *rv-delta* and present the minimum (min), median (med), average (avg), and maximum (max) values for each DGA in the last columns of Table II. For most DGAs, the minimum rv-delta is zero days, which means that a domain is registered on the same day that it becomes valid. Such registrations are most likely made by malicious actors because they do not want to give the defending party enough time to take countermeasures. Sinkhole operators, on the other hand, do not have to fear that their domains will be seized and can therefore register domains several days before the start of their validity period. The median and average values lay between zero and 173 days. The maximum values are between zero and 394, i.e., that at least one *Virut* domain entered the zone on the first day of our observation period and became active on the last day of our evaluation. In the past, AGDs with long rv-delta were registered by malicious actors to timely secure backup domains in case of a later takedown, speculating that these AGDs would not be discovered.

These results indicate that pre-generating AGDs a year in advance and rejecting AGD registrations could effectively prevent most harm caused by known DGA-based botnets.

TABLE III: Statistics on all 37 time-independent DGAs.

	total	**ver.**	**total**	**reg.-gen.**
DGA	**reg.**	**mal.**	**gen.**	**ratio**
banjori	1317	34	32120	4.10%
beebone	13	0	720	1.81%
chir	1	1	50	2.00%
darkshell	45	12	908	4.96%
dircrypt	104	79	1400	7.43%
dmsniff	16	11	269	5.95%
ebury	104	0	2000	5.20%
enviserv	17	9	417	4.08%
feodo	4	4	192	2.08%
fobber	23	4	2000	1.15%
gspy	2	2	49	4.08%
hesperbot	10	0	178	5.62%
kfos	12	7	81	14.81%
m0yv	93	68	888	10.47%
makloader	2	1	512	0.39%
metastealer	43	22	80000	0.05%
necro	3	2	2048	0.15%
omexo	2	2	20	10.00%
phorpiex	104	55	838	12.41%
pseudomanuscrypt	138	30	2300	6.00%
pushdotid	5	1	4808	0.10%
pykspa2s	1049	420	8351	12.56%
ramdo	25	12	6000	0.42%
ramnit	383	237	18867	2.03%
redyms	5	1	34	14.71%
rovnix	24	2	1537	1.56%
shifu	19	16	1554	1.22%
simda	89	53	14551	0.61%
tempedreve	28	21	460	6.09%
tinba	193	64	83977	0.23%
tinyfluff	390	0	30000	1.30%
tsifiri	29	29	59	49.15%
ud3	3	0	20	15.00%
urlzone	2	0	32018	0.01%
vawtrak	121	48	2700	4.48%
vidrotid	1	0	200	0.50%
volatilecedar	14	5	498	2.81%
37 DGAs	4433	1252	332624	1.33%

2) Time-independent DGAs: In Table III, we present the statistics for the 37 time-independent DGAs. Overall, we observed 4433 AGD registrations during the 13-month evaluation period, which is significantly fewer than for the time-dependent DGAs. However, on the other side, we were able to classify 1252 (28.24%) as verified malicious. The AGDs generated by *Banjori* and *Pykspa2s* are the most frequently registered. For *Pykspa2s* we were able to attribute the most samples as verified malicious, i.e., 420 (40.04%) AGDs. The reg.-gen. ratio is highest for *Tsifiri* with 49.15%, here 29 of the 59 generated AGDs were registered. For five DGAs (*Chir*, *Feodo*, *Gspy*, *Omexo*, and *Tsifiri*) we were able to classify all registered AGDs as verified malicious. In total, the 37 time-independent DGAs generate 332 624 AGDs across 44 TLDs, of which only 4433 (1.33%) were registered. Thus, similar to time-dependent DGAs, most requests from an infected host result in NX responses.

Overall, we classified 1252 AGDs generated by 30 DGAs as verified malicious, at least 6 of which are used by botnets that have been the target of previous takedown operations.

3) Key Takeaways:

1) Registrars today do not seem to check domains against DGA blocklists before registering them.
2) Several DGAs, some of which have been known for a long time, are still being used to spread malicious executables. These include DGAs whose botnets have been the target of different takedown efforts in the past.
3) The success of takedown operations is often of temporary nature and supposedly defunct C2 infrastructure can be used to take over dormant infections.
4) Registrars that pre-generate AGDs for about a year in advance would prevent the majority of malicious domain registrations for known reverse-engineered DGAs.

B. ML-based Classification Study

In our second study, we leverage ML techniques to identify clusters of potential unknown DGAs. To this end, we use the trained classifier (see Section III-B2) to assess all domains added daily in all observed zone files. This enables us to detect not only AGDs generated by known DGAs, but also AGDs from yet unknown DGAs. In this context, we also measure the reduction in detection time achieved by the classifier compared to the time of blocking by the DNS service providers.

The classification of all newly registered domains in the period between 2023-06-01 and 2023-07-01 results in a total of 1 102 917 domains that were marked as malicious. During this period, we observed the registration of 43 259 AGDs generated by the known DGAs included in DGArchive, of which our classifier identified 15 007 (34.7%) as malicious at the threshold of 0.9.[2] Notably, this includes 763 AGDs generated by six DGAs that were unknown at training time.

Analyzing the DNS responses of the DNS service providers for the samples classified as malicious by the classifier, we can detect 99 921 (9.06%) samples blocked by Cloudflare or Quad9. 3602 of which were generated by the known DGAs. This corresponds to 8.33% of the AGDs registered by the known DGAs during this period. Therefore, the classifier detects approximately four times more AGDs of known DGAs than are blocked by the service providers.

Since we query the domains classified as malicious on a daily basis, we can calculate how long it takes for the two DNS service providers to block a malicious domain after it is registered. Of all the domains that are eventually blocked, Cloudflare blocks a total of 1993 domains, while Quad9 blocks 98 682. The minimum time required for blocking a malicious labeled domain is zero for both providers, i.e., a malicious domain is blocked on the same day it is registered. Cloudflare blocks domains after one day in the median and after four days on average, for Quad9 it takes one day longer in each case. For both providers, the maximum time required to block a domain flagged as malicious is 29, which means that a malicious domain is registered on the first day of the evaluation period, but is not blocked until the last day. This suggests that other domains classified as malicious by the classifier could be blocked by the DNS service providers at a later date.

```
pf3q5.cfd
84nfgu.cfd
k9gvrw.cfd
```
Cluster 1

```
uuvp.cfd
zxcloifsa.cfd
yyjbpxzjlt.cfd
```
Cluster 2

```
1w2mm.cfd
778aa.cfd
ungqq.cfd
```
Cluster 3

```
111cxzv.cfd
111gdfhdf.cfd
333gbfdbfd.cfd
```
Cluster 4

```
bhdbpidjcogbbobeffiiejrsfbssupmu.makeup
bsicspejegjfppeemfpgfsumrsraegpr.makeup
cpodjdohmfcapacoouufjdfhebspigba.makeup
```
Cluster 5

```
uc1qgc0kuzjajg21nbu-7otq.lat
uc2-jcvrrq-krxt2cotejknw.pics
ucyy4krbsugzoj1cjyj4nzqq.pics
```
Cluster 6

```
bwfknhu.live
bwfknhu.site
bwfknhu.online
```
Cluster 7

```
aydwuihwuqoha0.info
aydwuihwuqoha1.info
aydwuihwuqoha2.info
```
Cluster 8

```
amazonprgkcg.com
amazonddksisd.com
amazonklbphbty.xyz
```
Cluster 9

```
35374543.xyz
81024199.buzz
23875773.online
```
Cluster 10

```
d6f8c08166.com
29fa20230608.live
c13a856f4a879a89e9a638207efd6c94.biz
```
Cluster 11

```
deny-attempted-access.app
paypal-authorise-login.com
restricted-page-business.solutions
```
Cluster 12

```
addresslecture.shop
securedcitizenslogin.com
popupdistrictfoodhall.online
```
Cluster 13

```
client23-portal.com
trackid-gb174819.com
auth-sett1ngsvrfy.com
```
Cluster 14

```
please-confirm9872454.click
update-cyberspace324912.click
complete-profile57652129.click
```
Cluster 15

```
resolvebnzaccess.com
bnzloginapproval.com
bnzauthenticationauthorisation.com
```
Cluster 16

```
sleamcomnnunily.ru
steamcommmunlty.xyz
steamscomnnunily.com
```
Cluster 17

Fig. 2: Examples of clusters found in the blocked domains.

1) Clustering Blocked Domains: Now we move to clustering all 99 921 blocked samples to find groups of similar domains that most likely belong to the same DGA. In Fig. 2, we present examples of found clusters.

The largest number of domains we observe clustering TLD-specific domains is for the *.cfd* zone. In total, we cluster 27 336 *.cfd* domains which we present in Clusters 1 to 4. These clusters are randomly looking and some of them seem very similar, however, they were separated based on different features such as domain length, used character sets, or common prefix and suffix patterns. However, we cannot rule out that some clusters may still belong to the same campaign.

Cluster 5 contains only samples of length 32 with the *.makeup* TLD. Such clusters are noticeable because there are more domains in the TLD-specific clusters for a certain length than for all other domain lengths. Cluster 6 contains domains of length 24 with *.lat* and *.pics* TLDs. Similar to Cluster 5, such clusters can also be found across multiple TLDs. Cluster 7 includes domains with the same e2LD but with different TLDs. In Cluster 8 there are domains with the same e2LD concatenated to a counter. Such clusters come in different forms, where an incrementing number can be at the beginning, the middle, or the end of a domain. Cluster 9 contains domains with a common prefix. Similar other clusters use a common string that can appear as either a prefix, infix, or suffix. Cluster 10 contains samples consisting only of numbers, while Cluster 11 contains hex-based domains.

[2] Using a high threshold minimizes the load on DNS service providers. A more conservative threshold would naturally increase the detection rate.

Clusters 12 to 17 are wordlist-based clusters that are separated according to various characteristics, such as whether a domain contains hyphens or numbers, as well as the position of certain symbols, and the TLDs used. Clusters 16 and 17 are particularly noticeable because they are target-specific. Cluster 16 comprises phishing domains targeting users of *Bank of New Zealand*, while Cluster 17 consists of hard to recognize typo domains of *steamcommunity.com*. In fact, the domains uncovered in Cluster 17 were later independently verified to be generated by a DGA [86].

In total, we were able to cluster 95 341 of the blocked domains. The remaining 4580 samples are spread across 105 TLDs, 30 of which were not included in any of the clusters we found.

2) Clustering Unblocked Domains: Finally, we also examine the proportion of domains that were classified as malicious by the classifier but not blocked by the DNS service providers, from the perspective of whether they can be classified into similar clusters as the blocked samples. Note that the service providers' blocklists only contain domains that have already acted maliciously, while the classifier also picks up domains that have not yet acted at all. Moreover, a study by Vissers et al. [87] revealed that approximately 20% of malicious domain registrations do not end up in blocklists, and therefore a certain percentage of presumed false positives end up being true positives. Hence, we investigate if the remaining 1 002 996 samples flagged by the classifier form similar clusters, indicating their potential maliciousness.

In total, we were able to group 483 303 (48.19%) domains into similar clusters. In addition to the clusters of the blocked domains, we found another, large cluster consisting of 487 286 (48.58%) domains across 480 different TLDs. All domains in this cluster have a length of 32, consisting of a random combination of letters *a* to *z* and numbers *0* to *9*, which suggests they are highly likely to be algorithmically generated. The remaining 32 407 (3.23%) samples are distributed among 254 TLDs, with 138 TLDs unseen in any blocked domain group.

In order to assess the maliciousness of at least a fraction of domains, we decide to verify all domains that include at least three or more English words via VirusTotal, targeting wordlist-based DGAs. In total, there are 12 886 domains that include three or more words. We were able to classify 1253 (9.72%) as malicious via VirusTotal. The total number of malicious domains is likely even higher. For instance, within the domains that were not blocked by any of the DNS service providers there are two domains that clearly belong to the Cluster 16 of Fig. 2 (*bnzaccessapproval.com* and *bnzconfirmauthenticator.com*). Of these two domains, only one is classified as malicious by VirusTotal. In addition, we observed 69 further domains that include names of popular phishing targets such as *PayPal*, *Facebook*, or *Microsoft*, which are neither blocked by the service providers nor classified as malicious by VirusTotal.

3) Key Takeaways:

1) The classifier is promising for detecting unknown malicious AGDs and shortens detection times by a median of 1-2 days and an average of 4-5 days for all domains that are eventually blocked by the DNS service providers.
2) A large proportion of domains classified as malicious are well clustered and therefore most likely originate from unknown DGAs.
3) A large proportion of domains that are not blocked by the DNS providers are by no means just false positives but can be grouped similarly as the blocked domains.

These results empirically support our decision to use `TLSA` records for the identification of benign domains for classifier training in order to mitigate the problem of missing ground truth. While a thorough performance evaluation of the classifier is not possible due to the lack of ground truth, we note that the classifier has completely fulfilled its intended use of providing insight into the latent threat posed by unknown botnets and highlighting the need for improved countermeasures to combat them effectively. Nevertheless, in the next section, we go beyond providing basic metrics and critically examine the potential operational context for the classifier.

V. Impact & Discussion

In this section, we critically analyze possible approaches to mitigate the threats posed by botnets based on the insights gained in the previous section. Our study revealed that even known and long-standing botnets continue to spread malware. Notably, even botnets that have been subject to previous takedown efforts remain active, highlighting the limited and temporary nature of these interventions. Furthermore, our ML-based classification study revealed the latent threat posed by unknown botnets, emphasizing the urgent need for enhanced countermeasures to effectively counter these persistent threats.

To mitigate the problem with known DGA-based botnets, predictive blocking could be implemented at the registrar/registry level to prevent possible malicious registrations. As shown in Section IV-A, pre-generating AGDs up to a year in advance would have prevented the majority of malicious activities observed in our study. AGD generation is instantaneous and non-resource-intensive, thereby not placing an undue burden on registrars, making it feasible to generate AGDs several years in advance. This mitigates the issue for all known deterministic DGAs.

Here it is important to distinguish between deterministic and non-deterministic DGAs. Most known DGAs are deterministic [1], i.e., all parameters required for DGA execution are known, thus all possible AGDs can be computed in advance. Non-deterministic DGAs use unpredictable but publicly available data for seeding to prevent arbitrary prediction of future AGDs. Hence, for non-deterministic DGAs, attackers and defenders must compete to register domains in each active time window as soon as the unpredictable data used for seeding becomes available. Therefore, for non-deterministic DGAs, AGD generation would need to occur at the time of registration to prevent malicious domain registrations, which completely solves this problem. Further, periodic reassessment of all domains within a registry should be considered after a certain period of time to capture AGDs registered even further in advance as well as when new DGAs emerge.

In this work, we focused on time-dependent AGDs that were registered in time (i.e., before their validity period expires and bots stop querying them) to target AGDs that are most likely to be used for malicious purposes, significantly reducing the number of AGDs to observe and aligning with quota limitations for verifying malicious domains. However, our research also revealed that a significant number of registered AGDs (498 846, or 78.8%) were registered after their intended expiry date. Notably, utilizing AGDs beyond their original validity periods may be an evasion tactic to circumvent simple blocklisting. In fact, in [10], the authors have already observed AGDs being queried in large corporate networks outside of their actual validity periods. Consequently, preventing the registration of time-dependent AGDs outside their validity periods is crucial to mitigate this vulnerability and effectively close the loophole.

Although, mitigating domain abuse is consistent with registrars' responsibilities under the ICANN Registrar Accreditation Agreement [88], and some registrars already have shown their goodwill in preventing abuse (e.g. [89]), this approach increases the workload for registrars. Liu et al. [90] analyzed the impact of various registrar-level interventions and concluded that even if some registrars intervene, attackers still have the ability to quickly switch to a non-intervening registrar. Thus, predictive blocking would only be effective if it were implemented by all registrars/registries. To address this issue, it is essential that all registries implement policies requiring registrars to check domains against known DGA domains. An initiative to enforce such a policy could be spearheaded by ICANN, given their oversight of the DNS root, providing them with a unique vantage point to monitor compliance across all registries. The actual checking process could be facilitated through cooperation with OSINT providers, such as DGArchive. Alternatively, a collaborative effort between researchers, registrars, and registries could focus on reverse-engineering DGAs from captured malware samples and compiling them into accessible lists for the community. A notable example of efforts in this direction is Johannes Bader's GitHub repository [91], which currently contains 53 reverse engineered DGAs. Since DGA domains collide only rarely with benign domains [1], predictive blocking would not lead to problems too often. Note that a domain that is withheld for registration would not pose an immediate problem as the domain is not yet active. Moreover, informing registrants that a domain they intend to register may potentially be included in predictive blocklists could prompt the registrants to register a different domain, thereby avoiding the potential inconvenience of the domain being blocked and the need to manage any associated botnet traffic.

Regarding the threats posed by unknown DGA-based botnets, our ML-based classification study has provided valuable insights. The trained ML classifier successfully fulfilled its purpose, contributing to our goal of shedding light on the latent threat posed by unknown DGA-based botnets and raising awareness of the need for further efforts to contain them. In this context, our classification approach successfully identified multiple clusters of malicious AGDs, including a DGA that was later independently verified, as well as AGDs that clearly belong to malicious clusters not covered by public and commercial threat intelligence feeds. However, we currently consider the classifier's direct application to preemptively block domain registrations with malicious intent to be infeasible. While we were able to group a large fraction of the non-blocked domains of Section IV-B (96.77%) into clusters similar to the blocked domains, and we verified that there are indeed malicious clusters, it is still unclear how many domains of these are false positives. We anticipate that no matter how high the TPR and how low the FPR, the total number of false positive results will be unmanageable due to the significant imbalance between the benign and malicious base rates.

Nevertheless, it is already conceivable that registrars/registries could use the classifier together with the presented clustering, while maintaining a list of known malicious clusters, as an enrichment tool to analyze the maliciousness of a domain registration. In addition, emerging clusters of newly registered domains could be an indicator of new DGAs. Our classification approach thus opens up a promising research direction and holds considerable potential for containing the spread of malicious domain registrations.

Furthermore, we consider the use of the classifier by network operators who have an incentive to keep their networks clean as conceivable. As we have seen in Section IV-A, only a small fraction of the generated AGDs are actually registered. Thus, bots generate multiple NX domain responses before querying a registered domain. These can be analyzed to detect malware-infected machines before they are instructed to perform malicious actions. When using the classifier, it is important to make the decision of whether a host is infected with unknown DGA-based malware dependent on multiple classifications over an evaluation epoch rather than a single result to further reduce false positives in practice.

VI. Conclusion

In this work, we conducted a comprehensive measurement study on the current landscape of registered DGA domains. To this end, we systematically analyzed and quantified the latent threat posed by botnets, including both active botnets and those with seemingly defunct C2 infrastructure. Takedowns are often only of temporary nature and cleanup rates of infected devices are slow. This creates a particularly dangerous situation because the bots, whose botnet was taken down in the past, continue to wait for the attackers to find a way to reconnect to them. During our evaluation period, we observed a decade-old botnet being reactivated by new actors, allowing them to receive incoming connections from previous dormant infections and to take over a number of machines. In our study, we were able to uncover a lower bound of malicious activities performed via 7058 AGDs generated by 58 different known DGAs and showed that at least 17 DGAs are still being used to spread malicious executables, although the respective botnets have been the target of different takedown efforts in the past. Implementing predictive blocklists at the registration stage would have prevented most malicious activities uncovered in our study. However, to make this a reality, registrars need to be incentivized to adopt this practice, requiring the introduction of new mechanisms. Our results emphasize that, despite years of extensive takedown efforts and high detection rates achieved by DGA classifiers in local networks, the issue of botnet containment remains unresolved, calling for a renewed focus from the research community. Finally, our ML classifier, which provided valuable insights into the threat of unknown botnets and demonstrated the potential of ML-based techniques to mitigate malicious domain registrations, also opens up promising avenues for further research.

Acknowledgment

We thank the Cyber Analysis & Defense department of Fraunhofer FKIE and OpenINTEL for providing data for our research. Additionally, we thank all organizations that made their zone data available, either through ICANN's CZDS or through direct publication. The research leading to the results presented in Section IV-B was made possible by OpenINTEL (https://www.openintel.nl/), a joint project of the University of Twente, SIDN, NLnet Labs and SURF. We thank VirusTotal for providing us access to their academic API.

References

[1] D. Plohmann, K. Yakdan, M. Klatt, J. Bader, and E. Gerhards-Padilla, "A Comprehensive Measurement Study of Domain Generating Malware," in *USENIX Security Symposium*. USENIX Association, 2016, https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/plohmann.

[2] D. Piscitello, "Guidance for Preparing Domain Name Orders, Seizures & Takedowns," Internet Corporation for Assigned Names and Numbers, Tech. Rep., 2012, https://www.icann.org/about/staff/security/guidance-domain-seizures-07mar12-en.pdf.

[3] H. Asghari, M. Ciere, and M. J. van Eeten, "Post-Mortem of a Zombie: Conficker Cleanup After Six Years," in *USENIX Security Symposium*. USENIX Association, 2015, https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/asghari.

[4] Y. Nadji, M. Antonakakis, R. Perdisci, D. Dagon, and W. Lee, "Beheading Hydras: Performing Effective Botnet Takedowns," in *Conference on Computer and Communications Security*. ACM, 2013, https://doi.org/10.1145/2508859.2516749.

[5] Y. Nadji, R. Perdisci, and M. Antonakakis, "Still Beheading Hydras: Botnet Takedowns Then and Now," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 5, 2017, https://doi.org/10.1109/TDSC.2015.2496176.

[6] Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, "Identification and Disruption of QakBot Infrastructure," CISA and FBI, Tech. Rep., 2023, https://www.cisa.gov/sites/default/files/2023-08/aa23-242a-identification-and-disruption-of-qakbot-infrastructure.pdf.

[7] Europol, "Qakbot Botnet Infrastructure Shattered after International Operation," 2023, https://www.europol.europa.eu/media-press/newsroom/news/qakbot-botnet-infrastructure-shattered-after-international-operation, online, accessed 2024-09-24.

[8] C. Ardagna, S. Corbiaux, and K. Van Impe, "ENISA Threat Landscape 2024," European Union Agency for Cybersecurity, Tech. Rep., 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[9] E. Alowaisheq, P. Wang, S. Alrwais, X. Liao, X. Wang, T. Alowaisheq, X. Mi, S. Tang, and B. Liu, "Cracking the Wall of Confinement: Understanding and Analyzing Malicious Domain Take-downs," in *Network and Distributed System Security*. Internet Society, 2019, https://dx.doi.org/10.14722/ndss.2019.23243.

[10] A. Drichel, U. Meyer, S. Schüppen, and D. Teubert, "Analyzing the Real-World Applicability of DGA Classifiers," in *International Conference on Availability, Reliability and Security*. ACM, 2020, https://doi.org/10.1145/3407023.3407030.

[11] S. Schüppen, D. Teubert, P. Herrmann, and U. Meyer, "FANCI : Feature-based Automated NXDomain Classification and Intelligence," in *USENIX Security Symposium*. USENIX Association, 2018, https://www.usenix.org/conference/usenixsecurity18/presentation/schuppen.

[12] J. Woodbridge, H. S. Anderson, A. Ahuja, and D. Grant, "Predicting Domain Generation Algorithms with Long Short-Term Memory Networks." arXiv:1611.00791, 2016, https://arxiv.org/abs/1611.00791.

[13] B. Yu, J. Pan, J. Hu, A. Nascimento, and M. De Cock, "Character Level based Detection of DGA Domain Names," in *International Joint Conference on Neural Networks*. IEEE, 2018, https://doi.org/10.1109/IJCNN.2018.8489147.

[14] A. Drichel, J. von Brandt, and U. Meyer, "Detecting Unknown DGAs without Context Information," in *International Conference on Availability, Reliability and Security*. ACM, 2022, https://doi.org/10.1145/3538969.3538990.

[15] I. A. N. A. (IANA), "List of Top-Level Domains: Version 2024102500," 2024, https://data.iana.org/TLD/tlds-alpha-by-domain.txt, online, accessed 2024-10-25.

[16] Domain Name Industry Brief Staff, "The Domain Name Industry Brief, Quarterly Report, Q3 2024," 2024, https://dnib.com/articles/the-domain-name-industry-brief-q3-2024, online, accessed 2024-11-22.

[17] Cloudflare, "Set up Cloudflare 1.1.1.1 resolver," 2024, https://developers.cloudflare.com/1.1.1.1/setup/, online, accessed 2024-08-07.

[18] Quad9, "Threat Blocking," 2024, https://www.quad9.net/service/threat-blocking/, online, accessed 2024-08-07.

[19] M. Kührer, C. Rossow, and T. Holz, "Paint It Black: Evaluating the Effectiveness of Malware Blacklists," in *Research in Attacks, Intrusions and Defenses*. Springer, 2014, https://link.springer.com/chapter/10.1007/978-3-319-11379-1_1.

[20] W. Xu, K. Sanders, and Y. Zhang, "We Know It Before You Do: Predicting Malicious Domains," in *Virus Bulletin Conference*, 2014, https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-XuZhangSanders.pdf.

[21] Google, "Google Safe Browsing," 2024, https://safebrowsing.google.com/, online, accessed 2024-01-04.

[22] The Spamhaus Project SLU, "Spamhaus," 2024, https://www.spamhaus.org/, online, accessed 2024-01-04.

[23] SURBL BV, "SURBL BV - Intelligence and Reputation Services," 2024, https://www.surbl.org/, online, accessed 2024-01-04.

[24] abuse.ch, "URLhaus," 2024, https://urlhaus.abuse.ch/, online, accessed 2024-01-04.

[25] A. Drichel and U. Meyer, "False Sense of Security: Leveraging XAI to Analyze the Reasoning and True Performance of Context-less DGA Classifiers," in *International Symposium on Research in Attacks, Intrusions and Defenses*. ACM, 2023, https://doi.org/10.1145/3607199.3607231.

[26] J. Saxe and K. Berlin, "eXpose: A Character-Level Convolutional Neural Network with Embeddings For Detecting Malicious URLs, File Paths and Registry Keys." arXiv:1702.08568, 2017, https://arxiv.org/abs/1702.08568.

[27] D. Tran, H. Mac, V. Tong, H. A. Tran, and L. G. Nguyen, "A LSTM based framework for handling multiclass imbalance in DGA botnet detection," *Neurocomputing*, vol. 275, 2018, https://doi.org/10.1016/j.neucom.2017.11.018.

[28] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster, "Building a Dynamic Reputation System for DNS," in *USENIX Security Symposium*. USENIX Association, 2010, https://www.usenix.org/legacy/events/sec10/tech/full_papers/Antonakakis.pdf.

[29] M. Antonakakis, R. Perdisci, W. Lee, N. V. II, and D. Dagon, "Detecting Malware Domains at the Upper DNS Hierarchy," in *USENIX Security Symposium*. USENIX Association, 2011, https://www.usenix.org/conference/usenix-security-11/detecting-malware-domains-upper-dns-hierarchy.

[30] M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee, and D. Dagon, "From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware," in *USENIX Security Symposium*. USENIX Association, 2012, https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/antonakakis.

[31] L. Bilge, S. Sen, D. Balzarotti, E. Kirda, and C. Kruegel, "Exposure: A Passive DNS Analysis Service to Detect and Report Malicious

Domains," *Transactions on Information and System Security*, vol. 16, no. 4, 2014, https://doi.org/10.1145/2584679.

[32] M. Grill, I. Nikolaev, V. Valeros, and M. Rehak, "Detecting DGA Malware Using NetFlow," in *IFIP/IEEE Integrated Network Management*. IEEE, 2015, https://doi.org/10.1109/INM.2015.7140486.

[33] S. Schiavoni, F. Maggi, L. Cavallaro, and S. Zanero, "Phoenix: DGA-Based Botnet Tracking and Intelligence," in *Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2014, https://doi.org/10.1007/978-3-319-08509-8_11.

[34] Y. Shi, G. Chen, and J. Li, "Malicious Domain Name Detection Based on Extreme Machine Learning," *Neural Processing Letters*, vol. 48, no. 3, 2018, https://doi.org/10.1007/s11063-017-9666-7.

[35] S. Yadav and A. L. N. Reddy, "Winning with DNS Failures: Strategies for Faster Botnet Detection," in *Security and Privacy in Communication Networks*. Springer, 2012, https://doi.org/10.1007/978-3-642-31909-9_26.

[36] J. Peck, C. Nie, R. Sivaguru, C. Grumer, F. Olumofin, B. Yu, A. Nascimento, and M. De Cock, "CharBot: A Simple and Effective Method for Evading DGA Classifiers," *IEEE Access*, vol. 7, 2019, https://doi.org/10.1109/ACCESS.2019.2927075.

[37] R. Sivaguru, C. Choudhary, B. Yu, V. Tymchenko, A. Nascimento, and M. D. Cock, "An Evaluation of DGA Classifiers," in *International Conference on Big Data*. IEEE, 2018, https://doi.org/10.1109/BigData.2018.8621875.

[38] J. Spooren, D. Preuveneers, L. Desmet, P. Janssen, and W. Joosen, "Detection of Algorithmically Generated Domain Names Used by Botnets: A Dual Arms Race," in *SIGAPP Symposium on Applied Computing*. ACM, 2019, https://doi.org/10.1145/3297280.3297467.

[39] A. Drichel, N. Faerber, and U. Meyer, "First Step Towards EXPLAINable DGA Multiclass Classification," in *International Conference on Availability, Reliability and Security*. ACM, 2021, https://doi.org/10.1145/3465481.3465749.

[40] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards Deep Learning Models Resistant to Adversarial Attacks." arXiv:1706.06083, 2017, https://arxiv.org/abs/1706.06083.

[41] A. Drichel, M. Meyer, and U. Meyer, "Towards Robust Domain Generation Algorithm Classification," in *Asia Conference on Computer and Communications Security*. ACM, 2024, https://doi.org/10.1145/3634737.3656287.

[42] H. S. Anderson, J. Woodbridge, and B. Filar, "DeepDGA: Adversarially-Tuned Domain Generation and Detection," in *Workshop on Artificial Intelligence and Security*. ACM, 2016, https://doi.org/10.1145/2996758.2996767.

[43] I. Corley, J. Lwowski, and J. Hoffman, "DomainGAN: Generating Adversarial Examples to Attack Domain Generation Algorithm Classifiers." arXiv:1911.06285, 2019, https://doi.org/10.48550/arXiv.1911.06285.

[44] N. Gould, T. Nishiyama, and K. Kamiya, "Domain Generation Algorithm Detection Utilizing Model Hardening Through GAN-Generated Adversarial Examples," in *Deployable Machine Learning for Security Defense*. Springer, 2020, https://doi.org/10.1007/978-3-030-59621-7_5.

[45] X. Hu, H. Chen, M. Li, G. Cheng, R. Li, H. Wu, and Y. Yuan, "ReplaceDGA: BiLSTM-Based Adversarial DGA With High Anti-Detection Ability," *Transactions on Information Forensics and Security*, vol. 18, 2023, https://doi.org/10.1109/TIFS.2023.3293956.

[46] Q. Liu, G. Yu, Y. Wang, and Z. Yi, "A Novel DGA Domain Adversarial Sample Generation Method By Geometric Perturbation," in *International Conference on Advanced Information Science and System*. ACM, 2022, https://doi.org/10.1145/3503047.3503080. [Online]. Available: https://doi.org/10.1145/3503047.3503080

[47] W. Liu, Z. Zhang, C. Huang, and Y. Fang, "CLETer: A Character-level Evasion Technique Against Deep Learning DGA Classifiers," *Endorsed Transactions on Security and Safety*, vol. 7, no. 24, 2021, https://doi.org/10.4108/eai.18-2-2021.168723.

[48] L. Nie, X. Shan, L. Zhao, and K. Li, "PKDGA: A Partial Knowledge-based Domain Generation Algorithm for Botnets." arXiv:2212.04234, 2022, https://doi.org/10.48550/arXiv.2212.04234.

[49] X. Shu, C. Cao, L. Wang, and F. Tao, "GWDGA: An Effective Adversarial DGA," in *Frontiers in Cyber Security*. Springer, 2021, https://doi.org/10.1007/978-981-19-0523-0_3.

[50] L. Sidi, A. Nadler, and A. Shabtai, "MaskDGA: An Evasion Attack Against DGA Classifiers and Adversarial Defenses," *IEEE Access*, vol. 8, 2020, https://doi.org/10.1109/ACCESS.2020.3020964.

[51] X. Yun, J. Huang, Y. Wang, T. Zang, Y. Zhou, and Y. Zhang, "Khaos: An Adversarial Neural Network DGA With High Anti-Detection Ability," *Transactions on Information Forensics and Security*, vol. 15, 2020, https://doi.org/10.1109/TIFS.2019.2960647.

[52] Y. Zhai, J. Yang, Z. Wang, L. He, L. Yang, and Z. Li, "Cdga: A GAN-based Controllable Domain Generation Algorithm," in *International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2022, https://doi.org/10.1109/TrustCom56396.2022.00056.

[53] Y. Zheng, C. Yang, Y. Yang, Q. Ren, Y. Li, and J. Ma, "ShadowDGA: Toward Evading DGA Detectors with GANs," in *International Conference on Computer Communications and Networks*. IEEE, 2021, https://doi.org/10.1109/ICCCN52240.2021.9522282.

[54] A. Drichel, U. Meyer, S. Schüppen, and D. Teubert, "Making Use of NXt to Nothing: Effect of Class Imbalances on DGA Detection Classifiers," in *International Conference on Availability, Reliability and Security*. ACM, 2020, https://doi.org/10.1145/3407023.3409190.

[55] M. Tong, G. Li, R. Zhang, J. Xue, W. Liu, and J. Yang, "Far from Classification Algorithm: Dive into the Preprocessing Stage in DGA Detection," in *International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2020, https://doi.org/10.1109/TrustCom50675.2020.00070.

[56] S. Lloyd, C. Hernandez-Gañan, and S. Tajalizadehkhoob, "Towards more rigorous domain-based metrics: quantifying the prevalence and implications of "Active" Domains," in *European Symposium on Security and Privacy Workshops*. IEEE, 2023, https://doi.org/10.1109/EuroSPW59978.2023.00066.

[57] L. B. Metcalf, D. Ruef, and J. M. Spring, "Open-source Measurement of Fast-flux Networks While Considering Domain-name Parking," in *Learning from Authoritative Security Experiment Results*. USENIX Association, 2017, https://www.usenix.org/conference/laser2017/presentation/metcalf.

[58] B. Rahbarinia, R. Perdisci, M. Antonakakis, and D. Dagon, "SinkMiner: Mining Botnet Sinkholes for Fun and Profit," in *USENIX Workshop on Large-Scale Exploits and Emergent Threats*. USENIX Association, 2013, https://www.usenix.org/conference/leet13/workshop-program/presentation/rahbarinia.

[59] T. Tomatsuri, D. Chiba, M. Akiyama, and M. Uchida, "Time-Series Measurement of Parked Domain Names," in *Global Communications Conference*. IEEE, 2020, https://doi.org/10.1109/GLOBECOM42002.2020.9322425.

[60] T. Vissers, W. Joosen, and N. Nikiforakis, "Parking Sensors: Analyzing and Detecting Parked Domains," in *Network and Distributed System Security Symposium*. Internet Society, 2015, https://www.ndss-symposium.org/ndss2015/ndss-2015-programme/parking-sensors-analyzing-and-detecting-parked-domains/.

[61] P. Yang, C. Shan, D. Wang, L. Su, J. Li, and X. Wan, "Mechanism of Parked Domains Recognition Based on Authoritative DNS Servers," in *World Symposium on Software Engineering*. ACM, 2020, https://doi.org/10.1145/3425329.3425335.

[62] J. Zirngibl, S. Deusch, P. Sattler, J. Aulbach, G. Carle, and M. Jonker, "Domain Parking: Largely Present, Rarely Considered!" in *Network Traffic Measurement and Analysis Conferenc*. IEEE, 2022, https://tma.ifip.org/2022/wp-content/uploads/sites/11/2022/06/tma2022-paper26.pdf.

[63] Phil Arkwright, "DGA Domain Detection using Bigram Frequency Analysis," 2017, https://github.com/philarkwright/DGA-Detection, online, accessed 2024-01-08.

[64] Internet Corporation for Assigned Names and Numbers (ICANN), "Centralized Zone Data Service," 2024, https://czds.icann.org/home, online, accessed 2024-08-07.

[65] Estonian Internet Foundation, "Publicly Accessible DNS Zone File: *.ee*," 2024, https://www.internet.ee/domains/ee-zone-file, online, accessed 2024-01-04.

[66] Association Française pour le Nommage Internet en Coopération (AFNIC), "Publicly Accessible DNS Zone Files: *.fr*, *.pm*, *.re*, *.tf*, *.wf*, and *.yt*," 2024, https://www.afnic.fr/en/products-and-services/fr-and-associated-services/shared-data-reuse-fr-data/, online, accessed 2024-01-04.

[67] Swedish Internet Foundation, "Publicly Accessible DNS Zone Files: *.nu*, and *.se*," 2024, https://internetstiftelsen.se/en/zone-data/, online, accessed 2024-01-04.

[68] REG.RU, "Publicly Accessible DNS Zone Files: *.ru*, *.su*, and *.xn–p1ai*," 2024, https://statonline.ru/, online, accessed 2024-01-04.

[69] SK-NIC, "Publicly Accessible DNS Zone File: *.sk*," 2024, https://sk-nic.sk/subory/domains.txt, online, accessed 2024-01-04.

[70] VirusTotal, "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." 2024, https://www.virustotal.com/, online, accessed 2024-08-07.

[71] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczynski, and W. Joosen, "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," in *Network and Distributed System Security Symposium*. Internet Society, 2019, https://www.ndss-symposium.org/ndss-paper/tranco-a-research-oriented-top-sites-ranking-hardened-against-manipulation/.

[72] P. E. Hoffman and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA," RFC 6698, 2012, https://www.rfc-editor.org/info/rfc6698.

[73] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras, "A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 6, 2016, https://doi.org/10.1109/JSAC.2016.2558918.

[74] T. Holz, C. Gorecki, K. Rieck, and F. Freiling, "Measuring and Detecting Fast-Flux Service Networks," in *Network and Distributed System Security Symposium*. The Internet Society, 2008, https://www.ndss-symposium.org/ndss2008/measuring-and-detecting-fast-flux-service-networks/.

[75] F. Pendlebury, F. Pierazzi, R. Jordaney, J. Kinder, and L. Cavallaro, "TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time," in *USENIX Security Symposium*. USENIX Association, 2019, https://www.usenix.org/conference/usenixsecurity19/presentation/pendlebury.

[76] D. Dittrich and E. Kenneally, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," U.S. Department of Homeland Security, Tech. Rep., 2012, https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf.

[77] C. Partridge and M. Allman, "Ethical considerations in network measurement papers," *Communications of the ACM*, vol. 59, no. 10, 2016, https://doi.org/10.1145/2896816.

[78] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast Internet-wide Scanning and Its Security Applications," in *USENIX Security Symposium*. USENIX Association, 2013, https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/durumeric.

[79] Johannes Bader, "Domain Generation Algorithms (DGAs) of Malware reimplemented in Python: Suppobox," 2023, https://github.com/baderj/domain_generation_algorithms/tree/master/suppobox, online, accessed 2023-10-10.

[80] Malpedia, "Alien Malware," 2022, https://malpedia.caad.fkie.fraunhofer.de/details/apk.alien, online, accessed 2023-10-10.

[81] M. Singh, M. Singh, and S. Kaur, "TI-16 DNS Labeled Dataset for Detecting Botnets," *IEEE Access*, vol. 11, 2023, https://doi.org/10.1109/ACCESS.2023.3287141.

[82] S. Hawley, G. Roncone, T. McLellan, E. Mattos, and J. Wolfram, "Turla: A Galaxy of Opportunity," 2023, https://www.mandiant.com/resources/blog/turla-galaxy-opportunity, online, accessed 2023-10-10.

[83] P. Delcher and I. Kwiatkowski, "Tomiris called, they want their Turla malware back," 2023, https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/, online, accessed 2023-10-10.

[84] D. Kapur, T. Shloman, R. Venal, and J. Fokker, "Cyberattacks Targeting Ukraine Increase 20-fold at End of 2022 Fueled by Russia-linked Gamaredon Activity," 2023, https://www.trellix.com/en-us/about/newsroom/stories/research/cyberattacks-targeting-ukraine-increase.html, online, accessed 2023-10-10.

[85] Robert Lemos, "Russia-Linked Turla APT Sneakily Co-Opts Ancient Andromeda USB Infections," 2023, https://www.darkreading.com/attacks-breaches/russia-turla-apt-hijacks-andromeda-usb-infections, online, accessed 2023-10-10.

[86] D. Wise, "RDGAs: The New Face of DGAs," 2023, https://blogs.infoblox.com/threat-intelligence/rdgas-the-new-face-of-dgas/, online, accessed 2024-10-25.

[87] T. Vissers, P. Janssen, W. Joosen, and L. Desmet, "Assessing the Effectiveness of Domain Blacklisting Against Malicious DNS Registrations," in *Security and Privacy Workshops*. IEEE, 2019, https://doi.org/10.1109/SPW.2019.00045.

[88] ICANN, "Registrar Accreditation Agreement," 2013, https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-30apr23-en.pdf, online, accessed 2023-10-12.

[89] Dark Reading Staff, "Google, GoDaddy Help Form Group To Fight Fake Online Pharmacies," 2010, https://www.darkreading.com/risk/google-godaddy-help-form-group-to-fight-fake-online-pharmacies, online, accessed 2023-10-12.

[90] H. L. Liu, K. Levchenko, M. Felegyhazi, C. Kreibich, G. Maier, and G. M. Voelker, "On the Effects of Registrar-level Intervention," in *Workshop on Large-Scale Exploits and Emergent Threats*. USENIX Association, 2011, https://www.usenix.org/conference/leet11/effects-registrar-level-intervention.

[91] Johannes Bader, "Domain Generation Algorithms (DGAs) of Malware reimplemented in Python," 2025, https://github.com/baderj/domain_generation_algorithms, online, accessed 2025-07-16.

[92] S. Alrwais, K. Yuan, E. Alowaisheq, Z. Li, and X. Wang, "Understanding the Dark Side of Domain Parking," in *USENIX Security Symposium*. USENIX Association, 2014, https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/alrwais.

[93] A. Newton and S. Hollenbeck, "Registration Data Access Protocol (RDAP) Query Format," RFC 7482, 2015, https://www.rfc-editor.org/info/rfc7482.

[94] Maltrail, "Maltrail, a Malicious Traffic Detection System," 2023, https://github.com/stamparm/maltrail, online, accessed 2023-10-10.

[95] Malware Sinkhole List, "Malware Sinkhole List in various formats," 2022, https://github.com/brakmic/Sinkholes, online, accessed 2023-10-10.

[96] T. Halvorson, M. F. Der, I. Foster, S. Savage, L. K. Saul, and G. M. Voelker, "From .Academy to .Zone: An Analysis of the New TLD Land Rush," in *Internet Measurement Conference*. ACM, 2015, https://doi.org/10.1145/2815675.2815696.

[97] T. Halvorson, K. Levchenko, S. Savage, and G. M. Voelker, "XXXtortion? Inferring Registration Intent in the .XXX TLD," in *International Conference on World Wide Web*. ACM, 2014, https://doi.org/10.1145/2566486.2567995.

[98] T. Halvorson, J. Szurdi, G. Maier, M. Felegyhazi, C. Kreibich, N. Weaver, K. Levchenko, and V. Paxson, "The BIZ Top-Level Domain: Ten Years Later," in *Passive and Active Measurement*. Springer, 2012, https://link.springer.com/chapter/10.1007/978-3-642-28537-0_22.

Appendix

In this section, we provide an overview of all registered DGA domains. To this end, we evaluate all registered AGDs of a single day according to whether they are sinkholed, parked, or blocked by the two major DNS service providers Cloudflare and Quad9.

Sinkholing is used by law enforcement agencies and security researchers to disrupt active botnets. There, the botnet's C2 infrastructure is targeted by redirecting traffic from AGDs to a new destination, the sinkhole. This is achieved by setting the DNS records of the AGDs to be taken down to point to the sinkhole server. With this technique, it is possible to mimic the operation of a C2 server to prevent the infected hosts from connecting to other C2 domains.

A parked domain resolves to an undeveloped website that has no content except for automatically computed advertisements, with the intention of making profit from it. The domain parking business generates significant revenues in the millions [92]. AGDs can be parked to abuse auto-generated traffic routed from infected hosts to a domain parking system [1].

Before presenting our findings, we first describe our methodology and additional ethical considerations.

A. Methodology

We analyze all AGDs that were active on 2023-06-30, the last day of our evaluation period. Thereby, we analyze all domains that were included in our previous study of newly registered DGA domains (see Section III-B1 and Section IV-A), provided they were not removed from the zone files by that date. In addition, we also analyze all AGDs that were registered before the start of our evaluation period on 2022-06-01 and whose registration status did not change during the observation period.

We attribute all active AGDs according to whether they are (1) sinkholed, (2) parked, or (3) blocked by two major DNS service providers (Cloudflare and Quad9). For all domains, we query the DNS `A` records via the DNS servers of Cloudflare, Quad9, and Google. We also query possible `NS` and `PTR` records via the Google DNS server. Lastly, if we could not attribute a domain with the data already collected, we additionally perform a Registration Data Access Protocol (RDAP) [93] query. In this way, we reduce the load on third parties and only perform an RDAP query when necessary.

1) Sinkholed Domains: To identify sinkholed AGDs we follow a semi-automatic approach:

First, we compile a list of known sinkhole name servers. We base our list on the data from [9] in which the authors manually reviewed published takedown court orders and security reports that described takedown incidents to identify domain names of sinkhole name servers. Further, we extend the list using additional resources that were publicly available including data gathered from open source projects such as [94], [95]. We do not use the sinkhole IPs reported in the data sources because some of the resources are even older than ten years and therefore the reported IPs are likely outdated.

Second, for each domain name, we check whether the collected `SOA`, `NS`, `PTR`, and `CNAME` records or potentially collected RDAP information contain a known sinkhole name server. If this is the case, we perform an RDAP query on the IP address to which the domain resolves to identify possible sinkhole operator networks.

Third, we manually review the potential sinkhole operator networks and remove all network ranges for networks of hosting providers that allow Internet users to host arbitrary content to avoid mislabeling when we filter for the identified sinkhole operator networks. Then, we filter all unassigned domains against the list of sinkhole operator networks and classify domains as sinkholed if their IP address lies in the network of a sinkhole operator.

2) Parked Domains: To identify parked domains, we use the DNS-based indicators proposed in the study by Zirngibl et al. [62] in 2022. The authors state that the DNS-based indicators retain their validity over time due to the general stability of parked domains. Note that DNS name sever labeling to identify parked domains, such as carried out in [19], [58], was identified to be suboptimal and leads to false positive results [56].

3) Blocked Domains: Lastly, we analyze what fraction of DGA domains are blocked by Cloudflare and Quad9, which actively refuse to resolve domain names with malicious intent. Both DNS service providers integrate commercial and publicly available threat intelligence feeds. To this end, we compare the collected DNS `A` records from Cloudflare and Quad9 with those from Google, which does not perform any blocking. If Google resolves a domain name but one of other providers does not, the domain is considered as blocked.[3]

B. Additional Ethical Considerations

The same ethical considerations as described in Section III-C apply to this study. At this point, however, we also emphasize our ethical considerations regarding the use of RDAP/WHOIS information. Similar to previous studies on zone files (e.g. [56], [96]–[98]), we also make partial use of RDAP/WHOIS data to improve our analysis.

First, we reduce the total number of domains to be queried as far as possible. To portray the current landscape of registered DGA domains, we focus on all registered domains in a single day, rather than over the entire observation period. Here, we explicitly focus on domains that are included in DGArchive which reduces the total amount of domains to analyze from approximately 240 million to 757 311 domains. Then, before performing any RDAP/WHOIS requests, we first try to classify a domain based on collected `SOA`, `NS`, `PTR`, and `CNAME` records. Only if we cannot classify a domain on the basis of this data do we resort to an RDAP/WHOIS query. Thus, similarly to [56], we first significantly reduce the list of domains to a reasonable size before conducting any RDAP/WHOIS requests.

Note that we limit our analysis to known DGA domains included DGArchive and do not relate to users, personally identifiable information, or otherwise privacy-sensitive data. Since AGDs have been shown to collide only marginally with benign domain names [1], sensitive data from benign users is practically not captured. Even if sensitive data may occasionally still be present, it is not considered in any way.

Finally, we limit the query rate in order to distribute the traffic over time and avoid traffic peaks for data providers. During our measurements, we did not receive any inquiries to opt out of our study.

C. Evaluation Results

As of 2023-06-30, there are 757 311 AGDs registered within the observed zone files. Only 178 529 (23.57%) of which were also analyzed in our previous study of newly registered DGA domains in Section IV-A. The other 578 782 AGDs were registered prior to the start of our evaluation period on 2022-06-01 and their registration status did not change since then. Most of these older samples are likely less relevant for understanding current DGA-based threats, as they were registered a long time ago and their registration status has remained unchanged. Such samples could potentially be remnants of already mitigated campaigns.

With our classification approach described in Section A we are able to attribute 349 002 AGDs. In Fig. 3, we present a Sankey diagram to visualize the distribution between sinkholed, parked, and blocked AGDs. We split the attributed samples into potential malicious and verified malicious AGDs. Of the 7058 verified malicious AGDs from the previous evaluation (see Section IV-A), 1552 had already been deregistered,

[3] Cloudflare actually responds with “0.0.0.0” when a domain is blocked.

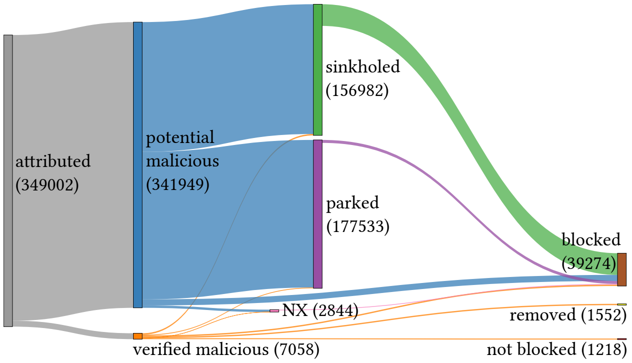

Fig. 3: Share of sinkholed, parked, and blocked AGDs.

leaving only 5506 remaining in the zone files as of 2023-06-30. We are able to classify most AGDs (177 533) as parked, 156 982 AGDs as sinkholed, and a total of 39 274 AGDs as blocked by at least one of the two DNS providers. In addition, we categorize 2844 AGDs as non-existent (NX) because they no longer had a valid A record. Note that 25 956 (66.09%) AGDs that are blocked are also sinkholed. This is not particularly useful because the sinkhole operator may mimic the operation of a C2 server to prevent the infected hosts from connecting to other C2 domains.

Of the verified malicious AGDs that are still registered, 1698 are sinkholed, of which 1347 are also blocked. 2099 AGDs are not sinkholed but blocked, so that a total of 3446 (62.59%) AGDs are actually blocked by DNS service providers. 1218 verified malicious AGDs are neither classified as parked, sinkholed, NX, nor blocked. However, this does not necessarily mean that they are still distributing malware. They could also be sinkholed by an unknown party.

Cloudflare and Quad9 block a different number of AGDs. Cloudflare blocks a total of 5689 domains, of which 2886 are not sinkholed. Quad9, on the other side, blocks 35 318 AGDs, of which 10 766 are not sinkholed. Together they block 13 318 not sinkholed domains.

Analyzing the available RDAP data for non sinkholed domains, we can estimate the distribution of registrars used by malicious actors and analyze whether there is a prevalence. The distribution of registrars is strongly imbalanced. In total, 893 different registrars were used. The most frequently used registrar accounts for 20.8% of all registrations. And the top ten registrars account for 55.6% of all registrations. We refrain from naming the registrars as domains can be transferred to other registrars by seizing orders and a registrar may also be a takedown executor.

In summary, we have provided a rough overview of the landscape of registered AGDs and have shown that a large number of domains are sinkholed but also a large number of them are additionally blocked, a combination which is not particularly useful. Although we could not attribute all AGDs and our classification approach is not 100% accurate, we were able to show that some malicious domains could go unnoticed and are not included in the set of public and commercial threat intelligence feeds used by the DNS service providers. This is critical due to the asymmetric situation where the defenders need to block all possible AGDs, while it is enough for the botnet master if a single domain successfully resolves. Note, while this evaluation presented here is based on a single day, we also partially evaluated the active DGArchive domains one month and four months prior to the actual evaluation and measured similar distributions of sinkholed, parked, and blocked AGDs.